IBM z13s and HCR77B1

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

Copyrights . . .

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 12 years

. . . And Trademarks

- Copyright © 2016 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

Agenda – IBM z13s and HCR77B1

- Hardware z13s (and z13)
  - CPACF
  - CEX5S (4767 Crypto processor)
- ICSF
  - HCR77B1
  - HCR77B0
- TKE 8.x

IBM z13s (Announcement Letter 116-002)

- Trusted, secure, and reliable operations for reduced business risk
  - Stronger and faster protection with integrity of data across a hybrid cloud environment with the new Crypto Express5S.
  - Enhanced public key support for constrained digital environments using cryptography for users of applications such as Google Chrome, Mozilla Firefox, and Apple iMessage, enhancing your cyber security.
  - Ability to minimize reformatting of databases with new exploitation of Visa Format Preserving Encryption (FPE) for payment processing.

The z13s (and z13)

- Simultaneous Multithreading
- CP Assist for Cryptographic Function
  - Message Security Assist-5 (MSA-5)
    - PPNO – Perform PseudoRandom Number Operation
  - Improved performance
    - TDES & AES – ~~2x~~ 2.3x faster than zEC12
    - ~~SHA512 – 3.5x faster than zEC12~~ Hashing - 3.9 x faster

Crypto Express5S – FC #0890

- New coprocessor chip the 4767
- More domains
  - 85 on the z13
  - 40 on the z13s
  - 256 per the 'Changes section' of the SPG
- Still a limit of 16 crypto engines per CEC
- Better performance in all 3 configurations (coprocessor, accelerator, PKCS #11 mode)
- HSM designed to meet
  - FIPS 140-2 level 4 (116-034, 4/26/16 announcement says already in process)
  - ANSI X9.97
  - Deutsche Kreditwirtschaft (DK)
  - PCI HSM

- Crypto Express4S – not supported on the z13 or z13s

4767 (PCIeCC2) Enhancements

- Increased performance
- Hardware accelerated Elliptic Curve Cryptography (ECC) key generation, along with digital signature generation and verification using the Elliptic Curve Digital Signature Algorithm (ECDSA).
- Enhanced firmware load security using ECDSA signatures
- Support for Visa Data Secure Platform with Point to Point Encryption (VDSP with P2PE), which includes Visa Format-Preserving Encryption (FPE)
- The ability to encipher and decipher data using the AES algorithm in Galois/Counter Mode (GCM).
- The creation of symmetric key material from a pair of Elliptic Curve Cryptography (ECC) keys using the Elliptic Curve Diffie-Hellman (ECDH) protocol and the ANSI-9.63-KDF key derivation method as specified in ANSI X9.63-2011.
- Newly selectable RSA public exponents 5, 17, and 257. This addition completes the series of the first five Fermat numbers.

Cryptographic Support for z/OS V1R13 – z/OS V2R2 (HCR77B1)

- New operator commands
- OA46466 – CCA support for German Banking Industry (DK) defined PIN processing functions
- OA47016 – new ICSF callable services to simplify EMV payment processing (MCL required)
- OA47781 –
  - CCA support for generation of single key for certain key types
  - Support for RSA-OAEP block formatting for SHA-1 and SHA-256, consistent with RSA PKCS #1 v2.0 (MCL required)

Open Cryptographic Server

- Stand-alone devices that perform geography specific cryptography
  - Chinese SMx family of algorithms
  - IP connected
  - zEC12/zBC12 or later & HCR77B1

  - Open Cryptographic Server Master Key - OCS-MK
    - TKDS Header +x'84'
    - Managed by vendor utility, not ICSF

ICSF Options Changes (HCR77B1)

- REMOTEDEVICE(index,IP address, port #, # sockets)
- MASTERKCVLEN(2,3,4,5,6,ALL)

- HDRDATE (Deprecated)

Display ICSF Command

- LIST (members of sysplex)
- CARDS (coprocessors)
- KDS (active keystores)
- MKS (master key info, for each card)
- OPTIONS (FMID, KDS ref date interval & period, MK VP digits)
- REMOTEdevice (network attached open cryptographic servers)

secured by MVS.DISPLAY.ICSF profile

SETICSF Command

- Remotedevice
  - ACTivate (Index, Serial Number, Remote Device)
  - DEACTivate (Index, Serial Number, Remote Device)
  - RESTART (Index, Serial Number, Remote Device)
  - CHECK (Remote Device)
  - DELETE (Remote Device)
- Keystore (CKDS, PKDS, TKDS)
  - ENable
  - DISable
- Options (MKCVLEN, RISEC, RIPER)

secured by MVS.SETICSF profile

Enhanced Cryptographic Support for z/OS V1R13 – z/OS V2R1 (HCR77B0)

- IBM z13
- Crypto Express5s
- Visa Format Preserving Encryption (VFPE)
- Enhanced Random Number Generation
- Ability to disable the RNG cache
- Support for key archiving and key material validity

Format Preserving Encryption

- From Wikipedia:

In cryptography, **format-preserving encryption** (FPE) refers to encrypting in such a way that the output (the ciphertext) is in the same format as the input (the plaintext). The meaning of "format" varies. Typically only finite domains are discussed, for example:

  - To encrypt a 16-digit credit card number so that the ciphertext is another 16-digit number.
  - To encrypt an English word so that the ciphertext is another English word.
  - To encrypt an n-bit number so that the ciphertext is another n-bit number.

