Unscrambling the Complexity of Crypto!

Crypto Update (Crypto, z15, ICSF/HCR77D1 and the TKE)

Greg Boyd

gregboyd@mainframecrypto.com

November 2019

. . . And Trademarks

- Copyright © 2019 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

- General Crypto News
- IBM z15 & CEX7S
- ICSF – HCR77D1
- TKE 9.2
- Other ‘stuff’

FIPS 140-3

- Will replace FIPS 140-2

• March 22, 2019	Approval Date
• September 22, 2019	Effective Date
• CMVP Program Updates complete	March 22, 2020
• FIPS 140-3 Testing Begins	September 22, 2020
• FIPS 140-2 Testing Ends	September 22, 2021

- This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information
- Aligns with ISO/IEC 19790:2012(E) ‘Information technology – Security Techniques – Security requirements for cryptographic modules’ (https://csrc.nist.gov/publications/detail/fips/140/3/final)
- To conform, crypto modules must use approved security functions (crypto algorithms, crypto key management techniques and authentication techniques)

FIPS 140-3 Levels

- Levels 1 thru 4
  - Cryptographic Module Specification
  - Cryptographic Module Interfaces
  - Roles, Services and Authentication
  - Software / Firmware Security
  - Operational Environment
  - Physical Security
  - Non-Invasive Security
  - Security Parameter Management
  - Self-Tests

DES/TDES

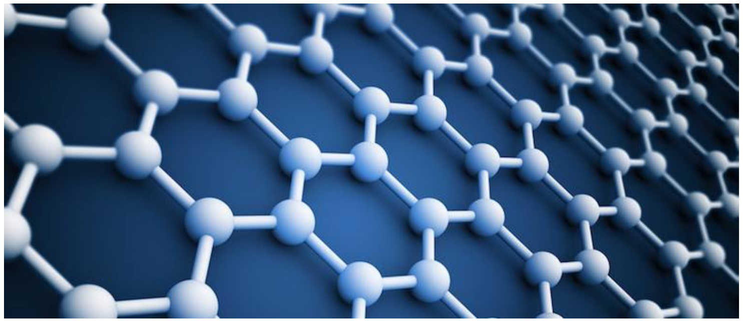
- ‘Transitioning the Use of Cryptographic Algorithms and Key Lengths’ NIST Special Publication 800-131A Revision 2, March 2019 (p. 7)

Algorithm	Status
Two-key TDEA Encryption	Disallowed
Two-key TDEA Decryption	Legacy Use
Three-key TDEA Encryption	Deprecated thru 2023 Disallowed after 2023
Three-key TDEA Decryption	Legacy Use
AES-128 Encryption and Decryption	Acceptable
AES-192 Encryption and Decryption	Acceptable
AES-256 Encryption and Decryption	Acceptable

Table 1 - Approval Status of Symmetric Algorithms Used for Encryption and Decryption

Quantum Safe

- Asymmetric algorithms are susceptible to attacks from quantum computers using Shor's algorithm
- Symmetric algorithms not susceptible
- NIST
  - Dec. 2016 - Call for public to submit post-quantum algorithms
  - Jan. 2019 – 26 submissions made it to round 2
  - Expected to run on large computers, smart phones, small computers (that make up the IOT)
  - Proposed solutions use lattices, code-based, multivariate or a few miscellaneous types



Crystals - Dilithium

- Crystals – Cryptographic Suite for Algebraic Lattices
- A lattice of numbers
  - Start with a list of 5 numbers
  - Add 3 of them together
  - Give you that sum
  - Can you figure out which 5 numbers I used?
- What if the list had a thousand numbers, each with thousands of digits and you have to pick 500?

z15 Announcement Letter ENUS119-027

- z15
  - CPACF improvements – Message-Security-Assist extension 9
  - Crypto Express7S
  - New release of ICSF, Cryptographic Support for V2R2-V2R4, aka HCR77D1
  - IBM Integrated Accelerator for zEnterprise Data Compression (DEFLATE Instruction)
  - Data Privacy for Diagnostics
    - Capability of 'tagging' sensitive data
    - Secure/Redact before sending the dump

