IBM Americas, ATS, Washington Systems Center

An Integrated Cryptographic Service Facility (ICSF HCR77A0) for z/OS Update for zEC12

Share 12685

San Francisco, CA February, 2013

Greg Boyd (boydg@us.ibm.com)

QR Code

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.

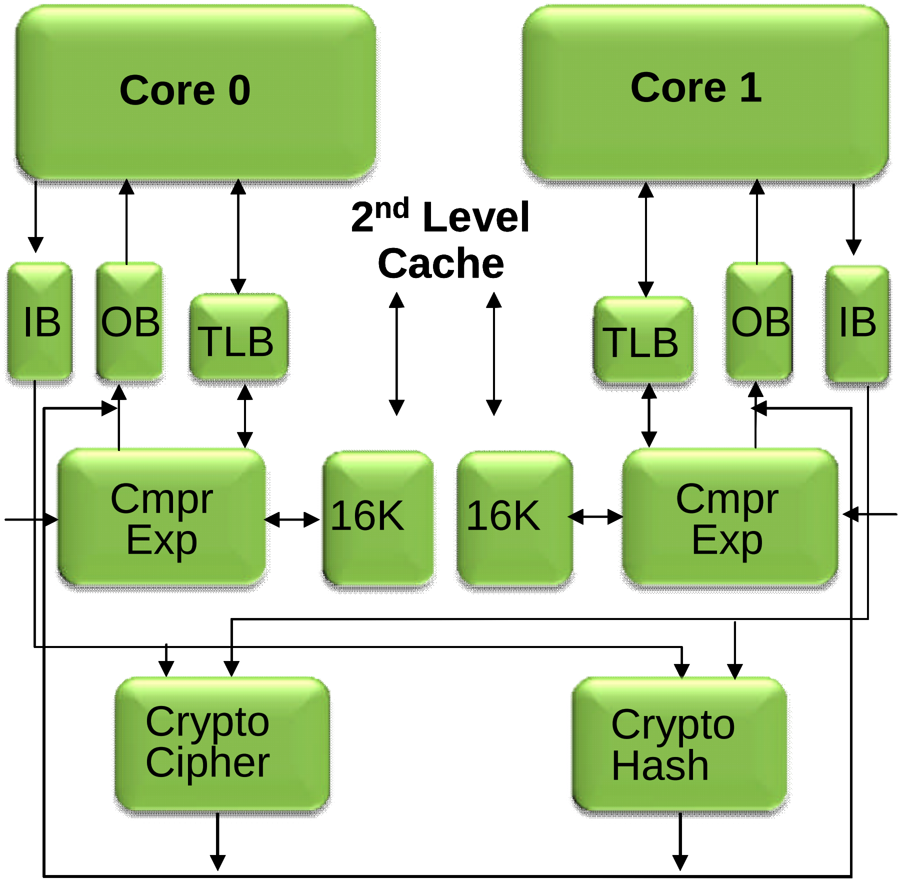
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- **zEC12 Hardware Changes**
  - –CPACF
  - –Crypto Express4S
- **TKE V7.2**
- **ICSF HCR77A0**
- **A couple of other things**

