88. GSE z/OS zExpertenForum
Spiez, 18.04.2018

IBM z14 Cryptography

Martin Söllig
soellig@de.ibm.com
0172-7344232

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 more complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*BladeCenter®, CICS®, DataPower®, DB2®, e business(logo)®, ESCON, eServer, FICON®, IBM®, IBM (logo)®, IMS, MVS, OS/390®, POWER6®, POWER6+, POWER7®, Power Architecture®, PowerVM®, PureFlex, PureSystems, S/390®, ServerProven®, Sysplex Timer®, System p®, System p5, System x®, z Systems®, System z9®, System z10®, WebSphere®, X-Architecture®, z13™, z13s ™, **z14 ™**, z Systems™, z9®, z10, z/Architecture®, z/OS®, z/VM®, z/VSE®, zEnterprise®, zSeries®, IBM Z ®

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 Sync 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.

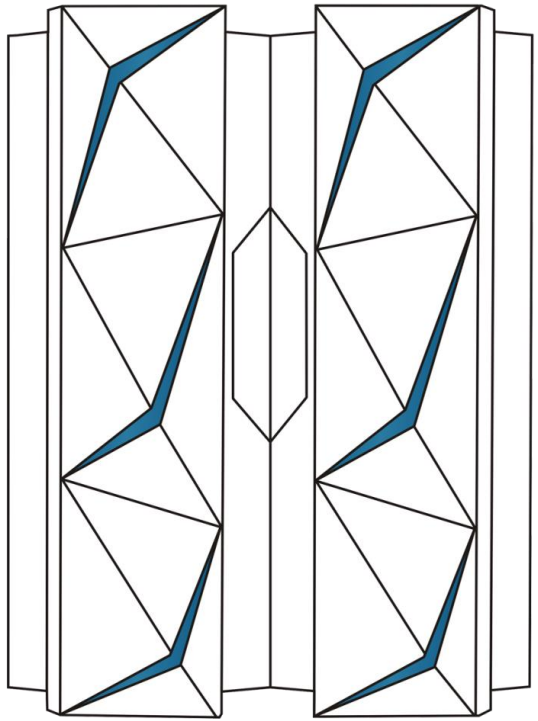
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available 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 Sync 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.

Table of Content

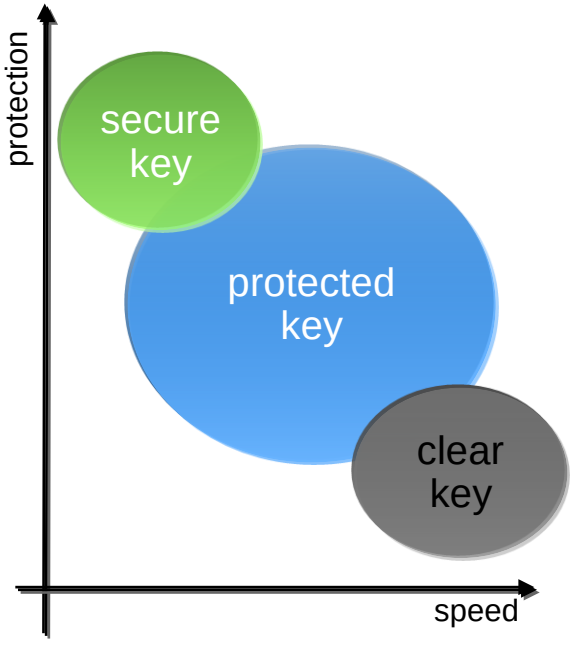


Business Security is dependent on Cryptography

- **Confidentiality**
  - *Keep business secrets secret (encryption/decryption)*
- **Data Integrity**
  - *Be sure your business data is left unchanged (Signature, sign, verify)*
- **Authentication & Non Repudiation**
  - *Positively identify users of your data (Certificate, Signature)*
- **No unacceptable overheads**
  - *Keep your system secure, manageable and productive*

Three levels of protection – Three levels of speed

- **Secure Key** – *key value* does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)
  - Example use: PIN handling and verification
- **Protected Key** – *key value* does not exist outside of physical hardware, although the hardware may not be tamper-resistant
  - Unique to System z
  - Example use: protection of data at rest
- **Clear Key** – *key value* is in the clear, at least briefly, somewhere in the environment
  - Example use: SSL transaction security



IBM z14 at a glance

System, Processor, Memory
Five hardware models: M01, M02, M03, M04, M05
10 core 5.2GHz 14nm PU SCM
1 - 170 PUs configurable as CPs, zIIPs, IFLs, ICFs, up to 196 Pus
Increased Uniprocessor capacity
Up to 33 sub capacity CPs at capacity settings 4, 5, or 6
CPC Drawers and backplane Oscillator
Enhanced SMT and new instructions for SIMD
Enhanced processor/cache design with 1.5x more on-chip cache sizes
Up to 32 TB DRAM, protected by Redundant Array of Independent Memory (RAIM)
Virtual Flash Memory (VFM)
192 GB HSA
Improved pipeline design and cache management