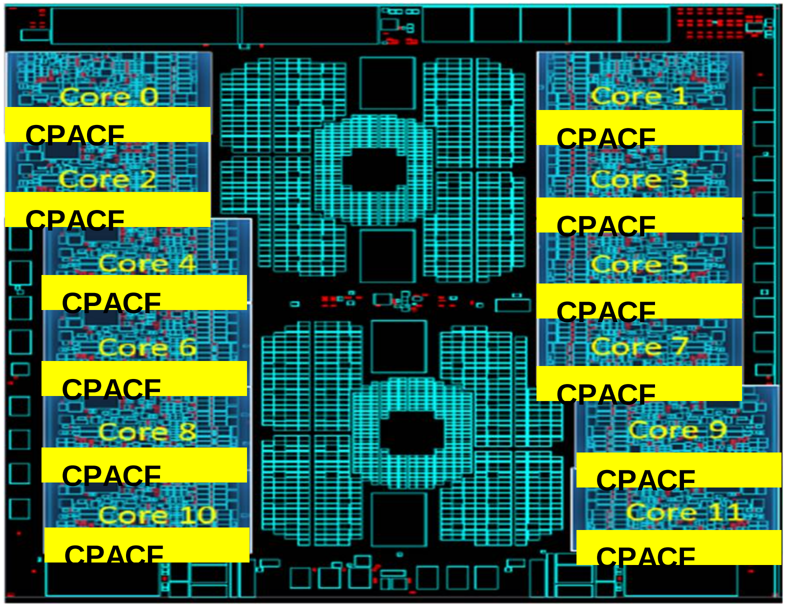
Other IBM Announcements

- 219-552 Revised availability: Support for sequential basic format and large format SMS-managed data sets in IBM z/OS Version 2 Release 4
  - APAR OA56622 is slipping from 1Q20 to 3Q20
- 219-452 IBM Data Privacy Passports V1.0 beta program delivers enhanced data protection and privacy for IBM z15 and LinuxONE III clients
  - Extends data protection beyond IBM Z to protect data-at-rest and data-in-motion
  - Data privacy passport controller, provides a view of sensitive data, based on policy

z15 MSA Extension 9

- Compute Digital Signature Authentication (KDSA)
  - Support for signing and verification using Elliptic Curve keys
- Perform Cryptographic Computation (PCC) adds Elliptic Curve Scalar Multiply functionality
- Perform Cryptographic Key Management Operation (PCKMO) now wraps Elliptic Curve Keys

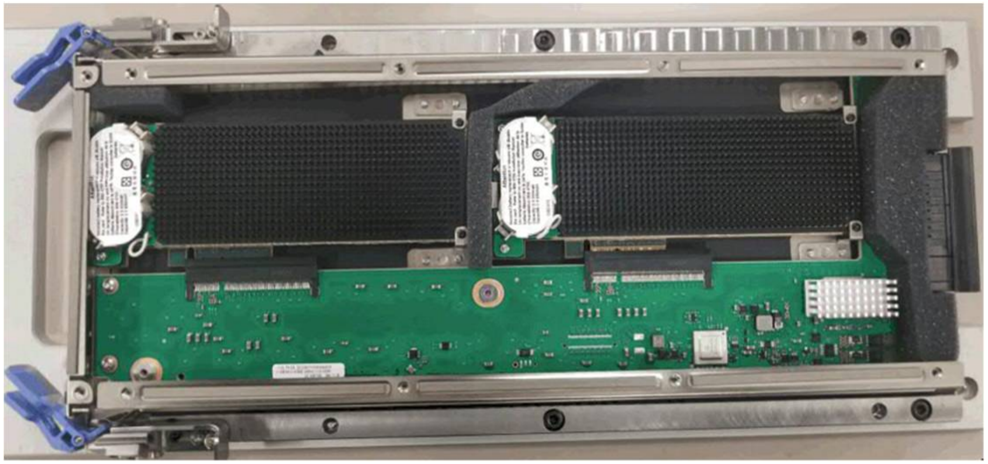
- Elliptic Curve Keys
  - P256 – 32 byte
  - P384 – 48 byte
  - P521 – 521 bits (right aligned, left-padded 0s)
  - Ed25519 – 256 bits
  - Ed448 – 57 bytes



z15 Crypto Express Cards

- Crypto Express7S Single Port (FC #0899)
- Crypto Express7S Dual Port (FC #0898)
- Crypto Express6S (FC #0893) – Carry forward from z14
- Crypto Express5S (FC #0890) – Carry forward from z13
- (Still a) Max of 16 engines on a CEC