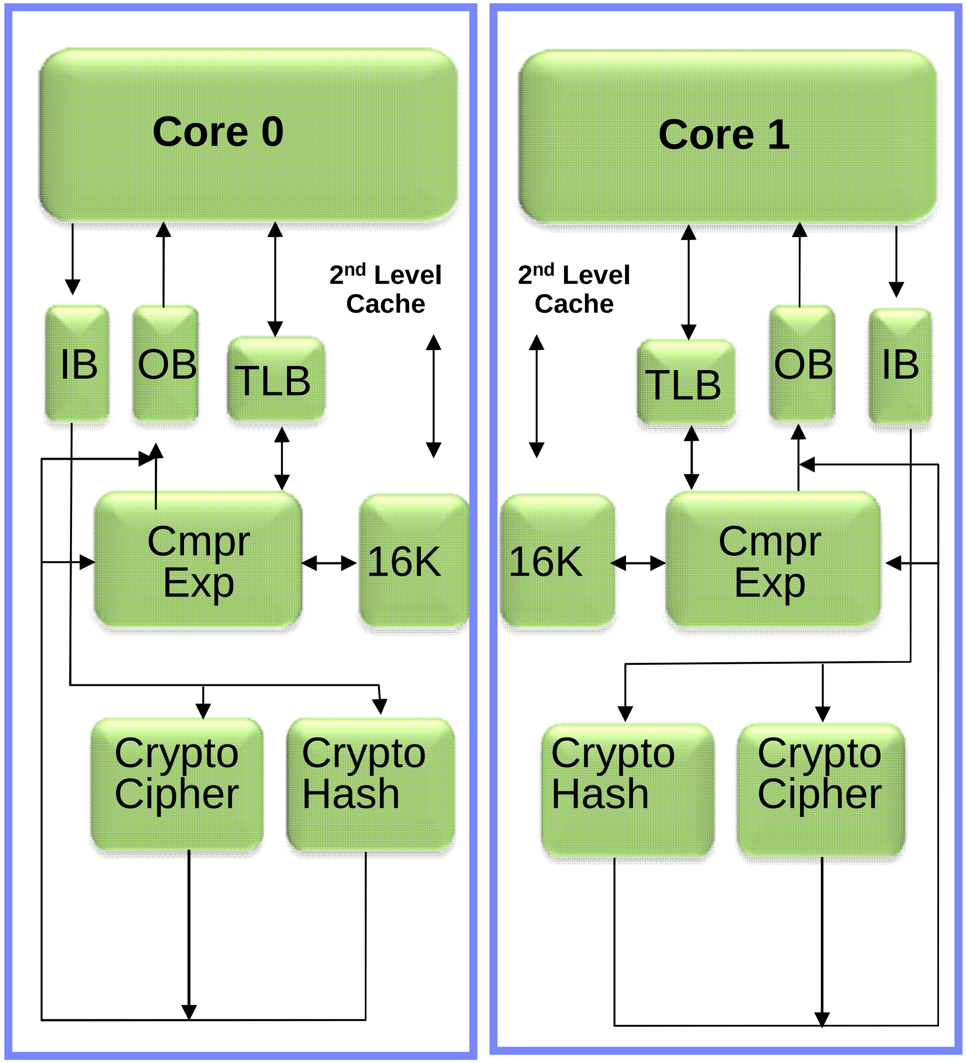
z196/z114/z10 Compression and Cryptographic Engine

- **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



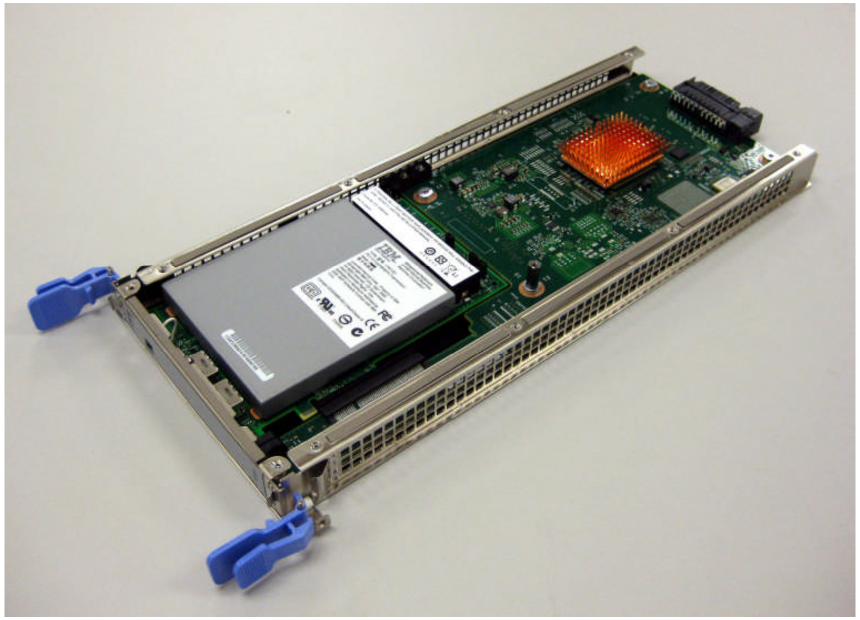
zEC12 Compression and Cryptographic Engine

