Hardware (HW) Crypto Support in IBM z Systems

Jan Tits
IBM systems
jantits@be.ibm.com
Hardware Crypto support in z Systems
z Systems Hardware Based Cryptography

Exploited by Java, DB2/IMS encryption tool, DB2® built in encryption z/OS Communication Server, IPsec/IKE/AT-TLS, z/OS System SSL, z/OS, z/OS Encryption Facility, Linux on z Systems and more...

CP Assist For Cryptographic Functions (CPACF)

- Provides a set of symmetric cryptographic and hashing functions for:
  - Data privacy and confidentiality
  - Data integrity
- Enhances the encryption/decryption performance of clear-key operations for SSL, VPN, Data storing applications
- Protected key support for additional security of cryptographic key
- Available on every Processor Unit defined as a CP, IFL, zAAP and zIIP

Crypto Express5S Co-processor

Hardware protected secure key cryptography

- Secure key transactions to protect your most sensitive information.
- Designed to meet the security requirements of Federal Processing Information Processing Standard (FIPS) 140-2 Level 4 for applications with the most stringent security requirements.
- Hardware optimized for Transport Layer Security (TLS) acceleration and clear key RSA operations allowing savings of CPU by offloading CPU intensive cryptographic algorithms.
- Supports open industry standard cryptography services
- Simplification of porting PKCS#11 applications to z Systems

Regional Crypto Enablement

- Framework to enable the integration of IBM certified 3rd party cryptographic hardware for regional or industry encryption requirements

Performance Results:

Enhanced performance over zBC12:
2X Encryption
3.5X Hashing

2x performance improvement over CEX4
Industry leading FIPS 140-2 Level 4 Certification Design

Rack-Mounted Trusted Key Entry

- Domain Cloning for easier and faster administration of Crypto Adapters
- Enhanced password security for the Console and Host Password protection
- Save/Restore Customized Data feature
- Launch coordinated master key role directly from the Trusted Key Entry Workstation
Crypto Express5S

- One PCIe adapter per feature
  - Initial order – two features
- Designed to be FIPS 140-2 Level 4
- Installed in the PCIe I/O drawer
- Up to 16 features per server
- Prerequisite: CPACF (#3863)
- Designed for 2X performance increase over Crypto Express4S

Three configuration options for the PCIe adapter

- Only one configuration option can be chosen at any given time
- All card secrets are erased when switching to or from EP11 Coprocessor mode

### Accelerator | CCA Coprocessor | EP11 Coprocessor
---|---|---
TKE | N/A | REQUIRED
CPACF | NO | REQUIRED
UDX | N/A | UDX
CDU | YES(SEG3) | CDU

Clear Key RSA operations and SSL acceleration

Secure Key crypto operations

Secure Key crypto operations

### Business Value

- High speed advanced cryptography; intelligent encryption of sensitive data that executes off processor saving costs
- PIN transactions, EMV transactions for integrated circuit based credit cards (chip and pin), and general-purpose cryptographic applications using symmetric key, hashing, and public key algorithms, VISA format preserving encryption (VFPE), and simplification of cryptographic key management.
- z13s adds Secure AES GCM encryption mode, Interoperable ECC key derivation algorithm, and addition of new Key Check Value algorithm
- Designed to be FIPS 140-2 Level 4 certification to meet regulations and compliance for PCI standards
z13 CPACF Performance Enhancements

- CP Assist for Cryptographic Function Co-processor redesigned from "ground up"
- Enhanced performance over zEC12
  - Does not include overhead for COP start/end and cache effects
  - Enhanced performance for large blocks of data
    - AES: 2x throughput vs. zEC12
    - TDES: 2x throughput vs. zEC12
    - SHA: 3.5x throughput vs. zEC12
- Exploiters of the CPACF benefit from the throughput improvements of z13's CPACF such as:
  - DB2/IMS encryption tool
  - DB2® built in encryption
  - z/OS Communication Server: IPsec/IKE/AT-TLS
  - z/OS System SSL
  - z/OS Network Authentication Service (Kerberos)
  - DFDSS Volume encryption
  - z/OS Java SDK
  - z/OS Encryption Facility
  - Linux on z Systems; kernel, openssl, openCryptoki, GSKIT
Secure Keys vs Clear Keys vs Protected Keys

- **Secure Key** - provides high security because the key material is protected by the master key. Master keys are loaded within the cryptographic coprocessor and are used to wrap and unwrap secure key material within the secure boundaries of the HSM. This prevents secure key material from ever appearing in the clear.