FC #0899



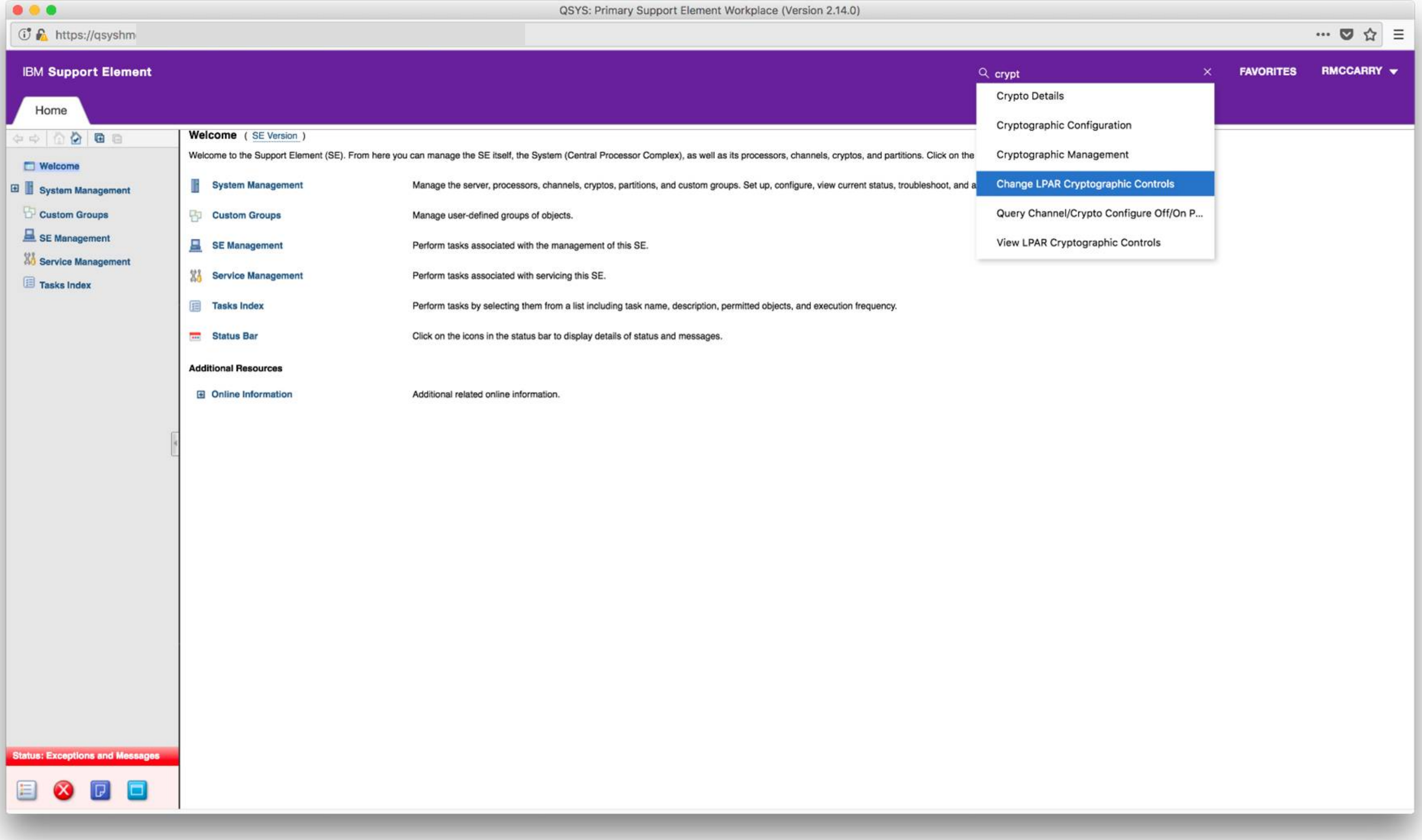
FC #0898

Crypto Express7S

- CCA 7.0
  - CEX7S designed to meet FIPS 140-2 Level 4
  - CCA 7.0 designed to meet HSM requirements from PCI-SSC
  - CCA 7.0 includes enhancements from limited availability release CCA 6.3
- CCA 6.3 Enhancements
  - ASC X9 TR-34 Support
  - X.509 Support
- EP11 Mode
  - Designed to meet requirements of BSI for conformance w/common criteria in version 3.1 (rev. 4) with EAL 4
  - EP11 4.7 adds support for PKCS #11 v2.4 standard
  - Adds Protected Key support for EP11 mode
  - Support for SHA3, EdDSA and EdDH
  - Dilithium support
- Double the number of public key crypto engines
- Designed for 2X Performance Improvement
- 3 x Performance when configured as an accelerator
- Processor types of 7A, 7C, 7P

Configuring Crypto

- HMC 2.15.0
  - Crypto Config/Management no longer requires Single Object Mode


QSYS: Primary Support Element Workplace (Version 2.14.0)
https://qsyshm
IBM Support Element
crypt
FAVORITES
RMCCARRY
Home
Crypto Details
Cryptographic Configuration
Cryptographic Management
Change LPAR Cryptographic Controls
Query Channel/Crypto Configure Off/On P...
View LPAR Cryptographic Controls
Welcome
System Management
Custom Groups
SE Management
Service Management
Tasks Index
Status: Exceptions and Messages

Welcome (SE Version)

Welcome to the Support Element (SE). From here you can manage the SE itself, the System (Central Processor Complex), as well as its processors, channels, cryptos, and partitions. Click on the

System Management	Manage the server, processors, channels, cryptos, partitions, and custom groups. Set up, configure, view current status, troubleshoot, and a
Custom Groups	Manage user-defined groups of objects.
SE Management	Perform tasks associated with the management of this SE.
Service Management	Perform tasks associated with servicing this SE.