- **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)**

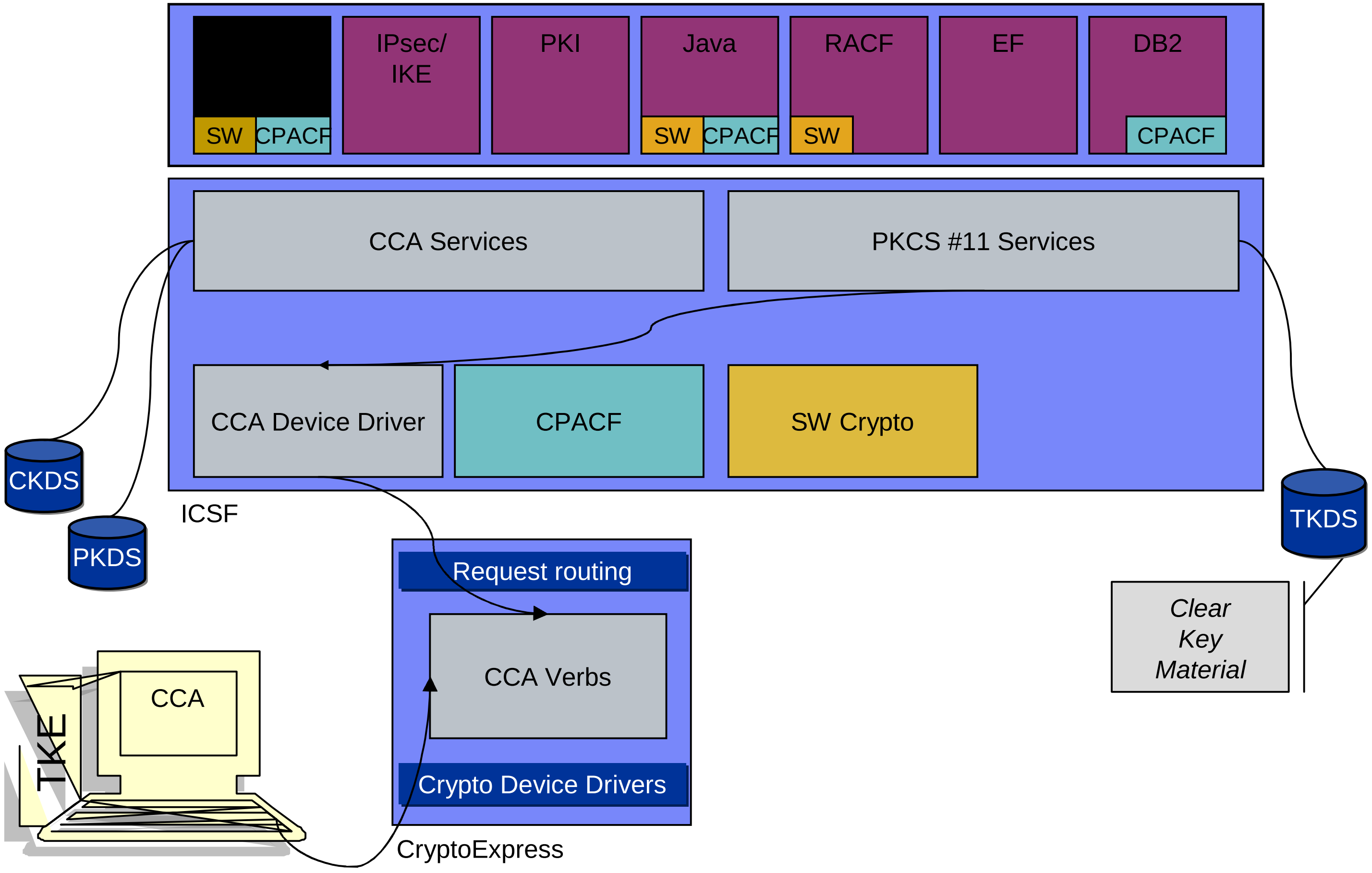
  Since there isn't a real standard for cryptographic tokens, this API has been developed to be an abstraction layer for the generic cryptographic token. **The PKCS #11 API defines most commonly used cryptographic object types (RSA keys, X.509 Certificates, DES/Triple DES keys, etc.) and all the functions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

