IBM Americas, ATS, Washington Systems Center

# 10192 ICSF Update – Cryptographic Support On z114 and z196

Greg Boyd (boydg@us.ibm.com)
March 12, 2012
Atlanta, GA


Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

# Agenda

- **HCR7790**
  - Dynamic PKA Master Key Change
  - Coordinated KDS Administration
  - KDS Related Changes
  - Other Enhancements
  - Suite B
- **TKE 7.1**
- **HCR7770**
  - MSA-3 (Protected Key)
  - CEX3
- **HCR7780**
  - FIPS SPE
- **Toleration and Migration**
- **VM and Linux**

# Dynamic RSA-MK Change

| Prior to HCR7790 or without CEX3 on z196/z114 | HCR7790 with CEX3 on z196/z114 |
|---|---|
| **Generate key parts and calculate checksums** | **Generate key parts and calculate checksums** |
| **Disable PKA Services** | |
| **Load the RSA-MK parts** | **Load the RSA-MK parts** |
| **Reencipher the PKDS under the new master key** | **Reencipher the PKDS under the new master key** |
| **Activate the PKDS** | **Change the RSA-MK and activate the PKDS** |
| **Enable PKA Services** | |
| **Enable PKA read, write, create and delete access** | |
| **Change the ICSF Options data set to point to the new PKDS** | **Change the ICSF Options data set to point to the new PKDS** |

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

- **Problem:**
  - ICSF CKDS Administration involves many manual steps that require repeating when LPARs share a CKDS in a sysplex environment.
- **Solution:**
  - Provide a function that coordinates CKDS administration across members of a sysplex cluster (ICSF instances sharing the same active CKDS).
- **Benefits:**
  - 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 Master Key Management

```
CSFMKM10  ---------------------- ICSF – Master Key management ----------------------------
OPTION ===>
Enter the number of the desired option.
  1  INIT / REFRESH / UPDATE CKDS – Initialize a Cryptographic Key Data Set or
                                    activate an updated Cryptographic Key Data Set
  2  SET MK                       -- Set a master key (AES, DES, ECC)
  3  REENCIPHER CKDS              -- Reencipher the CKDS prior to changing a symmetric
                                     master key
  4  CHANGE SYM MK                -- Change a symmetric master key and activate the
                                     reenciphered CKDS
  5  INIT/REFRESH/UPDATE PKDS --  Initialize a Public Key Data Set or
                                     activate an updated Public Key Data Set or
                                     update the Public Key Data set header
  6  REENCIPHER PKDS              -- Reencipher the PKDS
  7  CHANGE ASYM MK               -- Change an asymmetric master key and activate the
                                     reenciphered PKDS
  8  COORDINATED KDS REFERESH – Perform a coordinated KDS refresh
  9  COORDINATED KDS CHANGE MK – Perform a coordinated KDS change master key

Press ENTER to go to the selected option.
Press END     to exit the previous menu.
```

# Select the KDS to Refresh

CSFCRC4P ---------- ICSF - Coordinated Refresh KDS Selection ----------

Select one Key Data Set type and press ENTER to continue.

==> / CKDS - Cryptographic Key Data Set

# Coordinated KDS Refresh

```
CSFCRC10 ------------------- ICSF – Coordinated KDS Refresh -------------------

COMMAND ===>

To perform a coordinated KDS refresh to a new KDS, enter the KDS names below
and optionally select the rename option. To perform a coordinated KDS refresh
of the active KDS, simply press enter without entering anything on this panel.

    KDS Type ===>          CKDS
  Active KDS ===>          'PLEX.TEST.CKDS'
    New KDS ===>

          Rename Active to Archived and New to Active (Y/N) ===> N

          Archived KDS ===>

Press ENTER to perform a coordinated KDS refresh.

Press END to exit to the previous menu.
```

