IBM Advanced Technical Support , Washington Systems Center

ICSF (HCR7780) and Crypto on zEnterprise Update

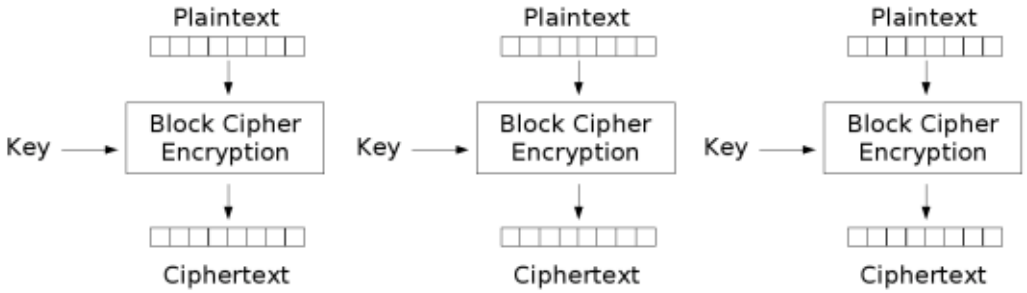
Greg Boyd (boydg@us.ibm.com)
June 2011

Agenda

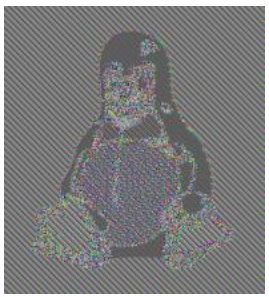
- **zEnterprise 196 Hardware**
  - CPACF
  - CEX3
- **ICSF**
  - HCR7780
  - FIPS SPE
  - Toleration and Migration
- **VM and Linux**
- **TKE 7.0**

z196 Hardware - CPACF

- **MSA-4 (Message Security Assist 4)**
  - New instructions for additional chaining options (CFB, OFB, Counter Modes)
  - New option for existing instructions (XTS-AES)



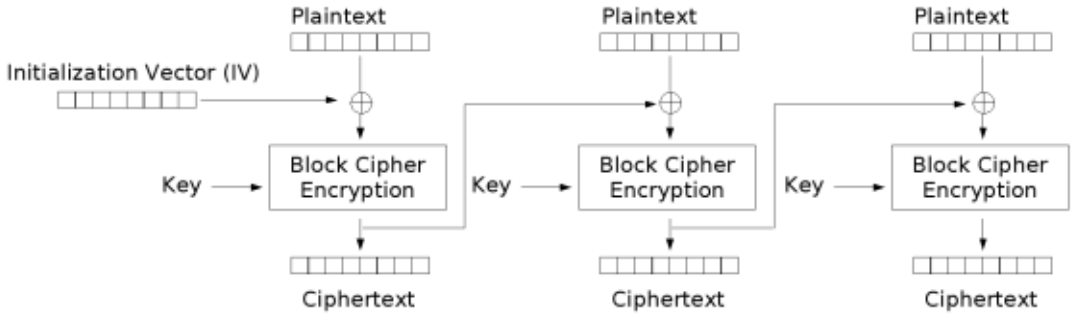
Electronic Codebook (ECB) mode encryption



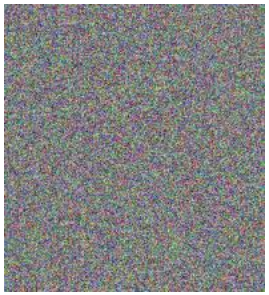
Images from Wikipedia

z196 Hardware - CPACF

- **MSA-4 (Message Security Assist 4)**
  - New instructions for additional chaining options (CFB, OFB, Counter Modes)
  - New option for existing instructions (XTS-AES)