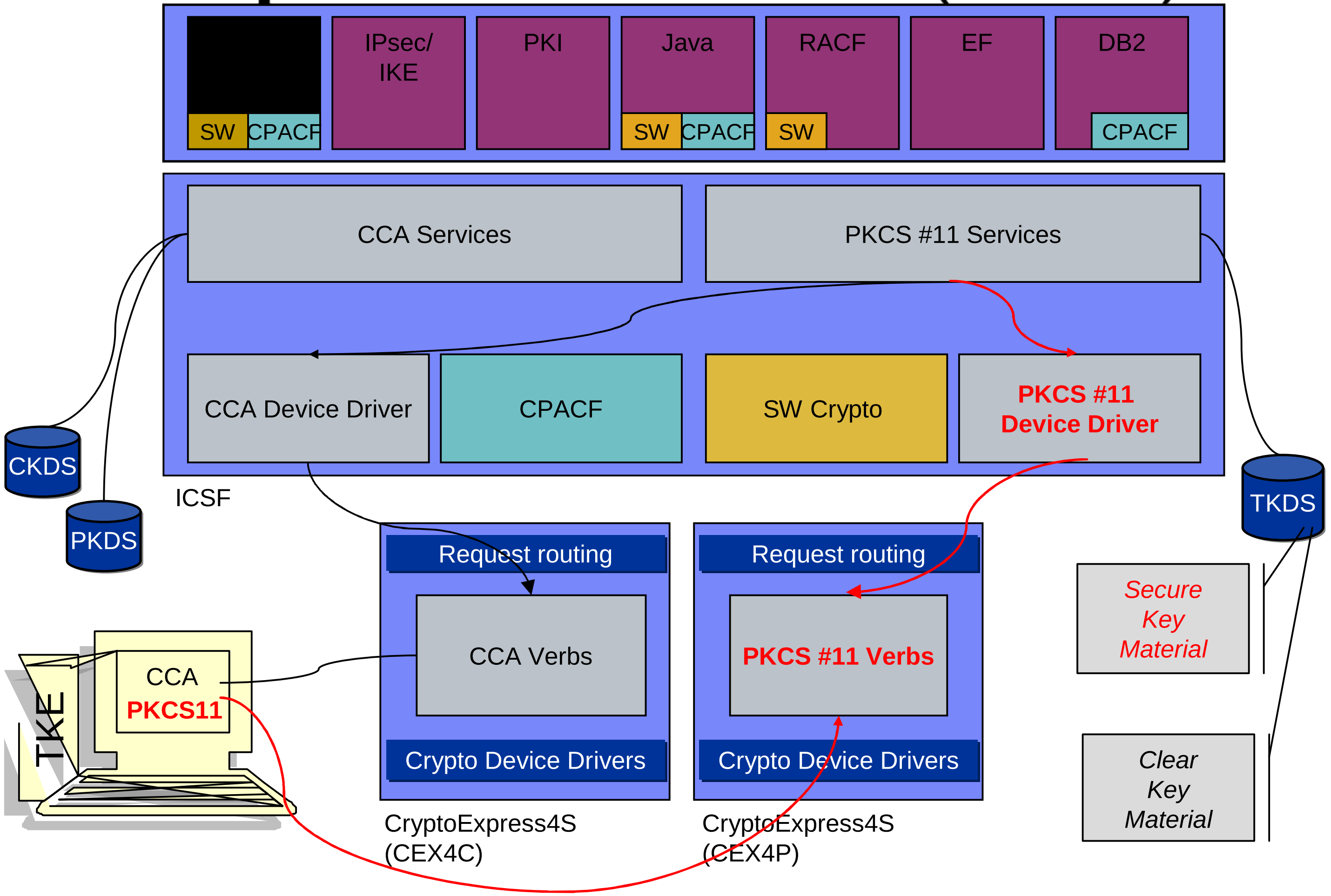
  This standard specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. **Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (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

zEC12 I/O Feature Cards

Features	Offered As	Maximum # of features	Maximum channels	Increments per feature	Purchase increments
FICON					
FICON Express8S	NB	**160**	**320 channels**	**2 channels**	**2 channels**
FICON Express8	CF*	**44**	**176 channels**	**4 channels**	**4 channels**
FICON Express4 10km LX, SX	CF*	**44**	**176 channels**	**4 channels**	**4 channels**
ISC-3 Coupling	CF*	**12**	**48 links**	**4 links**	**1 link**
OSA-Express					
OSA-Express4S 10 GbE	NB	**48**	**96 ports**	**1 port/1 channel**	**1 feature**
OSA-Express4S 1 GbE OSA-Express4S 1000BASE-T**	NB	**48**	**96 ports**	**2 ports/1 channel**	**1 feature**
OSA-Express3	CF*	**24**	**96 ports**	**2 (10 GbE) / 4 ports**	**1 feature**
Crypto					
Crypto Express4S**	NB	**16**	**16 PCIe adapters**	**1 PCIe adapter**	**1 feature *** **
Crypto Express3* **	CF*	**8**	**16 PCIe adapters**	**2 PCIe adapters**	**1 feature *** **
Special Purpose					
Flash Express**	NB	**8**	**8 PCIe adapters**	**1 PCIe adapter**	**2 features**

* CF - Carry forward ONLY

** NB – New Build (New on zEC12)

*** Two features initially, one thereafter

Not Supported – ESCON, Crypto Express2, FICON Express2 (or older FICON), OSA-Express2, and Power Sequence Control