Tasks Index	Perform tasks by selecting them from a list including task name, description, permitted objects, and execution frequency.
Status Bar	Click on the icons in the status bar to display details of status and messages.

Additional Resources

⊞ Online Information	Additional related online information.

z/OS Support for CEX7S

- Exploitation support with HCR77D1
  - z/OS 2.2 thru z/OS 2.4
  - Quantum Safe Support requires additional PTFs for SMF
- Toleration (CEX7S is treated like a CEX6S) support with PTFs
  - z/OS 2.1 thru z/OS 2.4
- VISA FPE
  - Requires z15 with CEX5S, CEX6S or CEX7S
  - Requires Service Agreement with Visa
- Quantum Safe
  - z/OS V2.4 w/PTFs and HCR77D1
  - z/OS V2.3 w/HCR77D1 and coexistence PTFs for SMF
  - z/OS V2.2 w/HCR77D1 and coexistence PTFs for SMF, PTFs
  - z/VM V7.1 w/ PTFs for guest exploitation
  - z/VM V6.4 w/ PTFs for guest exploitation

Other Operating System Support for CEX7S

- Exploitation support
  - z/VM V7.1 for guest exploitation and exploitation with the z/VM TLS/SSL server
  - z/VM V6.4 with PTFs for guest exploitation and exploitation with the z/VM TLS/SSL server
  - zTPF V1.1 with PTFs (limited to 15 domains)
- Toleration support
  - z/VM V7.1 for guest use
  - z/VM V6.4 with PTFs for guest use
  - z/VSE V6.2 with PTFs
  - zTPF V1.1 with PTFs (limited to 15 domains)
- Linux on Z – IBM is working with Linux distributors to provide support
  - SUSE Linux Enterprise Server 12 and SLES 11
  - Redhat Enterprise Linux (RHEL) 7 and Redhat Enterprise Linux 6
  - Ubuntu 16.04 LTS (or higher)
- KVM hypervisor

New z/VM Functionality

- Dynamic Crypto (APAR VM66266)
  - DEFINE CRYPTO
  - VARY ON/OFF CRYPTO
  - ATTACH/DETACH CRYPTO
  - QUERY CRYPTO DOMAINS & QUERY VIRTUAL CRYPTO enhanced

z/OS: ICSF Version and FMID Cross Reference (TD103782)