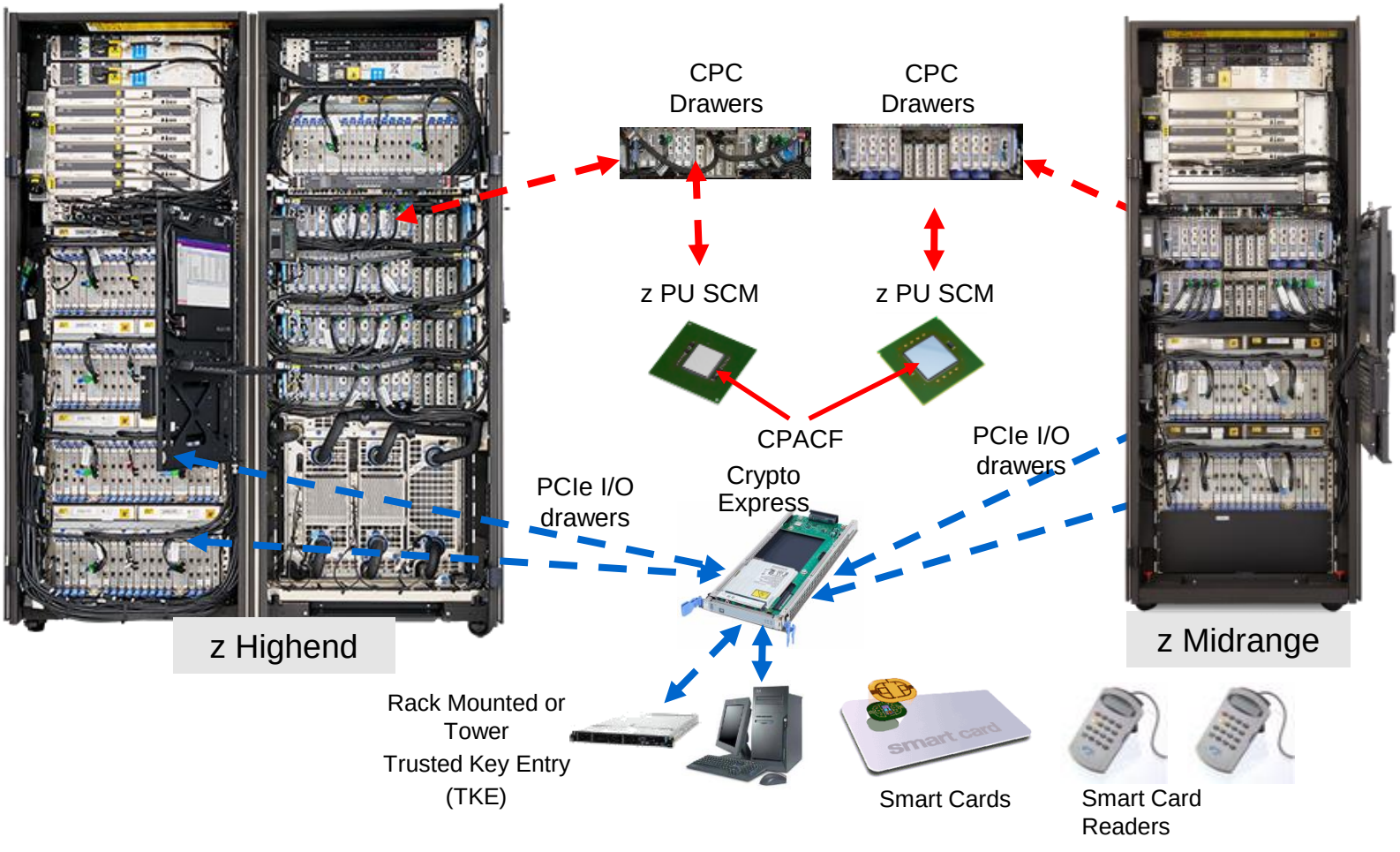
Announce: July 17, 2017

I/O Subsystem, Parallel Sysplex, STP, Security
PCIe Gen3 I/O fanouts with 16 GBps Buses
6 CSS, 4 Subchannel sets per CSS
0 – 5 PCIe I/O Drawer Gen3 (no I/O Drawer)
Next generation FICON Express16S+
10 GbE RoCE Express2
Integrated Coupling Adapter (ICA SR) and Coupling express LR for coupling links
Support for up to 256 coupling CHPIDs per CPC
CFCC Level 22
Crypto Express6S and CMPSC compression and Huffman Coding compression
STP configuration and usability enhancements (GUI)
IBM zHyperLink Express
OSA-Express6S
Secure Service Container