IBM Enterprise PKCS #11 Model

- **Based on PKCS #11 specifications v2.20 and more recent amendments**
- **Supports secure PKCS #11 keys**
  - Keys that never leave the secure boundary of the coprocessor unencrypted
- **Designed to meet Common Criteria (EAL 4) standards and FIPS 140-2 Level 4 requirements**
  - Certifications tailored to meet requirements of this market place
- **Conforms to the Qualified Digital Signature (QDS) Technical Standards**
  - Becoming a mandate by the European Union
  - High qualiity electronic signatures
    - Trusted to the same extent as hand written signatures
  - Uses: Smart passports, national id cards …
- **Supported on Crypto Express4S only**
- **Requires a TKE Workstation with TKE 7.2 LIC**

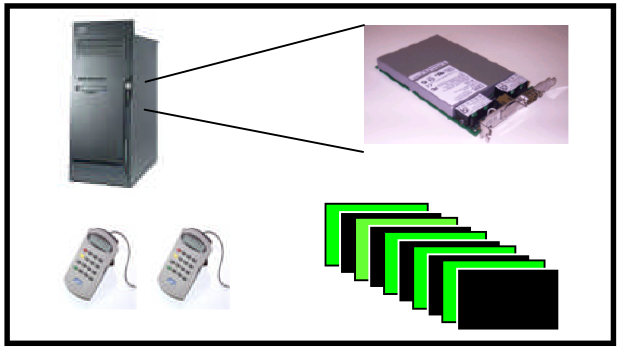
IBM Common Cryptographic Architecture (CCA) Enhancements

- **Wrap weaker keys with stronger keys for security standards compliance**
  - 24-Byte DES-MK
- **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**

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

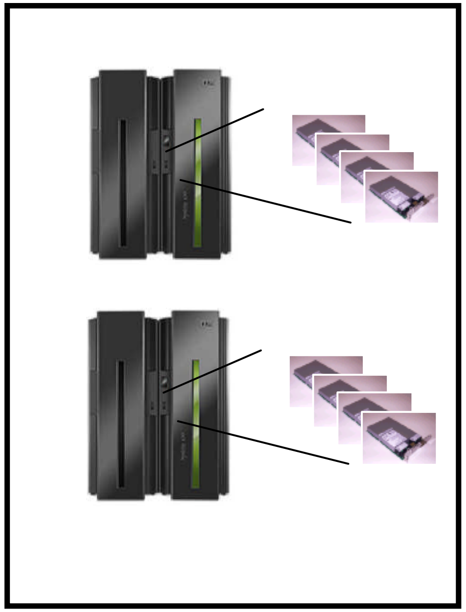


Purpose

- **Used to manage multiple Cryptographic Coprocessors and keys on various generations of System z (zEC12, 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



TKE 7.2 – Support up to four smart card readers

- EP11 host crypto module administration requires use of smart cards.
- EP11 host crypto modules command signing structure different from CCA.
  - Up to 8 signatures required. (User configured 1-8)
  - Each signer must have a unique smart card.
- The amount of smart card swapping could be very high, if reader count limited to 2.
  - Swapping implies constant PIN re-entry.
  - Potential usability issue even with low signature requirement.
- Support 2, 3, or 4 smart card readers on the TKE. The minimum of 2 will not change.
- Because of the “shortage” of USB ports on the workstation, you can install an unpowered or powered USB hub.

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

HCR77A0

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

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.

ICSF Coprocessor Management Panel

```
 --------------------------------------------------------------------------------
|                                                                                |
|  CSFGCMP0 ---------------- ICSF Coprocessor Management ---------------------  |
|  COMMAND ===>                                                                  |
| Select the coprocessors to be processed and press ENTER.                       |
| Action characters are: A, D, E, K, R, and S. See the help panel for details.  |
|                 Serial                                                         |
|   CoProcessor     Number         Status      AES    DES    ECC    RSA    P11   |
|   -----------    ---------       ------      ---    ---    ---    ---    ---   |
|  __ H01                          ACTIVE                                        |
|  __ G02          24778902        ACTIVE       A      A      A      A           |
|  __ G05          98001236        OFFLINE                                       |
|  __ SP08         97006090        ACTIVE                                  A     |
|  __ SA09         97006094        ACTIVE                                        |
|  __ SC14         97006062        ACTIVE       A      A      A      A           |
|                                                                                |
 ----------------------------------------------------------------------------
```

CEX4S prefix values:

- **SA – Accelerator**
- **SC – CCA Coprocessor**
- **SP – Enterprise PKCS #11 Coprocessor**

Software support at GA

z/OS Support :