**Older versions of ICSF may need toleration maintenance installed to support newer hardware

FMID	External Name	Applicable z/OS Releases	Availa-bility	Planned EoS	Supported Servers
HCR77B0	Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1	z/OS V1.13; z/OS V2.1	Feb 2015	TBD	z890/z990;z9;z10; z196/z114;zEC12/zBC12; z13/z13s**,z14/z14R1**, z15**
	z/OS 2.2	z/OS V2.2	Sep 2015	TBD	

HCR77B1	Cryptographic Support for z/OS V1R13-z/OS V2R2	z/OS V1.13;
		z/OS V2.1;
		z/OS V2.2
			Nov 2015	TBD	z890/z990;z9;z10; z196/z114;zEC12/zBC12;z13/z13s**,z14/z14R1**,z15**

HCR77C0	Cryptographic Support for z/OS V2R1 – z/OS V2R2	z/OS V2.2; z/OS V2.1	Oct 2016	TBD	z9; z10; z196/z114; zEC12/zBC12; z13/z13s; z14/z14R1**,z15**
	z/OS 2.3	z/OS V2.3	Sep 2017	TBD	
HCR77C1	Cryptographic Support for z/OS V2R1 – z/OS V2R3	z/OS V2.3; z/OS V2.2; z/OS V2.1	Sep 2017	TBD	z9; z10; z196/z114; zEC12/zBC12;z13;z14, z15**
HCR77D0	Cryptographic Support for z/OS V2R2 – z/OS V2R3	z/OS 2.2; z/OS V2.3	Dec. 2018	TBD	z10; z196/z114; zEC12/zBC12;z13;z14,z15**
	z/OS 2.4	z/OS 2.4	Oct 2018	TBD	
HCR77D1	Cryptographic Support for z/OS V2R2 – z/OS V2R3	z/OS V2.2; z/OS V2.3	Sept 2019	TBA	z10; z196/z114; zEC12/zBC12;z13;z14,z15

HCR77D1 – Cryptographic Support for z/OS V2R2-V2R4

- Support for CEX7S
- Support for ECC operations on the CPACF
  - CSNDDSG – Digital Signature Generate
  - CSNDDSV – Digital Signature Verify
- TR-34 APIs
- New SMF record for Master Key change
- New Health Checks
- Quantum safe algorithms

TR-34

- Technical Report for ANSI X9.24-2
  - Technical Report provides guidance, it is not a requirement
  - De fatco recommendation for key management using asymmetric techniques
- ANSI X9.24-2 Distribution of symmetric keys using asymmetric techniques, from a single Key Distribution Host (KDH) to many Key Receiving Devices (KRDs)
- Key Binding – During setup, the remote (KRD) device is bound to the host
- Chapter 10 in APG, ‘TR-34 symmetric key management’
  - TR-34 Bind-Begin
  - TR-34 Bind-Complete
  - TR-34 Key Distribution
  - TR-34 Key Receive

PCI-HSM

- Compliant tagged key support
  - AES keys can be COMP-TAGged
  - RSA keys can be COMP-TAGged
  - Protected keys can now be COMP-TAGged
  - AES symmetric key tokens must be variable-length, but must use fixed-length payloads

Dilithium

- Key Type LI2
- Algorithm Type LI2
- PKCS #11 Generate Key Pair (CSFPGKP/CSFPGKP6)
- RC=12, RS=DDE (3550) Dilithium operation failed because hardware does not support it

SMF

- New Subtype 49 Master Key Event
- CEX7C is added to many of the records and PCIXCC has been dropped

- CPU MF – new counters
  - ECC Function/Cycle Count
  - ECC Blocked

Health Check: ICSF_PKCS_PSS_SUPPORT

- Applies to HCR77C0 and later
  - Check is performed every time ICSF is started
- Detects whether the current hardware configuration supports PKCS-PSS algorithms
  - Requires ECC-MK be loaded
  - CCA 5.3 or higher
- Messages
  - CSFH0045I – Check for PKCS-PSS
  - CSFH0046I – PKCS-PSS may be exploited
  - CSFH0047E – missing ECC-MK
  - CSFH0048E – missing coprocessor