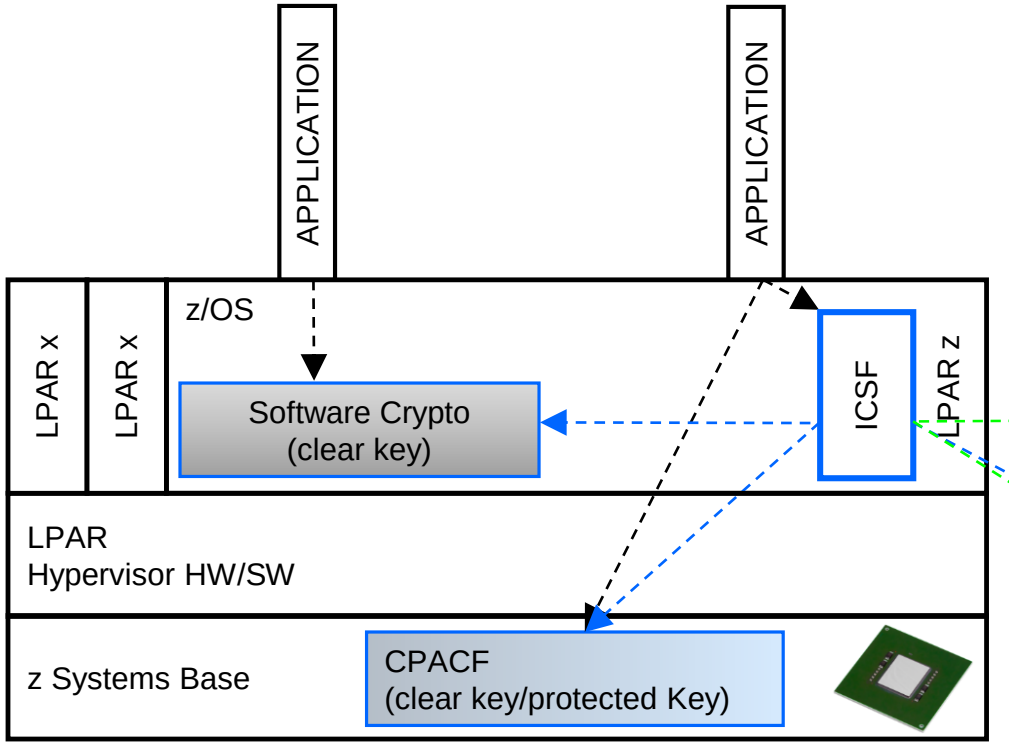
RAS, simplification and others	
L3 Cache Symbol ECC	**Acoustic and thin covers (space saving)**
N+1 radiator design for Air Cooled System	**Drop "Classic" HMC UI**
ASHRAE Class A3 design	**Enhanced SE and HMC Hardware (security)**
Support for ASHRAE Class A3 datacenter	TKE 9.0 LICC
Largesum TCP/IP hardware Checksum (OSA-Express6S)	Pause-less garbage collection
Universal Spare SCM s (CP and SC)	Simplified and enhanced functionality for STP configuration
Enhanced Dynamic Memory Relocation for EDA and CDR	Virtual Flash Memory (replaces IBM zFlash Express)

PR/SM
Up to 170 CPUs per partition
IBM Dynamic Partition Manager updates
Up to 85 LPARs
16 TB Memory per partition

Hardware Crypto support in IBM Z



Crypto support in IBM z14 (z/OS)



IBM z14

Software

TKE
Trusted Key Entry
(secure key)

HSM Crypto
(secure key & clear key)

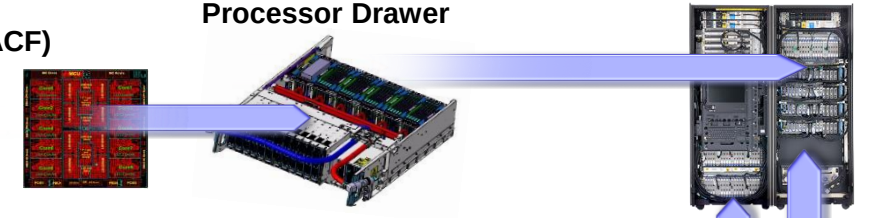
CPACF = Central Processor Assist for Crypto. Functions
ICSF = Integrated Cryptographic Service Facility

IBM System z - Hardware cryptographic implementation

Free but orderable

CP Assist for Cryptographic Functions (CPACF)

- A facility integrated in each PU
- Clear Key & Protected Key only
- Symmetric, hash, …



Optional Priced Feature

Crypto Express 6S (CEX6S)

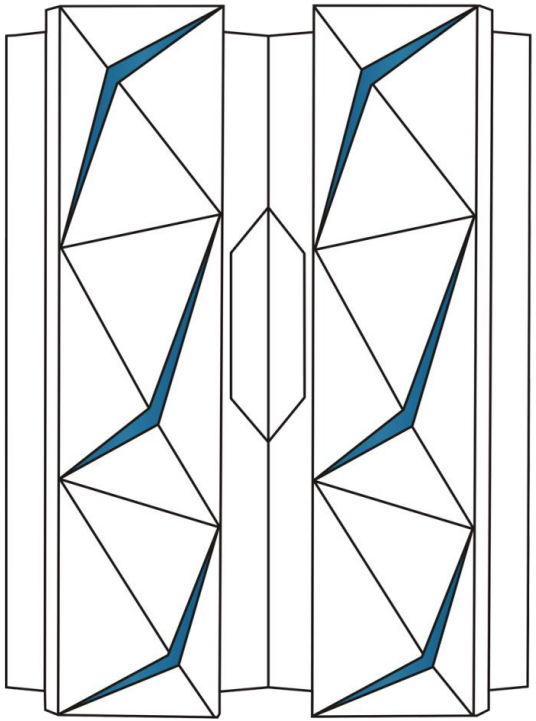
- 0-16 features in a system
- 1 secure **4768 coprocessors** per feature
- Secure key symmetric (DES, T-DES) and asymmetric (RSA)
- **PR/SM sharable**
- Manually configurable into an RSA accelerator
- Designed to meet Physical Security Standards like **FIPS 140-2 level 4** and **ANSI 9.97** (certification ongoing)

Three configuration options for the PCIe adapter:

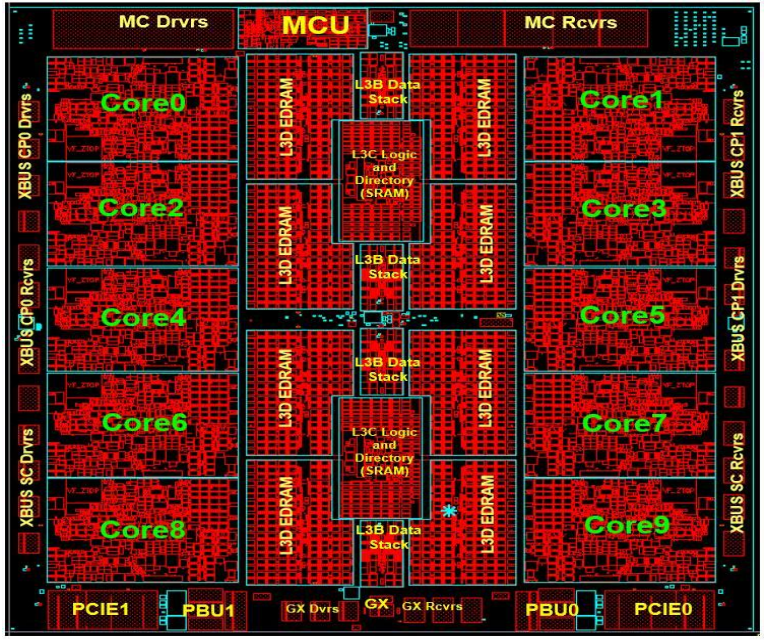
Accelerator	CCA Coprocessor	EP11 Coprocessor
Maximum Performance	*Maximum Security*	*PKCS#11 Compliance*

Table of Content

- z14 Cryptography
- CPACF
- Crypto Express6S
- Trusted Key Entry
- GDPR and Pervasive Encryption



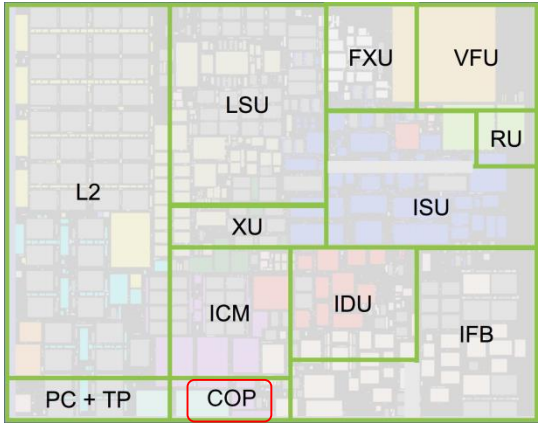
z14 processor design summary



- 6.1 Billion transistors
- 25.3 x 27.5 mm chip area
- 14nm SOI technology,
- 17 layers of metal
- 10 cores per CP-chip,
- 5.2GHz (4.5 GHz in z14 ZR1)

- Cache Improvements:
  - New power efficient logical directory design
  - 33% larger L1 I$ (128K)
  - 2x larger L2 D$ (4MB)
  - 2x larger L3 Cache with symbol ECC
- New Translation/TLB2 design
  - 4 concurrent translations
  - Reduced latency
  - Lookup integrated into L2 access pipe
  - 2x CRSTE growth
  - 1.5X PTE growth
  - New 64 entry 2gig TLB2
- Pipeline Optimizations
  - Improved instruction delivery
  - Faster branch wakeup
  - Reduced execution latency
  - Improved OSC* avoidance
  - Optimized 2nd generation SMT2
- Better Branch Prediction
  - 33% Larger BTB1 & BTB2
  - New Perceptron Predictor
  - New Simple Call Return Stack