- z/OS V1 R13 with PTFs (Exploitation plus Flash Express and IBM zAware Support)
- z/OS V1R12 with PTFs (Exploitation)
- z/OS V1R11 with PTFS (Toleration, Lifecycle Extension required after September 30, 2011)
- z/OS V1R10 (Toleration, Lifecycle Extension Required)

z/VM Support :

- VM65007 – Compatibility support for CEX4SA

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 will not recognize a CEX4S; it can use a CEX3 on the zEC12

TPF Support:

- PJ40362 – Support for CEX4S (accelerator mode only)
- PJ40387 – Support for local IPTE (nothing to do with crypto)

Linux on System z Support:

- IBM intends to support zEC12 with the following distributions:
  - SUSE SLES 10 and SLES 11,
  - Red Hat RHEL 5 and RHEL 6

Toleration Maintenance – HCR7770, HCR7780 or HCR7790 on zEC12

- **CEX4S Toleration – OA39075**
  - Versions of ICSF prior to HCR77A0 require this APAR to use the CEX4S in toleration mode (it treats the CEX4S like a CEX3)
- **VM Toleration – OA40267**
  - Timing issue with VM

Toleration Maintenance – HCR7750*, HCR7751*

- **CEX3 Toleration – OA29839**
  - Toleration support for CEX3

*These versions of ICSF are out of support

Toleration Maintenance – Sharing a PKDS

- **HCR7770, HCR7780, HCR7790 require toleration maintenance if they will share a key repository with HCR77A0**
  - Weak key wrapping – OA39484
    - New RSA private key section can't be used by earlier releases

Sharing a KDS (old news) - but still applies

- **Prior versions of ICSF introduced new key tokens**
  - HCR7770
    - New TKDS record - OA29997
  - HCR7790
    - X9.24 CBC Key Wrapping – OA33320
    - Variable Length AES keys – OA36718