Health Check: ICSF_WEAK_CCA_KEYS

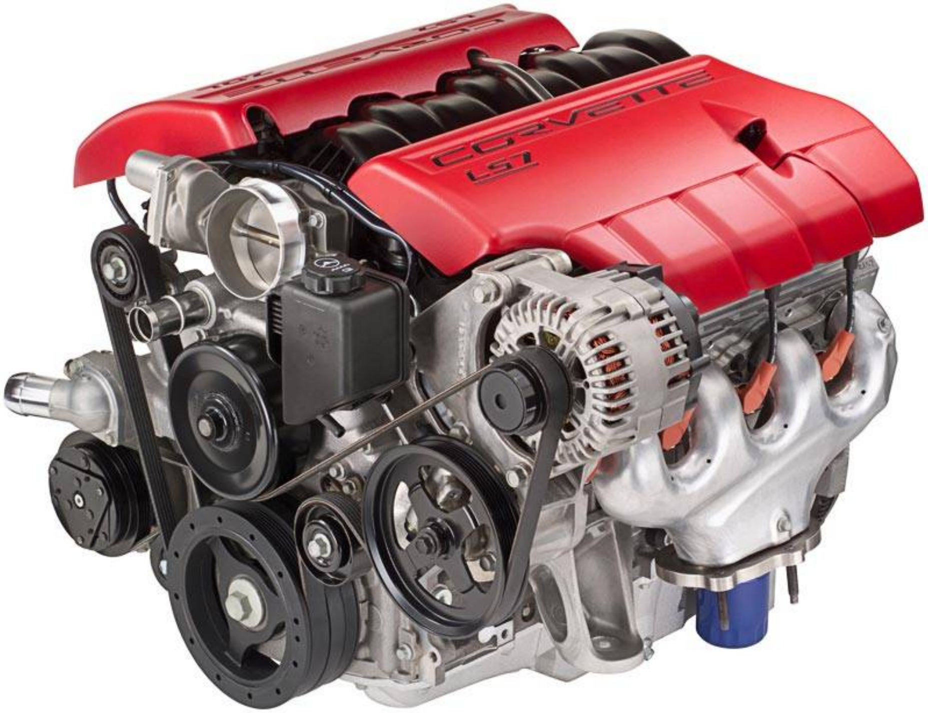
- Applies to HCR77D1 and later
  - Check is performed every time ICSF is started
- Lists labels of cryptographically weak keys in the PKDS
  - Modulus < 1024
  - Status (active, archived) does not matter
- Messages
  - CSFH0042 Check for weak CCA cryptographic keys in the PKDS
  - CSFH0043 No weak CCA cryptographic keys were found in the PKDS.
  - CSFH0044 Weak CCA cryptographic keys in the PKDS were found

Deprecated callable services

Old API	New API
Clear key Import (CSNBCKI/CSNECKI)	Multiple Clear Key Import (CSNBCKM/CSNECKM)
Key Translate (CSNBKTR/CSNEKTR)	Key Translate2 (CSNBKTR2/CSNEKTR2)
Prohibit Export (CSNBPEX/CSNEPEX)	Restrict Key Attribute (CSNBKRA/CSNEKRA)
Prohibit Export Extended (CSNBPEXX/CSNEPEXX)	Restrict Key Attribute (CSNBKRA/CSNEKRA)
Secure Key Import (CSNBSKI/CSNESKI)	Multiple Secure Key Import (CSNBSKM/CSNESKM)
Decode (CSNBDCO/CSNEDCO)	Symmetric Key Decipher (CSNBSYD/CSNBSYD1/CSNESYD/CSNESYD1)
Encode (CSNBECO/CSNEECO)	Symmetric Key Encipher (CSNBSYE/CSNBSYE1/CSNESYE/CSNESYE1)
Encrypted PIN Translate (CSNBPTR/CSNEPTR)	Encrypted PIN Translate2 (CSNBPTR2/CSNEPTR2)

ICSF Miscellaneous

- ICSF Application Programmer's Guide (SC14-7508-09)
  - Adds Appendix J, “Cryptographic hardware engines and software used by ICSF,”