# ICSF Master Key Management

```
CSFMKM10  ---------------------- ICSF – Master Key management ----------------------------
OPTION ===>

Enter the number of the desired option.

 1  INIT / REFRESH / UPDATE CKDS – Initialize a Cryptographic Key Data Set or
                                   activate an updated Cryptographic Key Data Set
 2  SET MK                      -- Set a master key (AES, DES, ECC)
 3  REENCIPHER CKDS             -- Reencipher the CKDS prior to changing a symmetric
                                   master key
 4  CHANGE SYM MK               -- Change a symmetric master key and activate the
                                   reenciphered CKDS
 5  INIT/REFRESH/UPDATE PKDS --  Initialize a Public Key Data Set or
                                   activate an updated Public Key Data Set or
                                   update the Public Key Data set header
 6  REENCIPHER PKDS             -- Reencipher the PKDS
 7  CHANGE ASYM MK              -- Change an asymmetric master key and activate the
                                   reenciphered PKDS
 8  COORDINATED KDS REFERESH – Perform a coordinated KDS refresh
 9  COORDINATED KDS CHANGE MK – Perform a coordinated KDS change master key

Press ENTER to go to the selected option.
Press END   to exit the previous menu.
```

# Select the KDS for the MK Change

CSFCRC4P ---------- ICSF - Coordinated Refresh KDS Selection ----------

Select one Key Data Set type and press ENTER to continue.

==> / CKDS - Cryptographic Key Data Set

# Coordinated KDS Change MK

```
CSFCRC20 ------------- ICSF – Coordinated KDS change master key ------------------
COMMAND ===>

To perform a coordinated KDS change master key, enter the KDS names below
and optionally select the rename option.

     KDS Type ===> CKDS
   Active KDS ===> 'PLEX.TEST.CKDS'
     New KDS ===>
           Rename Active to Archived and New to Active (Y/N) ===> N
           Archived KDS ===>
           Create a backup of the reenciphered KDS (Y/N) ===> N
           Backup KDS ===>

Press ENTER to perform a coordinated KDS refresh.
Press END to exit to the previous menu.
```

# Related Changes

- **New messages**

**CSFCM624I ICSF Communication Level Changed**

**CSFC0316 Reencipher Fail … for entry ckdslabel**

- **New healthcheck**

**ICSF_COPROCESSOR_STATE_NEGCHANGE**

**See TechDoc Flash10749 ‘Activation of Cryptographic Coprocessors and Cryptographic Algorithms with ICSF, HCR7780’**

# Coprocessor Management Panel

```
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
  -----------   ---------         ------    ---   ---   ----  ---
  __ G01          00000001        ONLINE    U     U     C     U
  __ G02          00000002        ACTIVE    A     U     A     E
  __ G03          00000003        ACTIVE    A     U     A     C
  __ E04          00000004        ACTIVE    A     U     -     C
  __ H05                          ACTIVE
```

# Other Enhancements

- **Additional ECC functionality**
  - ECC-DH
  - AES KEK for wrapping ECC private keys
- **Expanded AES key support**
  - AES KEK
  - Variable length AES keys (HMAC support)
- **Enhanced ANSI TR-31 interoperable secure key exchange**

# Other Enhancements

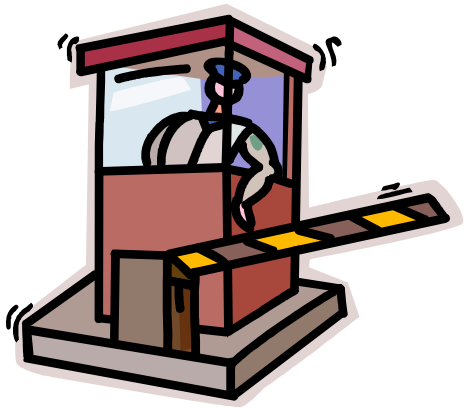
- **PIN Block Decimalization support**

  `0123456789ABCDEF`

  `0123456789012345`


- **PKA RSA OAEP with SHA-256 Algorithm**
- **Accelerator support for 2048 thru 4096-bit keys**