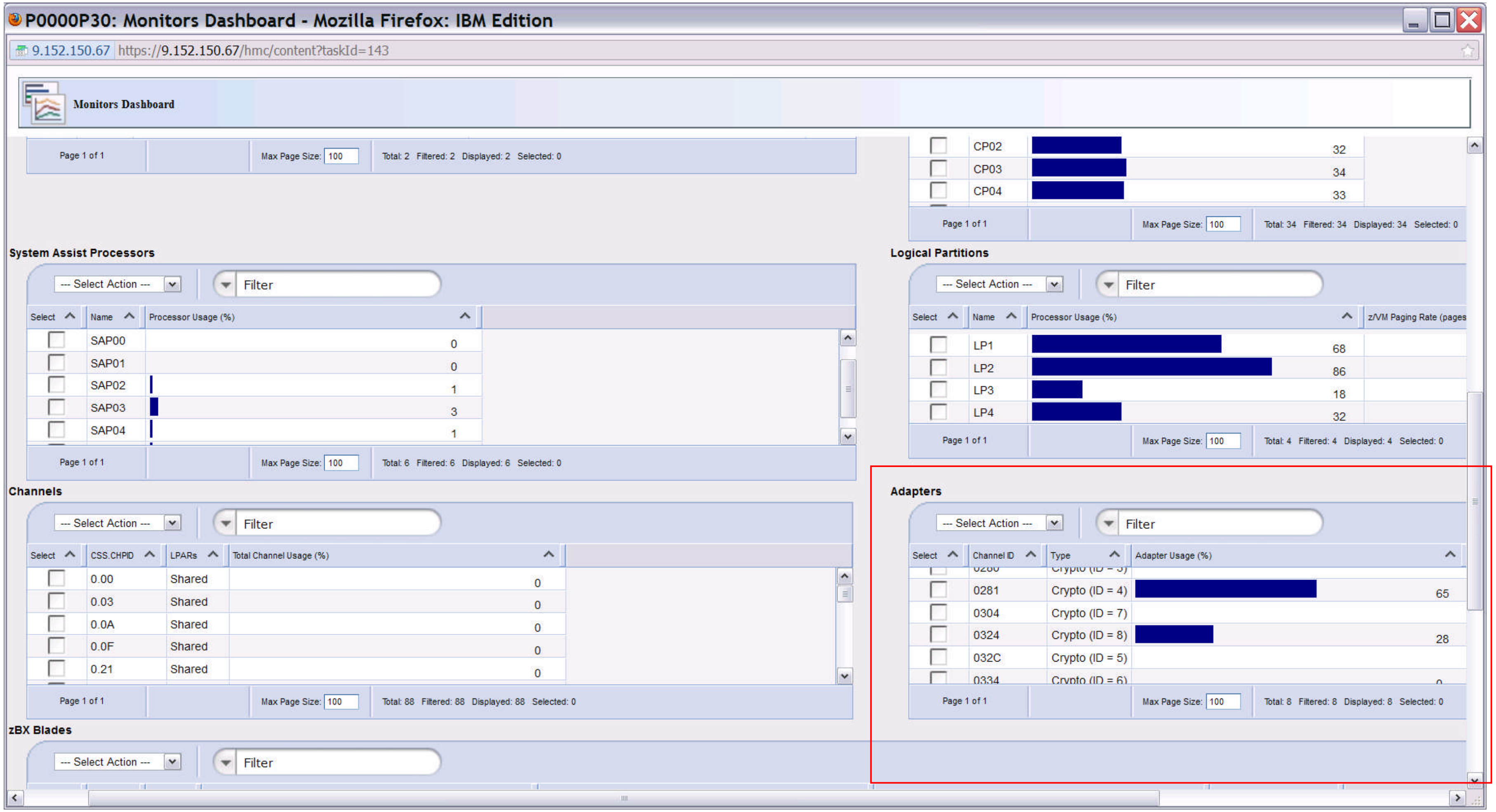
A Couple of Other Things

- **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



P0000P30: Monitors Dashboard - Mozilla Firefox: IBM Edition
9.152.150.67 https://9.152.150.67/hmc/content?taskId=143
Monitors Dashboard

Page 1 of 1 | Max Page Size: 100 | Total: 2 Filtered: 2 Displayed: 2 Selected: 0

Select	Name	Processor Usage (%)
□	CP02	32
□	CP03	34
□	CP04	33

Page 1 of 1 | Max Page Size: 100 | Total: 34 Filtered: 34 Displayed: 34 Selected: 0

System Assist Processors

--- Select Action ---
Filter

Select	Name	Processor Usage (%)
□	SAP00	0
□	SAP01	0
□	SAP02	1
□	SAP03	3
□	SAP04	1

Page 1 of 1 | Max Page Size: 100 | Total: 6 Filtered: 6 Displayed: 6 Selected: 0

Logical Partitions

Select	Name	Processor Usage (%)	z/VM Paging Rate (pages
□	LP1	68	
□	LP2	86	
□	LP3	18	
□	LP4	32	

Page 1 of 1 | Max Page Size: 100 | Total: 4 Filtered: 4 Displayed: 4 Selected: 0

Channels

Select	CSS.CHPID	LPARs	Total Channel Usage (%)
□	0.00	Shared	0
□	0.03	Shared	0
□	0.0A	Shared	0
□	0.0F	Shared	0
□	0.21	Shared	0

Page 1 of 1 | Max Page Size: 100 | Total: 88 Filtered: 88 Displayed: 88 Selected: 0

Adapters

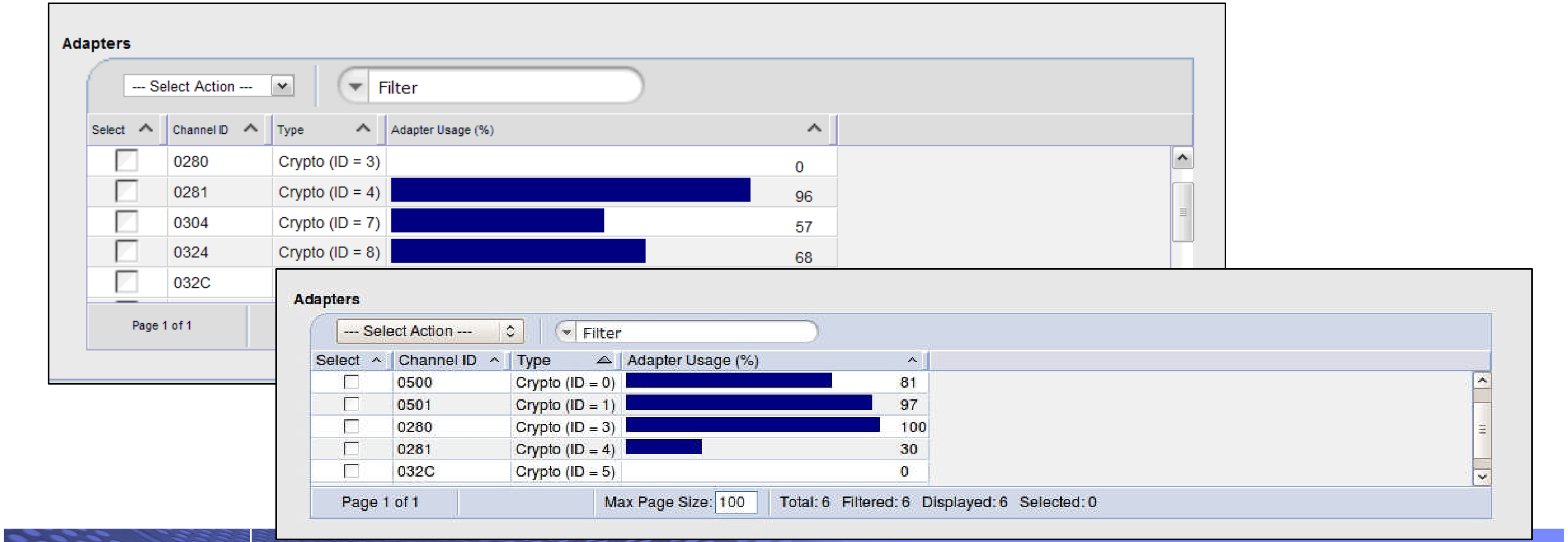
Select	Channel ID	Type	Adapter Usage (%)
□	0280	Crypto (ID = 3)	
□	0281	Crypto (ID = 4)	65
□	0304	Crypto (ID = 7)	
□	0324	Crypto (ID = 8)	28
□	032C	Crypto (ID = 5)	
□	0334	Crypto (ID = 6)	0