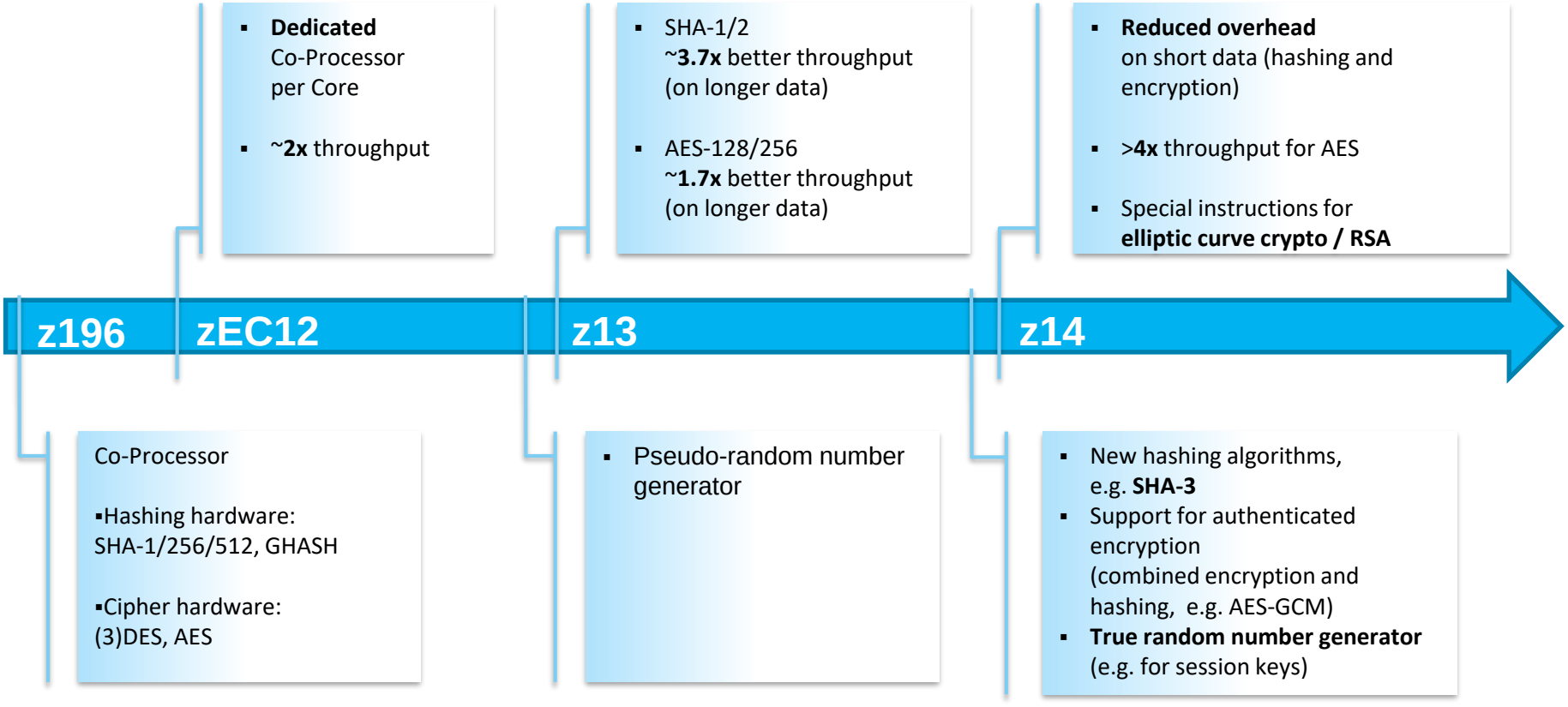
CPACF - CP Assist For Cryptographic Functions



Supported Algorithms	Clear Key	Protected Key
DES, T-DES	Y	Y
AES128	Y	Y
AES192	Y	Y
AES256	Y	Y
SHA3-224	Y	N/A
SHA3-256	Y	N/A
SHA3-384	Y	N/A
SHA3-512	Y	N/A
SHAKE-128	Y	N/A
SHAKE-256	Y	N/A
PRNG / DRNG	Y	N/A
TRNG	Y	N/A

- **Provides a set of symmetric cryptographic functions and hashing functions for:**
  - Data privacy and confidentiality
  - Data integrity
  - Random Number generation
  - Message Authentication
- **Enhances the encryption/decryption performance of clear-key operations for**
  - SSL
  - VPN
  - Data storing applications
- **Available on every Processor Unit defined as a CP, IFL and zIIP**
- **Supported by z/OS, z/VM, z/VSE, z/TPF and Linux on z Systems**
- **Must be explicitly enabled, using a no-charge enablement feature (#3863)**
  - SHA algorithms enabled with each server
- **Protected key support for additional security of H/ W protected keys over S/W protected cryptographic keys**
  - Crypto Express6S required in CCA mode

Crypto Functions in the Dedicated Co-processor – new for z14



- **New instruction added : KMGCM for end to end implementation of NIST GCM standard. (800-38D)**
- **KIMD / KLMD extended to implement SHA-3 standard. (FIPS 202)**
- **AES throughput improved to 3.5 to 4B/cycle**

Central Processor Assist for Cryptographic Function (CPACF)

Making Pervasive Encryption Affordable

- Feature Code 3863, No Charge
- Hardware accelerated encryption on every core with the Central Processor Assist for Cryptographic Function (CPACF) which is designed to provide faster encryption and decryption than previous servers.
- CPACF – 2-6X faster encryption than z13 of data in-flight and at-rest.
- Key Management requires Crypto Express5S/6S.

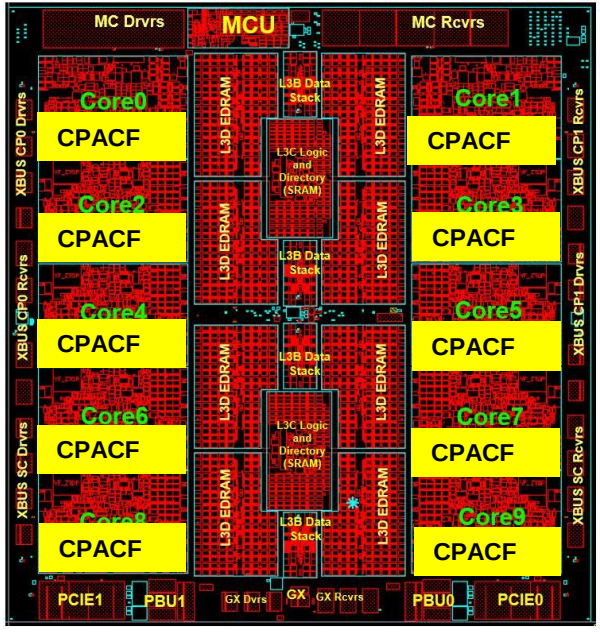
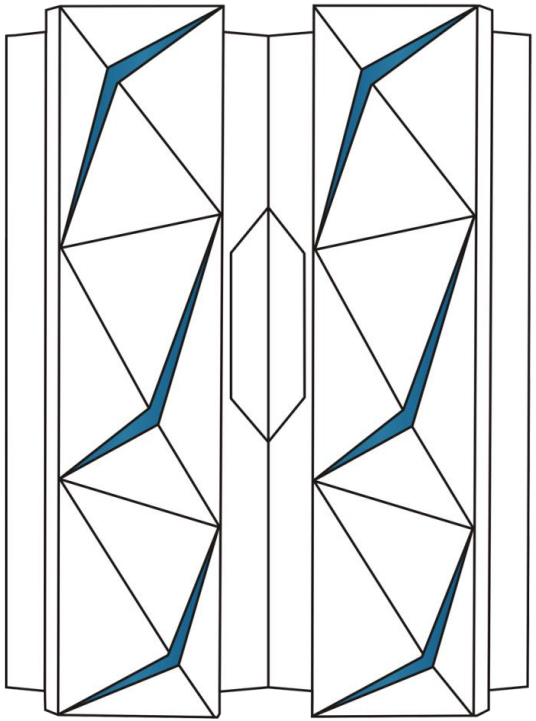