RACF and Crypto

- PassTickets –one-time-use password substitute to authenticate a user, enhances security across a network
  - PassTicket keys can be stored in an ICSF key token, as opposed to masking in the RACF database
  - Use SSIGNON segment of the PTKTDATA profile
- Dynamic RRSF VSAM Data Set Re-Allocation Support
  - RACF now supports the ability to dynamically reallocate (replace) Workspace data sets (INMSG/OUTMSG)
  - These are just VSAM data sets, so they can be encrypted using data set encryption (Pervasive Encryption)
- Identity Token – crypto keys must be stored in ICSF, not RACF

JES and Crypto

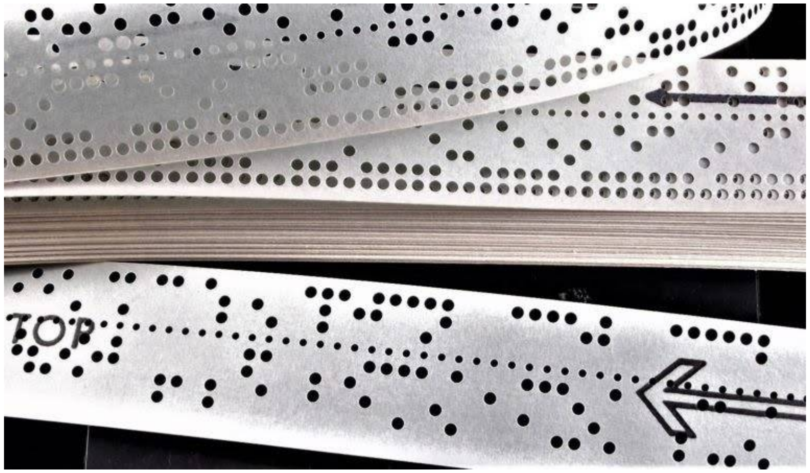
- Compress and Encrypt JES2 managed data sets on the spool
- DSKEYLBL is assigned similar to data set encryption
  - DSKEYLBL on DD statement
  - JESJOBS class ENCRYPT profile, which now has a JES segment
    - JES Segment contains the key label
  - Can be overridden, if you have READ Access
    - JES.ENCRYPT.SUBMITTER – for jobs submitted via internal reader
    - JES.ENCRYPT.OWNER - for jobs submitted via other means, such as card reader

zDMF

- Non-disruptive or minimally-disruptive data migration at the data set level
  - Simplifies encryption of data sets (pervasive encryption)
- Features
  - Volume consolidation
  - Multi-volume data set consolidation
  - Data set extent consolidation
  - Move non-EAV to EAV
- Future
  - Convert data set from basic format to extended format, and encrypt at the same time
  - Perform key rotation

TKE Feature Codes for a z15

- Ordering new TKE for z15 with CEX7S cards
  - FC #0086 TKE Hardware
    - FC #0157 TKE KMM
  - FC #0085 Rack Mounted TKE
    - FC #0156 TKE Rack Mount KMM
  - FC #0190 Customer supplies TKE Keyboard/Monitor/Mouse
  - FC #0881 TKE 9.2 LIC
  - FC #0891 2 Identiv Smart Card (SC) Readers with 20 SCs (Part #00RY790)
  - FC #0900 Package of 10 Smart Cards (Part #00RY790)
- z15 with CEX6S Cards
  - FC #0879 TKE 9.1 LIC
- z15 with CEX5S Cards
  - FC #0880 TKE 9.0 LIC or
  - FC #0879 TKE 9.1 LIC



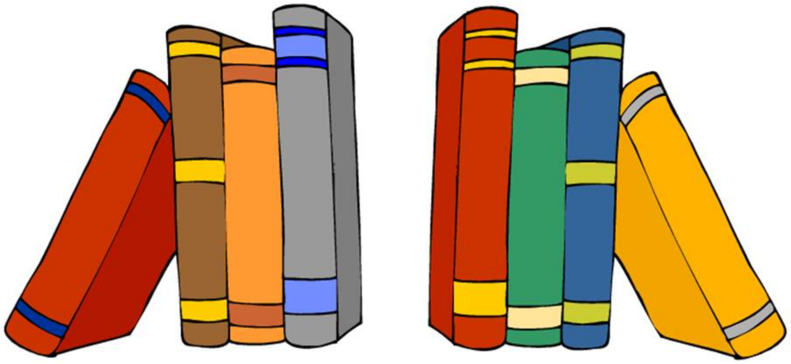
Upgrading a TKE

- Pre-TKE 9.0, requires a new feature (FC #0844)
- TKE Hardware FC #0847 & #0849 can only be upgraded to TKE 9.1 LIC
- Upgrading a TKE 9.0 to 9.2 requires going thru TKE 9.1
- TKE must be assigned to a z14 or later