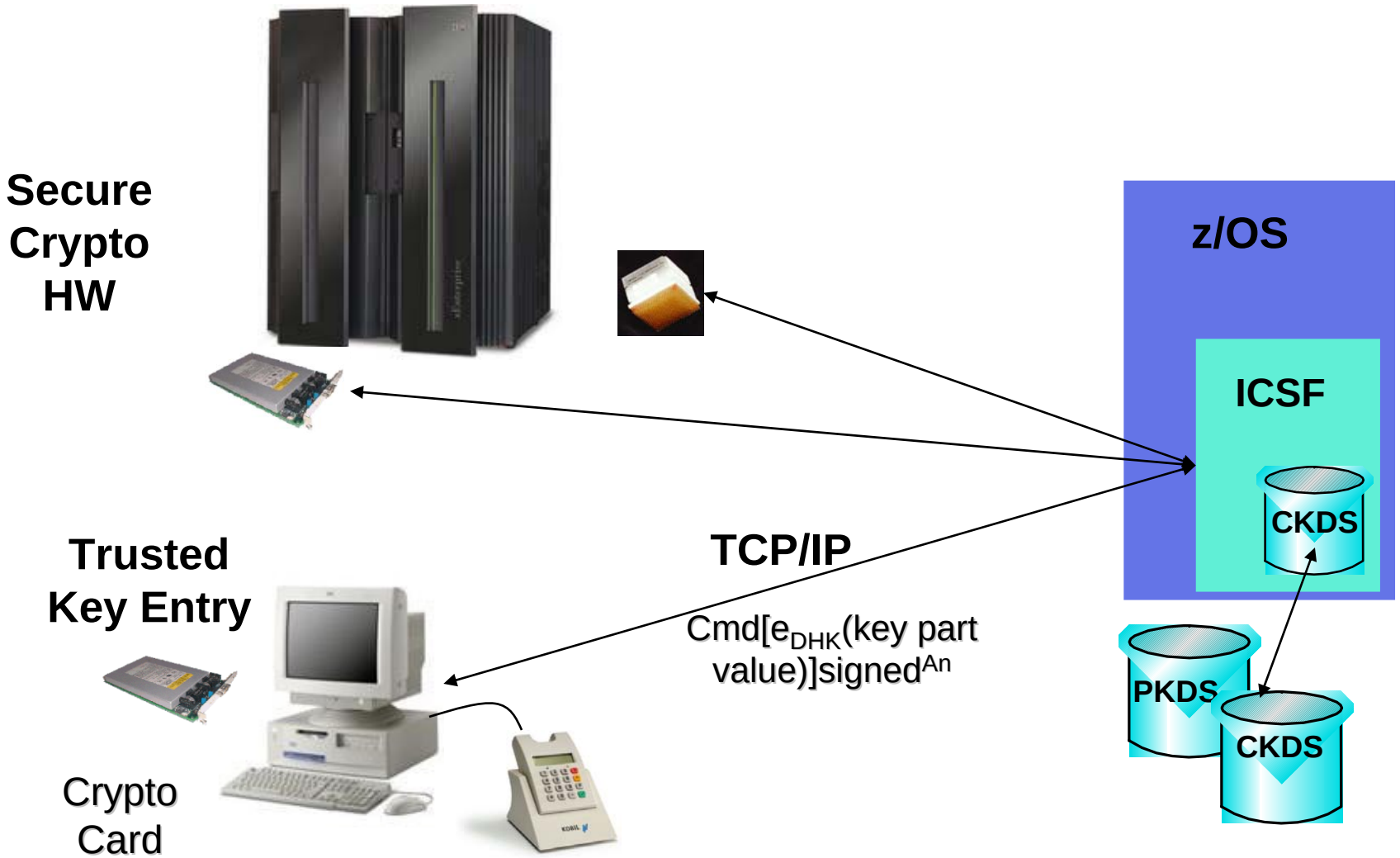
# Suite B



- **Symmetric Encryption**
  - AES w/key sizes of 128 and 256
- **Digital Signatures**
  - ECDSA – Elliptic Curve, Digital Signature Algorithm
- **Key Agreement**
  - ECDH – Elliptic Curve, Diffie Hellman
- **Message Digest**
  - SHA-2 (SHA-256 and SHA-384)