Table of Content



Cryptography Express6S

- One coprocessor per feature
  - Initial order – two features
- Up to 16 features per server
- Designed to be FIPS 140-2 Level 4 compliant
- Support for SHA-3
- Average, 1.5X to 2X performance increase over Crypto Express5S

Feature Code 0893

Three Crypto Express6S configuration options

- Only one configuration option can be chosen at any given time
- Switching between configuration modes will erase all card secrets
  - Exception: Switching from CCA to accelerator or vice versa

Accelerator		CCA Coprocessor		EP11 Coprocessor	
TKE	N/A	TKE	OPTIONAL	TKE	REQUIRED
CPACF	NO	CPACF	REQUIRED	CPACF	REQUIRED
UDX	N/A	UDX	YES	UDX	NO
CDU	N/A	CDU	YES(SEG3)	CDU	NO
Clear Key RSA operations and SSL acceleration		*Secure Key crypto operations*		*Secure Key crypto operations*	

"MiniBoot" is the secure code used to initialize the crypto card at power on. Provides additional trust there is nothing subversive buried in the card. Code moved from a firmware approach to a more secure hardware based method.

Cryptographic Primitives Supported in the ASIC

- Over **300** Cryptographic algorithms and modes supported directly in the hardware, including:
  - DES/TDES w DES/TDES MAC/CMAC
  - AES, AESKW, AES GMAC, AES GCM, AES XTS mode, CMAC
  - MD5, SHA-1, SHA-2 (224,256,384,512), HMAC
  - Visa Format Preserving Encryption
  - RSA (512, 1024, 2048, 4096)
  - ECDSA (192, 224, 256, 384, 521 Prime/NIST)
  - ECDSA (160, 192, 224, 256, 320, 384, 512 BrainPool)
  - ECDH (192, 224, 256, 384, 521 Prime/NIST)
  - ECDH (160, 192, 224, 256, 320, 384, 512 BrainPool)
  - Montgomery Modular Math Engine
  - Deterministic Random Number Generator
  - Prime Number Generator
  - Clear Key Fast Path (Symmetric and Asymmetric)

4768 Cryptographic Coprocessor

- Enhanced Performance
  - IBM PPC476 Processors @ 1.2Ghz (50% Improvement)
  - Modular Math Engines x2
  - Symmetric Key engines 50%
  - PCI Express Gen 2
- Enhanced Security
  - New Secure Boot Loader design
  - Persistent Memory Management supported through sidecar FPGA
- Improved Manufacturing Controls
  - Designed for PCI HSM and Common Criteria Certifications
  - Dual Control Secure Initialization during Manufacturing
  - Chain of custody reports

Security Certifications

- Physical Security Standards in progress/planned:
  - ✓ FIPS 140-2 level 4
  - ✓ Common Criteria EP11 EAL4
  - ✓ Payment Card Industry (PCI) HSM
  - ✓ German Banking Industry Commission (GBIC, formerly DK)

Note: PCI-HSM certification is new for Crypto Express6S. The others also apply to Crypto Express5S.

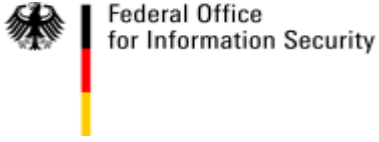
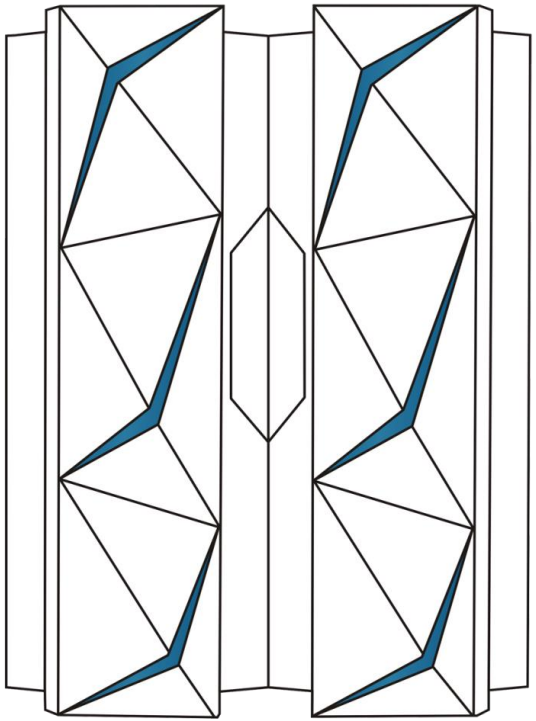