- **Clear Key** – when performing symmetric encryption, TDES and AES, with clear keys, ICSF uses the CPACF to provide high performance. Clear Key refers to key material that is in the clear, meaning the clear key value appears within application storage and within the keystore.

- **Protected Key** - provides a high performance and high security solution by taking advantage of the high speed CPACF while utilizing symmetric keys protected by the cryptographic coprocessor Master Key. To use a CKDS encrypted key, the ICSF segment of the CSFKEYS class general resource profile associated with the specified key label must contain SYMCPACFWRAP(YES).
User Defined Extensions (UDX)

- UDX support available for Crypto Express features defined as CCA coprocessors
- Allows additional functions to the CCA API, which execute inside the secure crypto feature
  - Standard CCA functions plus UDX enhancements available
- Tied to specific versions of the CCA code and the related host code
Trusted Key Entry (TKE) Workstation

Components
• Workstation with a 4767 Cryptographic Coprocessor
• TKE 8.1+ LIC
• Smart card readers and smart cards
  – Required if using Enterprise PKCS #11 LIC
  – Optional if using IBM CCA LIC

Purpose
• To securely manage multiple Cryptographic Coprocessors and keys on various generations of z Systems from a single point of control
  – Support of new hardware, firmware and software
  – Support requirements for standards
  – Simplification of tasks

Popular Features
• Domain Grouping
  – Ability to broadcast a command to a set of domains
• Wizards
  – Configuration Migration Tasks
  – Migrating IBM Host Crypto Module Public Configuration Data
  – TKE Workstation Setup
• NEW with TKE 8.1
  – Domain Cloning for easier and faster administration of Crypto Adapters
  – Enhanced password security for the Console and Host Password protection
  – Save/Restore Customized Data feature
  – Launch coordinated master key role directly from the Trusted Key Entry Workstation
z/OS Crypto Stack

z Systems Software
z/OS
- ICSF
- RACF
- RMF
- z/OS PKI Services
- System SSL
- Java PKCS#11 Provider

PKCS #11 Services
CCA Device Driver
CPACF
Software Crypto
PKCS #11 Device Driver

CCA Services

Secure Key Material
Clear Key Material

TKE
Trusted Key Entry
CCA | PKCS11

Crypto Express5S (CEX5C)
Crypto Express5S (CEX5P)

Request routing
CCA Verbs

Request routing
PKCS #11 Verbs
Linux on z Systems Crypto Stack

**Application Layer**
- openssh (ssh, scp, sftp)
- Apache (mod_ssl)
- Apache (mod_nss)
- IBM C/C++ SW.
- Customer C/C++ SW using PKCS#11
- WAS
- Customer Java/JCE SW
- Customer CCA SW

**Standard Crypto Interfaces**
- openssl / libcrypto
- ibmca engine
- openCryptoki (PKCS#11)
- ica token
- ep11 token
- cca token
- icsf token

**System z HW Crypto Libraries**
- ICA (libica)
- EP11 library
- CCA (libcsulca)
- z/OS crypto server via network

**Operating System**
- IPsec
- dmcrypt
- kernel crypto
- framework
- System z backend
- zcrypt device driver

**Kernel**
- Accelerator (RSA)
- EP11 Co-Processor
- CCA Co-Processor (RSA, RNG, ECC)

**Crypto Adapters**
- openssl / libcrypto
- openCryptoki
- ibmca engine
- ica token
- cca token
- ep11 token
- icsf token

**System z backend**
- Crypto Adapters
- openssh (ssh, scp, sftp)
- Apache (mod_ssl)
- Apache (mod_nss)
- IBM C/C++ SW.
- Customer C/C++ SW using PKCS#11
- WAS
- Customer Java/JCE SW
- Customer CCA SW