- For example:
  - SSN – 9-digit number
  - PAN (Credit Card Number) bbbbbb nnnnnnnn c

Format Preserving Encryption Card APIs

- New APIs
  - FPE Decipher (CSNBFPED/CSNEFPED) – Decrypts payment card data using Visa Data Secure Platform (VISA DSP) processing
  - FPE Encipher (CSNBFPEE/CSNEFPEE) – Encrypts payment card data using Visa Data Secure Platform (VISA DSP) processing
  - FPE Translate (CSNBFPET/CSNEFPET) – Translate payment card data from encryption under one key to encryption under another key using Visa Data Secure Platform (VISA DSP) processing
  - In a single call
    - PAN
    - Card Holder Name
    - Discretionary Track 1
    - Discretionary Track 2
    - ASCII/Binary
  - Secure Key TDES

Format Preserving Encryption APIs

- Field Level Decipher (CSNBFLD/CSNEFLD) – Encrypts payment related database fields, preserving the format of the fields using the Visa Format Preserving Encryption algorithm
- Field Level Encipher (CSNBFLE/CSNEFLE) – Encrypts payment related database fields, preserving the format of the fields using the Visa Format Preserving Encryption algorithm

- In a single call
  - Data
  - Charset: ASCII, Printable ASCII, EBCDIC, Printable EBCDIC, Ordinal
  - Secure Key, Clear Key, Protected Key
  - TDES or AES

VFPE Questions

- Visa Merchant Data Secure with Point to Point Encryption
- IBM Announcement Letter 115-170, Dec. 15, 2015
  - Clients who wish to use the FPE functionality of IBM z Systems cryptography features must first enter into a separate agreement with Visa for use of this advanced technology.
- NIST SP 800-38G 'Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption'
  - No mention of Visa FPE mode

Key Material Archiving/Validity

- KDSR format introduced in HCR77A0
- HCR77B0 – additional metadata
  - Dates: Creation/Update, Validity, Last Used Reference, Archive
  - Flags: Archive/Prohibit Archive
  - IBM & installation metadata blocks

Validity Dates and Archiving

- Validity Date – Start and End
  - Key material can't be used before the start date
  - Key material can't be used after the end date
  - SMF Type 82 is generated
- Archive
  - Archive Flag/Prohibit Archive Flag
  - RACF XFACILIT CSF.KDS.KEY.ARCHIVE.USE

    RDEFINE XFACILIT CSF.KDS.KEY.ARCHIVE.USE

    SETROPTS RACLIST(XFACILIT) REFRESH
  - SMF Type 82 records updated to record archives/recalls
  - KEYARCHMSG(YES/NO)

New ICSF Start-up Options

- KEYARCHMSG (YES or NO)
  - YES ICSF issues a message the first time an archived record is referenced by an application
  - NO ICSF does not issue a message when an archived record is referenced by an application
- RNGCACHE(YES or NO)
  - YES Maintain a cache of random numbers
  - NO Don't maintain a cache of random numbers
- Both of these show up on the ICSF Installation Options panel as well

ICSF Coprocessor Management Panel

CSFCMGP00 ---------- ICSF Coprocessor Management ---------- Row 1 to 2 of 2
Command =>

Select the cryptographic features to be processed and press ENTER.
Action characters are: A, D, E, K, R, and S. See the help panel for details

CRYPTO FEATURE	SERIAL NUMBER	STATUS	AES	DES	ECC	RSA	P11
. 5C00	16BA6173	Active	I	A	A	A	
. 5A01	N/A	Active					
. 5C02	16BA6175	Master key incorrect	I	A	C	E	
. 5A03	N/A	Active					
. 5P04	162C9378	Active					A

CICS Note!

- Add

```
//DFHRPL DD DISP=SHR,DSN=xxxxx.SDFHLOAD
//   DD DISP=SHR,DSN=yyy.SCSFMOD0 (ICSF callable service stubs)
//   DD DISP=SHR,DSN=yyy.SIEALNKE (ICSF shared libraries)
//   DD ...
...
//SYSIN DD DISP=SHR,DSN=xxxxx.SYSIN(DFH$SIPx)
```

ICSF – CEX5S Toleration

- OA45547 (HCR77A1/UA76042, HCR77A0/UA76041, HCR7790/UA76044, HCR7780/UA76043)
  - Older versions of ICSF don't know what a CEX5S is. This APAR will let them recognize a CEX5S as either a CEX4S or CEX3. (Coprocessor, Accelerator or PKCS #11 mode)
- OA39075 (HCR7780/UA90636, HCR7790/UA90637)
  - Toleration support for CEX4S (these versions of ICSF don't recognize CEX4S or CEX5S, so with this APAR, they'll be treated like a CEX3