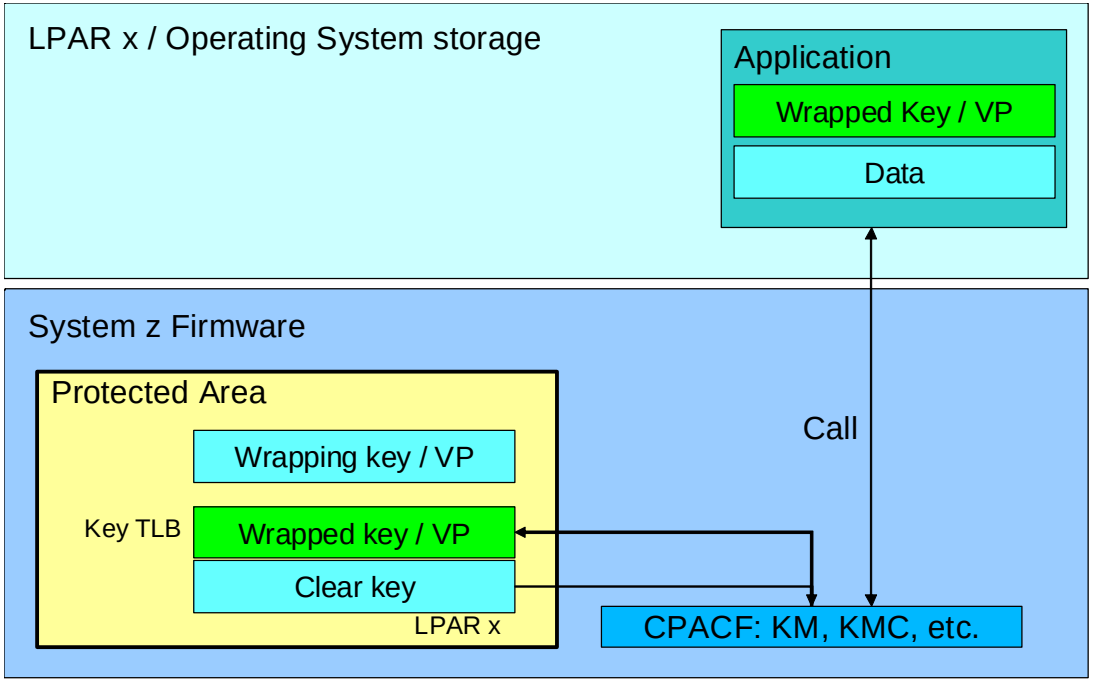
Cipher Block Chaining (CBC) mode encryption



Images from Wikipedia

z196 Hardware - CPACF

- **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,

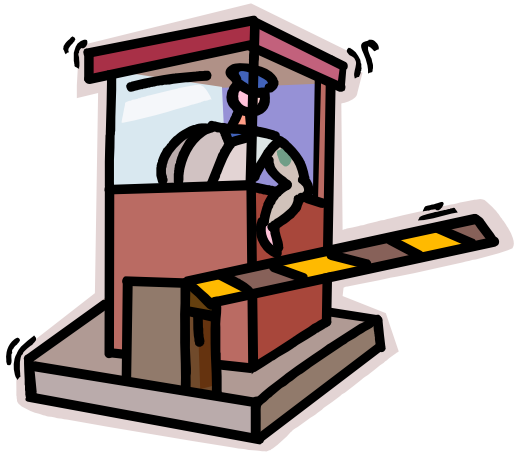
    'MY MSG ' ….)

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'

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/

z196 Hardware – CEX3

- **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: $\frac{(\pi n)^{1/2}}{2}$

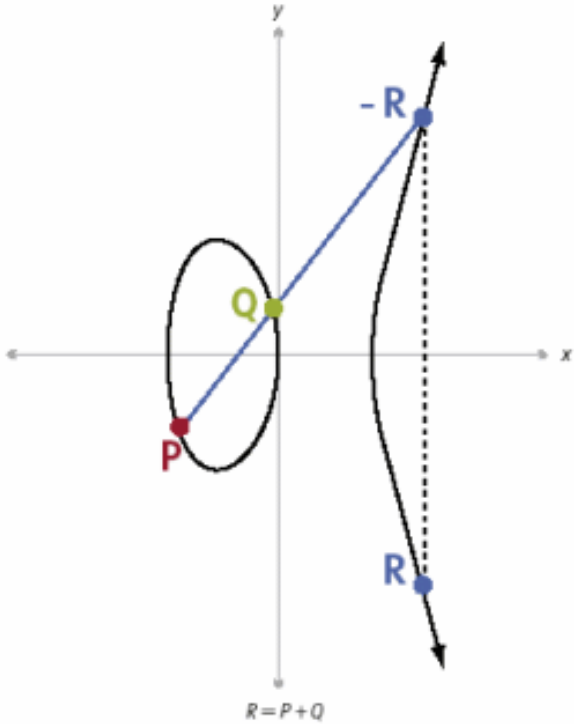


Image from DeviceForge and other sites

z196 Hardware – CEX3

- **CEX3**
  - –ANSI X9.8 (PIN Processing)
  - –ANSI X9.24 (CBC Key Wrapping)
  - –HMAC (w/APAR OA33260 in 1Q2011)
  - –Concurrent Patch Apply (CPA) / Concurrent Driver Upgrade (CDU)
  - –Thin Interrupts

    (aka CEX3 Interrupts)

ICSF – HCR7780

- **MSA-4, MSA-3**
- **Elliptic Curve Support**
  - –New 256-bit ECC Master Key
- **ANSI X9.8 PIN**
- **ANSI X9.24 (CBC Key Wrapping)**
  - –Original vs Enhanced
- **HMAC – variable length keys**
- **TKE 7.0**
- **ICSF Options**
  - –BEGIN(FMID)
  - –END