Page 1 of 1 | Max Page Size: 100 | Total: 8 Filtered: 8 Displayed: 8 Selected: 0

zBX Blades

Monitor Dashboard support for crypto

- **Monitors Dashboard on the HMC and SE was enhanced with a new Adapters table for System zEC12**
- **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)**



Adapters

Select	Channel ID	Type	Adapter Usage (%)
□	0280	Crypto (ID = 3)	0
□	0281	Crypto (ID = 4)	96
□	0304	Crypto (ID = 7)	57
□	0324	Crypto (ID = 8)	68
□	032C		

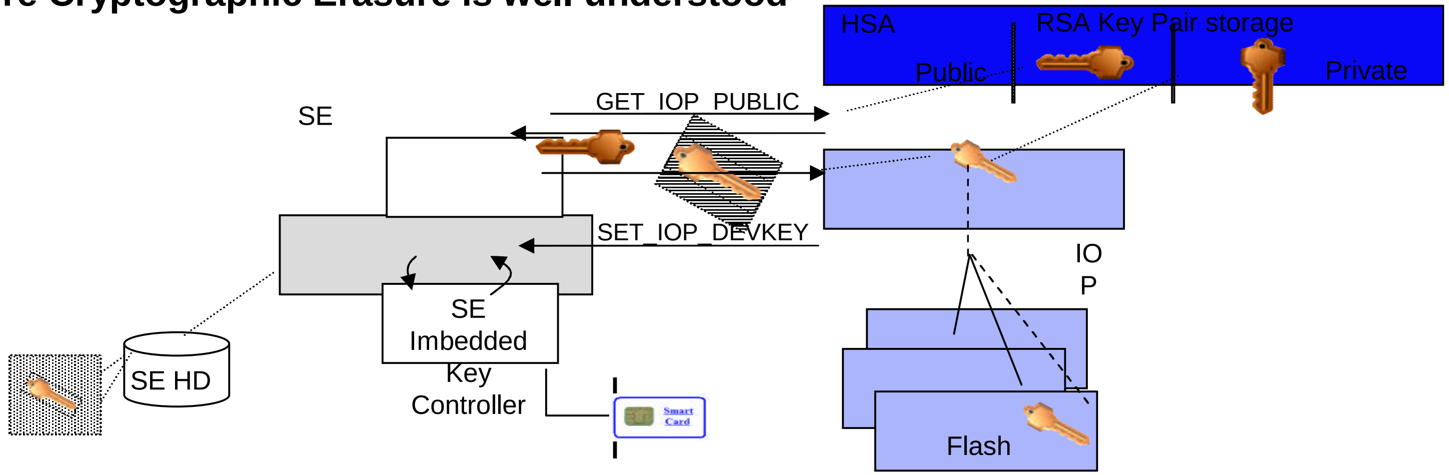
Adapters

Select	Channel ID	Type	Adapter Usage (%)
□	0500	Crypto (ID = 0)	81
□	0501	Crypto (ID = 1)	97
□	0280	Crypto (ID = 3)	100
□	0281	Crypto (ID = 4)	30
□	032C	Crypto (ID = 5)	0

Page 1 of 1 Max Page Size: 100 Total: 6 Filtered: 6 Displayed: 6 Selected: 0

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)

Questions

QR Code