**Hardware**
- clear key
- protected key
- secure key

**Operating System**
- JCA/JCE
- IBMPKCS11Impl
- NSS
- Customer CCA SW

**Standard Crypto Interfaces**
- openssl / libcrypto
- ibmca engine
- openCryptoki (PKCS#11)
- ica token
- ep11 token
- cca token
- icsf token

**System z HW Crypto Libraries**
- ICA (libica)
- EP11 library
- CCA (libcsulca)
- z/OS crypto server via network

**Operating System**
- IPsec
- dmcrypt
- kernel crypto
- framework
- System z backend
- zcrypt device driver

**Kernel**
- Accelerator (RSA)
- EP11 Co-Processor
- CCA Co-Processor (RSA, RNG, ECC)

**Crypto Adapters**
- openssl / libcrypto
- openCryptoki
- ibmca engine
- ica token
- cca token
- ep11 token
- icsf token

**System z backend**
- Crypto Adapters
- openssh (ssh, scp, sftp)
- Apache (mod_ssl)
- Apache (mod_nss)
- IBM C/C++ SW.
- Customer C/C++ SW using PKCS#11
- WAS
- Customer Java/JCE SW
- Customer CCA SW

**Hardware**
- clear key
- protected key
- secure key
Additional z Systems Operating Systems with Crypto Support

- **z/VM**
  - z/VM Guest Support for Crypto Express 5S in Accelerator mode
  - CCA Coprocessor mode and EP11 Coprocessor mode

- **z/VSE**
  - Supports Crypto Express 5S in Accelerator mode and CCA Coprocessor mode
  - CPACF support
  - OpenSSL Support
  - Encryption Facility support (w/ OpenPGP)
Security evaluations

- Security evaluations, conducted by independent, accredited evaluators provide assurance (confidence) in the evaluated products' security attributes.
- Some public and private sector organizations mandate that their acquired products are evaluated. Even when evaluations aren't mandatory, acquiring organizations benefit from them.
- The two security evaluation programs IBM products use are
  - Common Criteria (CC – a.k.a. ISO/IEC 15408)
  - FIPS (FIPS 140-2 - Cryptographic Module Validation Program, CMVP)
The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles.

**z/OS**
- Common Criteria EAL4+
  - z/OS 1.12, z/OS 1.13, z/OS V2R1 (OSPP)
  - z/OS 1.11 + RACF (OSPP)
- Common Criteria EAL5+
  - RACF V2R1 (OSPP)
  - RACF V1R13 (OSPP)
  - RACF V1R12 (OSPP)
- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services
- FIPS 140-2
  - System SSL z/OS 1.10 → 1.13
  - z/OS ICSF PKCS#11 Services – z/OS 1.11 → z/OS 1.13
- Statement of Integrity

**z/VM**
- Common Criteria EAL4+
  - z/VM 6.3 with OSPP with -LS and -VIRT
- FIPS 140-2 validated
  - z/VM 6.3 System SSL is FIPS 140-2 validated.
- System Integrity Statement

**Linux on System z**
- Common Criteria EAL4+
  - SUSE SLES11 SP2 certified at EAL4+ with OSPP
  - Red Hat EL6.2 EAL4+ with OSPP
- OpenSSL - FIPS 140-2 Level 1 validated
- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

**Virtualization with partitions**

**Cryptography**

- z Systems z13
  - Common Criteria EAL5+ with specific target of evaluation – LPAR: Logical partitions
  - Crypto Express5S – In evaluation
    - FIPS 140-2 level 4 Hardware Evaluation
    - zEnterprise 196 & zEnterprise 114; System zEC12 & BC12
    - Common Criteria EAL5+ with specific target of evaluation – LPAR: Logical partitions
  - Crypto Express3 & Crypto Express4S,
    - FIPS 140-2 level 4 Hardware Evaluation
    - Approved by German ZKA
  - CP Assist
    - FIPS 197 (AES)
    - FIPS 46-3 (TDES)
    - FIPS 180-3 (Secure Hash)
z/OS Integrated Cryptographic Services Facility (ICSF)

ICSF works with the hardware cryptographic features and the Security Server (RACF element) to provide secure, high-speed cryptographic services in the z/OS environment.