http://www.nsa.gov/ia/programs/suiteb_cryptography/

# TKE – Trusted Key Entry Workstation



# TKE 7.0 – New hardware platform

- **TKE 7.0 will run on a new hardware platform**
  - 4765 (CEX3) Crypto Card
  - Add USB ports; Drop serial ports
    - Old Kobil Smart Card readers used a serial port
    - New Omnikey Smart Card readers use the USB
    - Support USB Flash Memory Drive (as an alternative to the DVDRAM media)
  - New Smart Cards
    - JCOP41 NXP Smart Cards replacing the older Data Key Smart Cards
    - Six digit PINs

# TKE 7.0 - New Key Support

- **Support ECC Master Keys**
  - 32-byte AES Key to protect ECC Keys
  - Generation and loading of ECC keys not supported on TKE 7.0
- **CBC Key Wrapping**
  - KW-ENH Key Wrapping Enhanced
  - KW-ORIG Key Wrapping Original

# TKE 7.0 - Migration Wizard

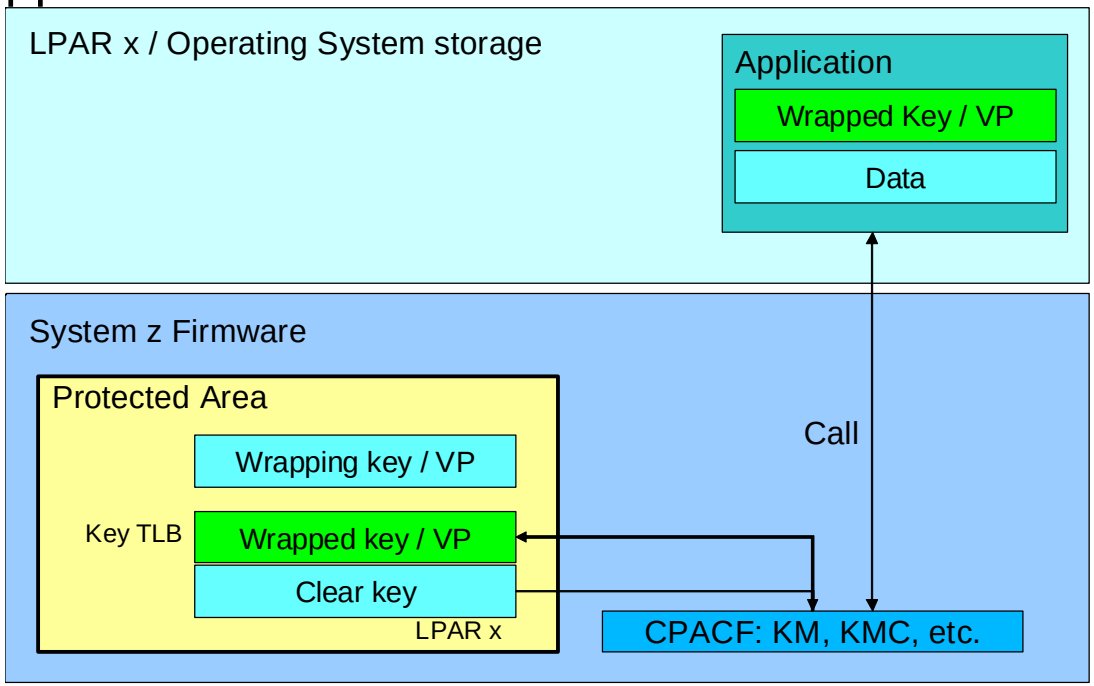
- **TKE 6.0 introduced a configuration migration utility to automate the process of replacing a host crypto adapter**
  - Captured public configuration data
    - Roles
    - Authorities
    - Domain Control Settings
    - Only ‘public’ (non-secret data), no key material
- **TKE 7.0 adds support for migration of key material**
  - Master Keys only
  - New Smart Card Types
    - Migration CA (MCA)
    - Injection Authority (IA)
    - Key Part Holder (KPH)