Table of Content

- z14 Cryptography
- CPACF
- Crypto Express6S
- Trusted Key Entry
- GDPR and Pervasive Encryption



The TKE Package

Base Feature:

- *TKE workstation* with a *Cryptographic Adapter*
- Running a version of the *TKE Licensed Internal Code (LIC)*

Additional Features: Smart card readers and smart cards

Smart cards and readers are required for some TKE functions

- Host module migration wizard
- Management of EP11
- **NEW:** Required for managing of PCI-HSM compliance mode

IBM Highly recommends using smart cards to hold key material

Why a TKE is required for Crypto Express6S

- **TKE has significant client value for both security and simplification when managing host crypto modules**

- **For Crypto Express6S, TKE provides the ability to do domain grouping, and Host Crypto Module cloning.**
  - Both of these options significantly reduce the time of deployment and brings a level of security one gets if not using TKE

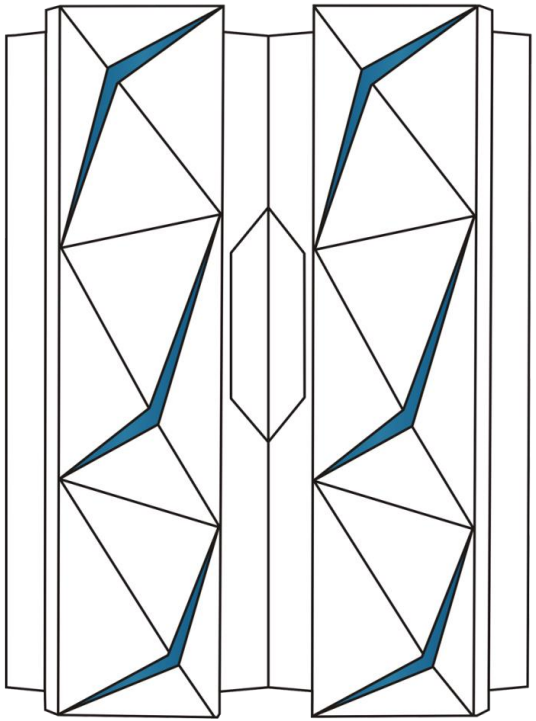
- **Benefit of using TKE:**
  - Easier to manage 85 domains without the benefit of domain grouping through the TKE.
  - TKE provides key part protection and dual control capabilities not available from ICSF
  - TKE can manage domains before the assigned LPAR is defined, or while the LPAR is inactive

- **For EP11 with Crypto Express6S TKE is required**

- **If a customer prefers not to have a TKE for Crypto Express6S and is comfortable with loading and then setting master keys in the clear from ICSF, they can continue to do that. Based on the value of the data being protected by the master key, this may not be appropriate. Customers can continue to operate Crypto Express6S BUT with no additional function.**

Table of Content

- z14 Cryptography
- CPACF
- Crypto Express6S
- Trusted Key Entry
- GDPR and Pervasive Encryption



Warum Datenschutz (und Verschlüsselung) ?

Eigeninteresse

Kundenvertrauen
Schutz von Kunden-/Unternehmensdaten
Sichere Kommunikation

IT Sicherheitsgesetz

Zielstellung
- Schutz kritischer Verfahren und Infrastrukturen
  - Verkehr, Energie, Information, Soziale Sicherungssysteme
  - Wasserversorgung, Ernährung
  - → KRITIS - Liste (ca. 2000 IT Dienstleister)

Anforderungen
- Einrichtung ISMS (BSI 100-1)
- Meldepflicht 24 x 7
- Nachweisbarkeit von Sicherheitsvorkehrungen

Betroffene
- Betreiber ‚Kritischer Infrastrukturen' (KRITIS)

Ergebnis
- Widerstandsfähigkeit gegen Angriffe
- Angriffe werden schneller erkannt und damit bekämpfbar

GDPR, BDSG/LDSG, TMG, ...

Europaweite Grundverordnung zum Datenschutz
- Privatpersonen
- Wirtschaft

Verbindlichkeit : Mai 2018

Überwiegend Ersatz länderspezifischer Gesetze (BDSG, LDSG)
- Aber Erwägungsgründe landespezifisch anwendbar !
- Folgeanpassungen erforderlich (TMG, VwVfG, VwGO,…)
- Zweckbindung und Zustimmungspflicht bleiben !
- Neu : Regularien für Löschung

§ 65/66 BDSG
Meldepflicht / Benachrichtigung
- Entbindung bei Vorkehrungen wie Verschlüsselungen

PCI DSS V.3.2

Seit 30. Juni 2015 für Alle verpflichtend, die personenbezogene Kartendaten akzeptieren, verarbeiten, speichern oder übermitteln

zwölf PCI-DSS-Anforderungen , u.a. :
3. Schutz der gespeicherten Daten der Kreditkarteninhaber
4. Verwendung von Verschlüsselung

A Paradigm Shift

From selective encryption to pervasive encryption

Encrypting only the data required to achieve compliance should be viewed as a minimum threshold, not a best practice.