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
```

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

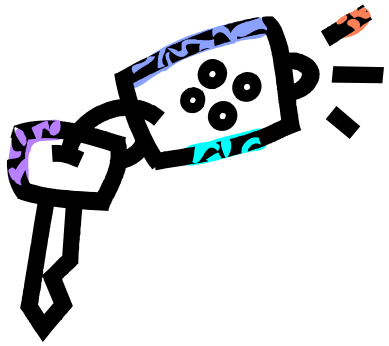
- **JSSE2 use of IBMPKCS11Impl**

ICSF – HCR7780

- **PCI Audit**
  - Several current subtypes will have additional info
    - RACF Userid
    - Connect Group
    - Certificate Issuer's Distinguished Name
    - Certificate Subject's Distinguished Name
    - Registry that authenticated the user
    - Jobname, Job Entry Date & Time
    - Terminal ID
    - Security Label
    - User-defined Identification Field
  - New SMF Type 82 Subtype 29 (TKE Offload)
- **AMODE 64 Support**

FIPS-198 Keyed HMAC Support (OA33260)

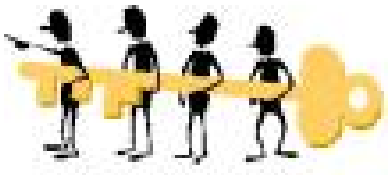
- **New algorithm**
- **New key/token**
  - Variable-length key token
- **Variable Length CKDS (LRECL 1024)**
  - Fixed- and variable-length records
  - Conversion Utility – CSFCNV2
- **New callable services**
  - Key Management
  - HMAC Generate and Verify



ICSF Versions supported on z196

- **ICSF FMIDs**
  - HCR7780 (www.ibm.com/systems/z/os/zos/downloads)
  - 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)

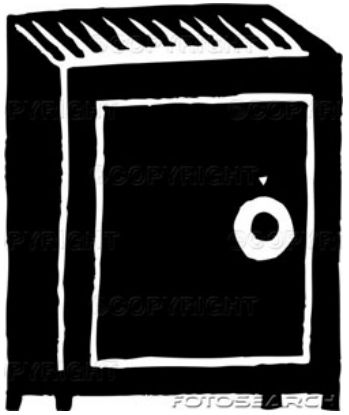


Crypto Express3 Support

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

ICSF Toleration

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



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
  - MSA-3 support in SUSE SLES10 SP3, SLES11 and RHEL 5.4
- **CEX3**
  - Drivers in SUSE SLES11 SP1 and SLES10 SP4 and RHEL 6.0 or later provide exploitation support for the CEX3
  - Drivers in SUSE SLES10 SP3 and SLES11 and 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)

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 7.0 - Audit Offload

- **Payment Card Industry Data Security Standards (PCI-DSS) driving new requirements**
  - With TKE 5.3 we provided additional logging for security-relevant events on the TKE
  - These records can be written to the DVD for post processing
- **With TKE 7.0 we'll support sending those records to a specified z/OS Host, using SMF**

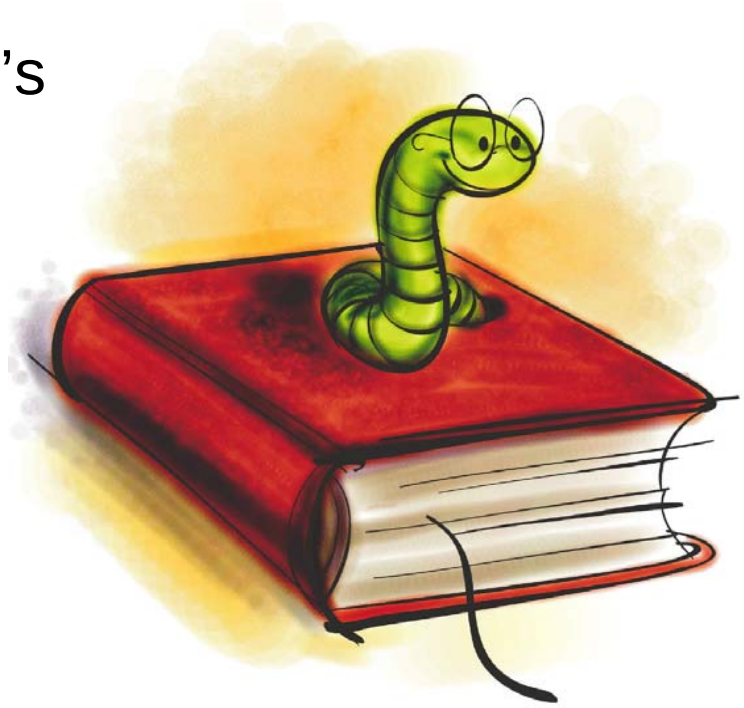
Summary

- **z196 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, 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:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

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.