# TKE 7.1

- **AES operational key support**
- **Single process for loading an entire key**
- **Single process for generating multiple key parts**
- **Use of ECDH to exchange encrypted key material with a CEX3**
- **New access control points**
- **Migrate roles utility**
- **Support for more key parts on a smart card**
- **Host cryptographic module support**
- **Display of active IDs on the TKE console**

# HCR7770 – Protected Key

- **MSA-3 (Message Security Assist 3)**
  - Became available on the GA3 of the z10 EC/GA2 of the z10 BC
    - Protected Key Support



# Protected Key – How it works

- **Create a key, with the value 'ABCD' and store it as a secure key in the CKDS (i.e. encrypted under the Master Key, MK)**
  - $E_{MK}$(x'ABCD') => x'4A!2' written to the CKDS and stored with a label of MYKEY
- **Execute CSNBSYE (the clear key API to encrypt data), but pass it the key label of our secure key, MYKEY; and text to be encrypted of 'MY MSG  '**
  - CALL CSNBSYE(….,

    MYKEY,

    'MY MSG  ' ….)

# Protected Key – How it works (cont …)

- **ICSF will read MYKEY from the CKDS and pass the key value x'4A!2' to the CEX3**
- **Inside the CEX3, recover the original key value and then wrap it using the wrapping key**
  - $D_{MK}$(x' 4A!2') => x' ABCD'
  - $E_{WK}$(x'ABCD') => x'*94E'
- **ICSF will pass the wrapped key value of x'*94E' to the CPACF, along with the message to be encrypted**
- **In the CPACF, we'll retrieve the wrapping key, WK**
  - $D_{wk}$(x'*94E') => x'ABCD'
  - $E_{x'ABCD'}$('MY MSG  ') => ciphertext of x'81FF18019717D183'

# HCR7770 – ECC Support

- **Effective Key Size Security**

| Symmetric Key Size | RSA Key Size | ECC Key Size |
|---|---|---|
| 80 | 1024 | 163 |
| 112 | 2048 | 224 |
| 128 | 3072 | 256 |
| 192 | 7680 | 384 |
| 256 | 15360 | 512 |

**From NIST SP 800-57 Part 1 (Table 2) at www.nist.gov**

- **Elliptic Curve Support**
  - ECDSA
  - New ECC Master Key

- Point multiplication $Q=kP$
- Repeated point addition and doubling: $9P = 2(2(2P)) + P$
- Public key operation: $Q(x,y) = kP(x,y)$
  - $Q$ = public key
  - $P$ = base point (curve parameter)
  - $k$ = private key
  - $n$ = order of P
- Elliptic curve discrete logarithm
  Given public key kP, find private key k
- Best known attack: Pollard's rho method with running time: $\frac{(\pi n)^{1/2}}{2}$