- ICSF provides the application programming interfaces by which applications request cryptographic services.
- ICSF is the default means by which the secure cryptographic features are loaded with master key values, allowing the hardware features to be used by applications.
- ICSF callable services and programs can be used to generate, maintain, and manage keys that are used in the cryptographic functions.

ICSF uses keys in cryptographic functions to
- Protect data
- Protect other keys
- Verify that messages were not altered
- Generate, protect and verify PINs
- Distribute keys
- Generate and verify signatures
IBM Common Cryptographic Architecture (CCA) for z/OS ICSF

IBM Common Cryptographic Architecture (CCA)

- IBM proprietary cryptographic application programmers interface (API) providing a broad range of cryptographic services including
- standard cryptographic algorithms
- financial services standards

z/OS ICSF Naming Conventions for CCA

- CSNB* = CCA 31-bit Symmetric Key API
- CSNE* = CCA 64-bit Symmetric Key API
- CSND* = CCA 31-bit Asymmetric Key API
- CSNF* = CCA 64-bit Asymmetric Key API

CCA Functions & Algorithms

- Encrypt / Decrypt (AES, DES, DES3, RSA)
- Sign / Verify (RSA, ECC)
- MAC Generate / Verify (AES, DES, DES3)
- HMAC Generate / Verify (HMAC)
- Key Generate (AES, DES, DES3, HMAC)
- Key Pair Generate (RSA, ECC)
- Key Agreement (ECC, DH)
- One Way Hash
- Random Number Generate
- Key Import / Export
- TR-31 Block Import / Export
- Financial Crypto
  - PIN Generate / Verify / Translate
  - PIN Encrypt
  - Diversified Key Generate
  - Derive Unique Key Per Transaction (DUKPT)
  - CVV Generate / Verify
  - Secure Messaging for Keys / Pins
  - … And Many More!
PKCS#11 Cryptographic Token Interface Standard for z/OS ICSF

PKCS #11 Cryptographic Architecture
- Originally published by RSA Laboratories, now maintained by OASIS
- Defines a standard API for devices that hold cryptographic information and perform cryptographic functions
- Enterprise PKCS#11 – EP11

z/OS ICSF Naming Convention for PKCS#11
- CSFP* = PKCS#11 APIs

PKCS#11 Functions & Algorithms
- Encrypt / Decrypt (AES, DES, TDES, RSA)
- Sign / Verify (RSA, DSA, ECDSA)
- HMAC Generate / Verify
- Key Generate (DES, TDES, AES, Blowfish, RC4)
- Key Pair Generate (RSA, DSA, EC)
- Key Derivation
- Domain Parameter Generation (DH)
- One Way Hash
- Random Number Generate
- Wrap / Unwrap Key

Designed for portability and FIPS/Common Criteria certification
ICSF Support for EC12 and z13

WD#13 – HCR77A1 – Sept 2013
- HW: CCA Firmware Support
- HW: Additional EP11 Algorithms
- Improved CTRACE Support
- KDS Key Utilization Statistics
- OWH/RNG SAF Check Removal
- Crypto Config Simplification

WD#14 – HCR77B0 – Feb 2015
- HW: CCA Firmware Support
- HW: 85 Domain Support *
- HW: CPACF Deterministic Random Bit Generator (NIST DRBG)
- HW: Format Preserving Encryption
- KDS Key Archiving
- Key Material Validity
- ICSF Health Checks
- ICSF UDX Exit Support

* 85 domains supported on the z13 with the Crypto Express5S

WD#15 - HCR77B1 – Nov 2015
- Regional Crypto Enablement
- MVS Console Commands
- 3Q2015 SPE Rollup

HCR77B1 SPEs – Planned March 2016
- TKE Remote Coordinated Change Master Key
- CCA Verb Algorithm Support
- Regional Crypto Enablement Phase 2
- Format Preserving Encryption Point to Point Encryption (P2PE)
z Systems Software Exploiters of ICSF

z/OS Software Components
• System SSL
• Java Cryptography Extension
• RACF Security
• DB2 Database
• PKI Services
• IBM Tivoli Directory Server
• Kerberos Network Authentication Service
• Websphere MQ
• Websphere Application Server
• z/OS Communications Server

IBM Solutions
• IBM Infosphere Guardium
• Sterling Connect:Direct
• …