ICSF Coexistence

- OA42014 (HCR7780/UA70712, HCR7790/UA70713, HCR77A0/UA70710)
  - HCR77A1 introduced a common keystore record format and new keytype, DESUSECV
- OA39484 (HCR7780/UA90639, HCR7790/UA90640)
  - HCR77A0 introduced new key wrapping support for ECC private key tokens wrapped with ECC-MK; PKCS #11 secure keys in the TKDS
- OA36718 (HCR7780/UA62059)
  - HCR7790 introduced variable length CKDS keys support

TKE 8.x Features

- TKE 8.0 LIC (FC #0877) / TKE 8.1 LIC (FC #0878)
- TKE workstation (FC #0847)
- 4767 TKE Crypto Adapter (FC #0894)
- TKE Smart Card Reader (FC #0891)
- TKE additional smart cards (FC #0892)

TKE 8.x Hardware Connectivity

- z13
- zEC12/zBC12

Crypto Cards Managed by TKE 8.x

- CEX2 Coprocessor
- CEX3 Coprocessor
- CEX4S CCA or PKCS #11 Coprocessor
- CEX5S CCA or PKCS #11 Coprocessor

TKE 8.0 LIC

- CEX5S support
  - Migration support (collect data from your CEX4S and apply it to your CEX5S)
- Support > 16 crypto domains
- FIPS Certified Smart Cards Part Num 00JA710
- Full function migration wizard for EP11
- New master key management functions
  - Wizard to generate set of master key parts for each different type of Master Key (DES, AES, RSA, ECC, P11)
  - Wizard to load new master key parts for each different type of Master Key (DES, AES, RSA, ECC, P11)

TKE 8.0 LIC (cont.)

- Smart Card Readers Available indicator
- Configure Displayed Hash Size
- ENC-Zero Support for 24-byte DES-MK
- ECC Authority Signature Keys
- Print Capability (drivers from GUTENPRINT or HPLIP)
- Crypto Node Management (CNM) Utility to load and save user profiles
- Usability Enhancements

TKE 8.1 LIC

- Domain cloning
- Launch coordinated master key change
- Guided create features for roles & authority indexes
- Two new Certificate Authority wizards (for creating smart cards)
- Display crypto module settings
- Support for loading HMAC keys
- Save/Restore customized data feature
- Password protect console
- Binary key part file utility
- ACP usage info utility
- Require enhanced host password protection
- Operational key option on domain groups

Other OS

- z13/z13s requires at a minimum:
  - z/VM V6.4
  - z/VM V6.3 with PTFs (CEX5S, and enhanced crypto domain support for CEX4S and CEX5S, Regional Crypto Enablement Adapters)
  - z/VM V6.2 with PTFs (Compatibility, CEX5S, and enhanced crypto domain support for CEX4S and CEX5S , Regional Crypto Enablement Adapters)
  - z/VSE 6.1
  - z/VSE 5.1 with PTFs
  - z/VSE 5.2 with PTFs
  - z/TPF V1.1 with PTFs
  - KVM for IBM z Systems V1.1.1
  - Linux on z Systems:
    - SLES 12 and SLES 11 SP3
    - RHEL 7.1 and RHEL 6.6

Other OS

- CEX5S (#0890) support of VISA FPE requires at a minimum:
  - z/VM 6.2 with PTFs for guest exploitation
- CEX5S (#0890) support of > 16 domains requires at a minimum:
  - z/VM V6.2 with PTFs for guest exploitation
  - z/VSE V5.2 with PTFs
  - z/VSE V5.1 with PTFs
  - Linux on z Systems: IBM is working with partners to provide
    - SUSE Linux Enterprise (SLES) for System z: SLES 12 and SLES 11
    - Red Hat Enterprise Linux (RHEL) for System z: RHEL 7 and RHEL 6

Reference Materials

- Announcement Letters
  - 116-002, Feb. 16, 2016 — The IBM z13s
  - 116-034, April 26, 2016 — 4767 PCIe Crypto Coprocessor
  - 115-001, Jan. 14, 2015 — The IBM z13
  - 115-055, March 3, 2015 — Revised Availability: The IBM z13
  - 215-006, Jan. 14, 2015 — Preview: IBM z/OS Version 2 Release 2 – Fueling the new digital enterprise
- Redbooks www.ibm.com/
  - SG24-8294 IBM z13s Technical Guide
  - SG24-8250 IBM z13 and IBM z13s Technical Introduction
  - SG24-8260 IBM z13 Configuration Setup
  - SG24-8251 IBM z13 Technical Guide
  - TIPS-1257 Ultimate Security with the IBM z13
- Seattle Share presentations by Harv Emery & John Eells

z13 Performance

- 'IBM z13 Performance of Cryptographic Operations' (http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSW03283USEN or just Google the title

- Some pretty dramatic numbers for Java at

http://mainframeinsights.com/java-performance-ibm-z-systems-ibm-z13-ibm-java-sdk-8/

Questions?