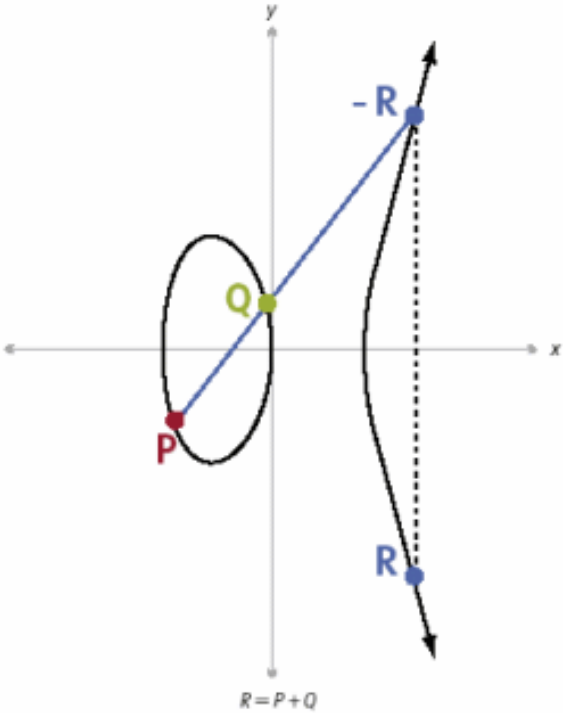


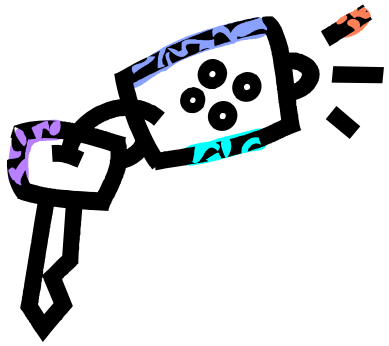

Image from DeviceForge and other sites

# ICSF – HCR7780

- **FIPS Mode SPE (OA32012/UA55967) for PKCS #11 – Public Key Cryptographic Token Interface**
  - PKCS #11 provides APIs for talking to devices which hold crypto info or perform crypto operations (think Smart Cards)
  - FIPSMODE was an option in HCR7770
  - SPE provides additional support required for FIPS certification
- **CKDS Constraint Relief**
  - CKT, in-storage copy of CKDS, above the bar
  - Optimized for speeding up searches (binary tree)
  - Limit performance impact of bulk updates
    - Buffering Read-Aheads
    - Tighten allocate / open / IO / close / deallocate process

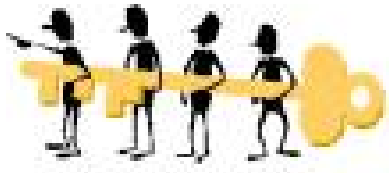
# FIPS-198 Keyed HMAC Support (OA33260)

- **New algorithm**
- **New Key/Token**
  - Variable-length key token
- **Variable Length CKDS (LRECL 1024)**
  - Fixed- and variable-length records
  - Conversion Utility – CSFCNV2
- **New callable services**
  - Key Management
  - HMAC Generate and Verify



# ICSF Versions supported on z196/z114

- **ICSF FMIDs**
  - HCR7790 (www.ibm.com/systems/z/os/zos/downloads)
  - HCR7780 (z/OS V1.13)
  - HCR7770 (z/OS V1.12)
  - HCR7751 (z/OS V1.11)
  - HCR7750 (z/OS V1.10)
  - HCR7740 (z/OS V1.9 with IBM Lifecycle Extension with PTFs)
  - HCR7731 (z/OS V1.8 with IBM Lifecycle Extension with PTFs)
  - HCR7731 (z/OS V1.7 with IBM Lifecycle Extension with PTFs)*



**(*note that z/OS V1.7 included HCR7720, but HCR7720 will not support the z196, you must have upgraded to HCR7731 or later on your z/OS 1.7 system)**

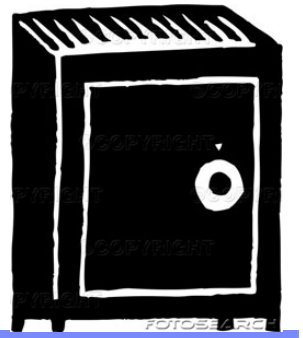
# Crypto Express3 Support

- **Crypto Express3 Toleration APARs**
  - ICSF OA29839
  - RMF OA28670
  - SAF OA29194
  - RACF OA29193

# ICSF Toleration

- **HCR7780 - Toleration APAR OA33320**
  - CBC Key Wrapping – 'Enhanced' key wrapping
  - ECDSA Keys in the PKDS
- **HCR7780 - HMAC Toleration Support OA34402**
  - Old versions of ICSF (HCR7750, HCR7751, HCR77770) will ignore XCF messages with a longer format coming from HCR7780 systems
- **HCR7790 - Variable Length AES OA36718**
  - HCR7780 can tolerate the new AES keys

See SMPE Support for ICSF FIXCAT ICSF790C/K



# z/VM 5.4 and z/VM 6.1

- **Provides guest support, VM does not directly use the crypto hardware**
  - Crypto Express3 - VM64656
  - Protected Key Support - VM64793