TKE 9.2

- Crypto Express7S support
- Option to use SSL/TLS to secure the communication between the TKE and the host
  - Comm Server configuration must define the host & port for SSL/TLS
  - Host definition must specify SSL/TLS
  - Must import the host certificate to the TKE
- EP11 Transport wrapping key policy
  - Uses EC-320 by default, with an effective key length of 128-bits
  - Will use EC-521, with a true 256-bit AES key
- Logon Profile Wizard will check the DEFAULT authorities every time it runs
- On previous TKEs, you can generate a 1024-bit RSA authority signature key. The CEX7S will support a 1024-bit RSA authority Signature key, but it cannot generate one
- P521 ECC key for an OA (Outbound Authentication) signature key
- Auto Accept of cryptographic modules
- CMACZERO support for AES keys

z15 & HCR77D1 References



- Announcment Letters
  - z15 119-027
    - https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS119-027&appname=lenovous&language=en
- IBM Manuals
  - SC14-7505-08 ICSF Overview
  - SC14-7506-08 ICSF Administrator's Guide
  - SC14-7507-08 ICSF System Programmer's Guide
  - SC14-7508-08 ICSF Application Programmer's Guide
  - SC14-7509-07 ICSF Messages
  - SC14-7510-06 ICSF Writing PKCS #11 Applications
  - GI11-9478-08 Program Directory for Cryptographic Services for z/OS V2R2 – z/OS V2R4

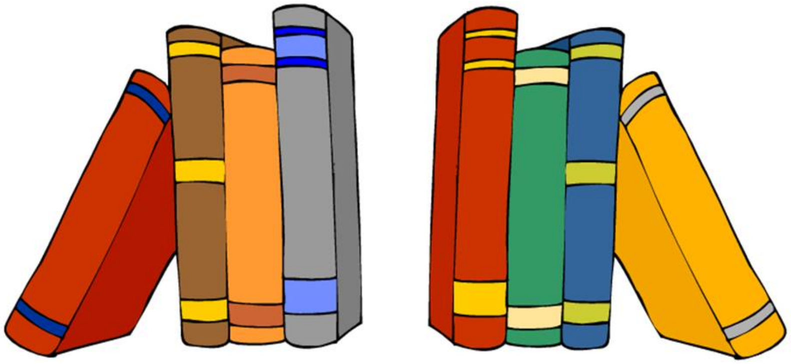
Other references

- Deprecation of DES/TDES
  - NIST SP 800-131A Rev. 2
    - https://www.nist.gov/publications/transitioning-use-cryptographic-algorithms-and-key-lengths
- FIPS 140-3
  - Announcement
    - https://www.nist.gov/news-events/news/2019/05/announcing-approval-and-issuance-fips-140-3-security-requirements
- Quantum Safe
  - NIST Competition
    - https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals
  - IBM
    - https://securityintelligence.com/how-to-future-proof-your-enterprise-with-quantum-safe-cryptography/

On the Web

- Techdocs – www.ibm.com/support/techdocs
  - TD103782 – z/OS: ICSF Version and FMID Cross Reference
  - Or search on ‘Crypto’
- z/OS Downloads – Cryptographic Support Downloads
  - https://www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosDownloads?OpenDocument
- Crypto Cards
  - https://www.ibm.com/security/cryptocards

zDMF References



- Announcment Letters
  - ZDMF / TDMF 218-533
    - https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=897/ENUS218-533&infotype=AN&subtype=CA
- Share Presentation
  - Pittsburgh, August 2019 by Rebecca Levesque of 21st Century Software
    - https://events.share.org/Summer2019/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=8644&SessionDateID=52

TKE References

- SC14-7511-09 ICSF Trusted Key Entry Workstation User’s Guide
- TKE YouTube Videos
  - See the WS UG for a list of TKE 9.1 videos
  - Google search
- TechDocs - TKE Hardware Support Info For TKE 9.2v1
  - http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD106423

Questions