# Linux on System z

- **CPACF**
  - MSA-4 support in a future distribution
- **CEX3**
  - Drivers in SUSE SLES11 SP1/SLES12 andd RedHat RHEL 6.0 provide exploitation support for the CEX3
  - Drivers in SUSE SLES10 SP3 and SLES11 and Red Hat RHEL 5.4 provide toleration support (CEX3 acts like a CEX2)
  - CCA (secure key support) software download at the CryptoCards website (http://www.ibm.com/security/cryptocards/?S_TACT=107AG01W&S_CMP=campaign)

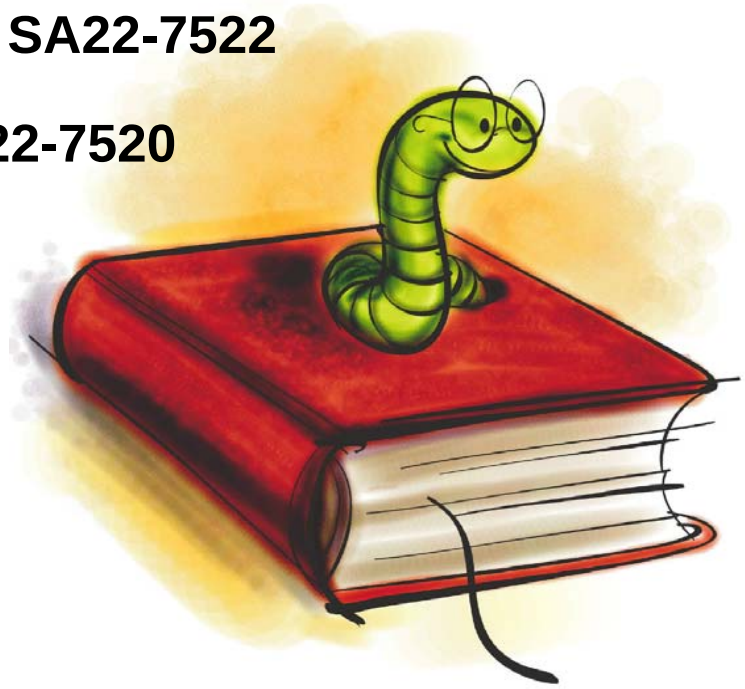
# Summary

- **z196 and z114 continues the implementation and support of new crypto technology, techniques and standards to support the evolving world of data security**

# References

## IBM Pubs

- **ICSF Overview, SA22-7519**
- **ICSF Administrator's Guide, SA22-7521**
- **ICSF Application Programmer's Guide, SA22-7522**
- **ICSF System Programmer's Guide, SA22-7520**



## TechDocs

- **www.ibm.com/support/techdocs**

  and search on 'crypto'

# Trademarks

**The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.**

| | | | |
|---|---|---|---|
| AlphaBlox* | GDPS* | RACF* | Tivoli* |
| APPN* | HiperSockets | Redbooks* | Tivoli Storage Manager |
| CICS* | HyperSwap | Resource Link | TotalStorage* |
| CICS/VSE* | IBM* | RETAIN* | VSE/ESA |
| Cool Blue | IBM eServer | REXX | VTAM* |
| DB2* | IBM logo* | RMF | WebSphere* |
| DFSMS | IMS | S/390* | zEnterprise |
| DFSMShsm | Language Environment* | Scalable Architecture for Financial Reporting | xSeries* |
| DFSMSrmm | Lotus* | Sysplex Timer* | z9* |
| DirMaint | Large System Performance Reference™ (LSPR™) | Systems Director Active Energy Manager | z10 |
| DRDA* | Multiprise* | System/370 | z10 BC |
| DS6000 | MVS | System p* | z10 EC |
| DS8000 | OMEGAMON* | System Storage | z/Architecture* |
| ECKD | Parallel Sysplex* | System x* | z/OS* |
| ESCON* | Performance Toolkit for VM | System z | z/VM* |
| FICON* | PowerPC* | System z9* | z/VSE |
| FlashCopy* | PR/SM | System z10 | zSeries* |
| * Registered trademarks of IBM Corporation | Processor Resource/Systems Manager | | |

**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 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.