The practice of pervasive encryption can:

- Decouple encryption from classification
- Reduce risk associated with undiscovered or misclassified sensitive data
- Make it more difficult for attackers to identify sensitive data
- Help protect *all* of an organization's digital assets
- Significantly reduce the cost of compliance

Pervasive encryption is the new standard

Pervasive Encryption with IBM z Systems

Enabled through full-stack platform integration

Integrated Crypto Hardware		Hardware accelerated encryption on every core – CPACF performance improvements of up to 7x Next Gen Crypto Express6S – up to 2x faster than prior generation
Data at Rest		Broadly protect Linux file systems and z/OS data sets[1] using policy controlled encryption that is transparent to applications and databases
Clustering		Protect z/OS Coupling Facility[2] data end-to-end, using encryption that's transparent to applications
Network		Protect network traffic using standards based encryption from end to end, including encryption readiness technology[2] to ensure that z/OS systems meet approved encryption criteria
Secure Service Container		Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest
Key Management		The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores.

1 Statement of Direction* in the z/OS Announcement Letter (10/4/2016) - http://ibm.co/2ldwKoC
2 IBM z/OS Version 2 Release 3 Preview Announcement Letter (2/21/2017) - http://ibm.co/2l43ctN

And we're just getting started …

Pervasive Encryption with IBM z Systems

Technical Foundation

z14 -- Designed for Pervasive Encryption

- CPACF – Dramatic advance in bulk symmetric encryption performance
- Crypto Express6s – Doubling of asymmetric encryption performance for TLS handshakes
- CFCC – Designed for CF data encryption (wrapped encryption key stored for recovery scenarios)

z/OS -- New approach to encryption in-flight and at-rest data

- z/OS data set encryption – Transparent encryption of data at-rest
- z/OS CF encryption –Transparent end-to-end encryption of CF data
- z/OS Communication Server - Intelligent Network Security discovery & reporting

Linux on z/LinuxONE -- Full Power of Linux Ecosystem combined with z14 Capabilities

- LUKS dm-crypt – Transparent file and volume encryption using industry unique CPACF protected-keys
- Network Security – Enterprise scale encryption and handshakes using z14 CPACF and SIMD
- Secure Service Container – Automatic protection of data and code for virtual appliance

zVM – **Encrypted paging support**
zTPF - Transparent database encryption (*available 8/2016*)

Software-only elements expected on previous generation of z Systems with differentiated value for z14

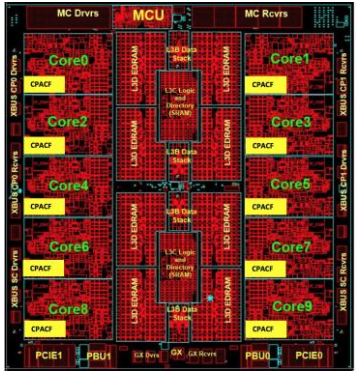
z14 Integrated Cryptographic Hardware

CP Assist for Cryptographic Functions (CPACF)

- Hardware accelerated encryption on every microprocessor core
- Performance improvements of up to 6x for selective encryption modes

Crypto Express6S

- Next generation PCIe Hardware Security Module (HSM)
- Performance improvements up to 2x
- Industry leading FIPS 140-2 Level 4 Certification Design

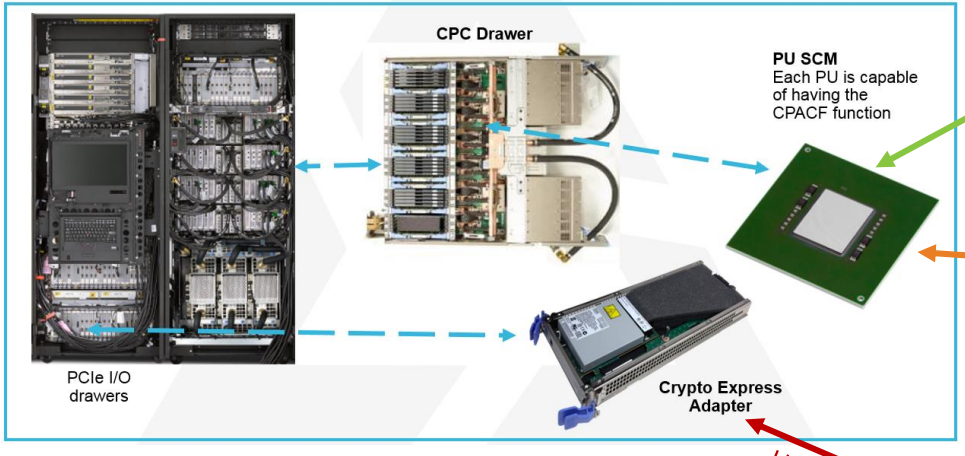


Why is it valuable:

- More performance = lower latency + less CPU overhead for encryption operations
- Highest level of protection available for encryption keys
- Industry exclusive “protected key” encryption

Understanding Clear, Secure and Protected Keys

- Secure keys have key values that are encrypted by a Master Key on a tamper-responding CryptoExpress adapter.



High speed

Clear Key

Key values are not encrypted. Crypto operations may be performed in CPACF or on a Crypto Express adapter

Speed & Security Hybrid

Protected Key

Key values are encrypted under a CPACF wrapping key. Crypto operations are performed only using CPACF

High security

Secure Key

Key values are encrypted under a Master Key. Crypto operations are performed only on a Crypto Express adapter

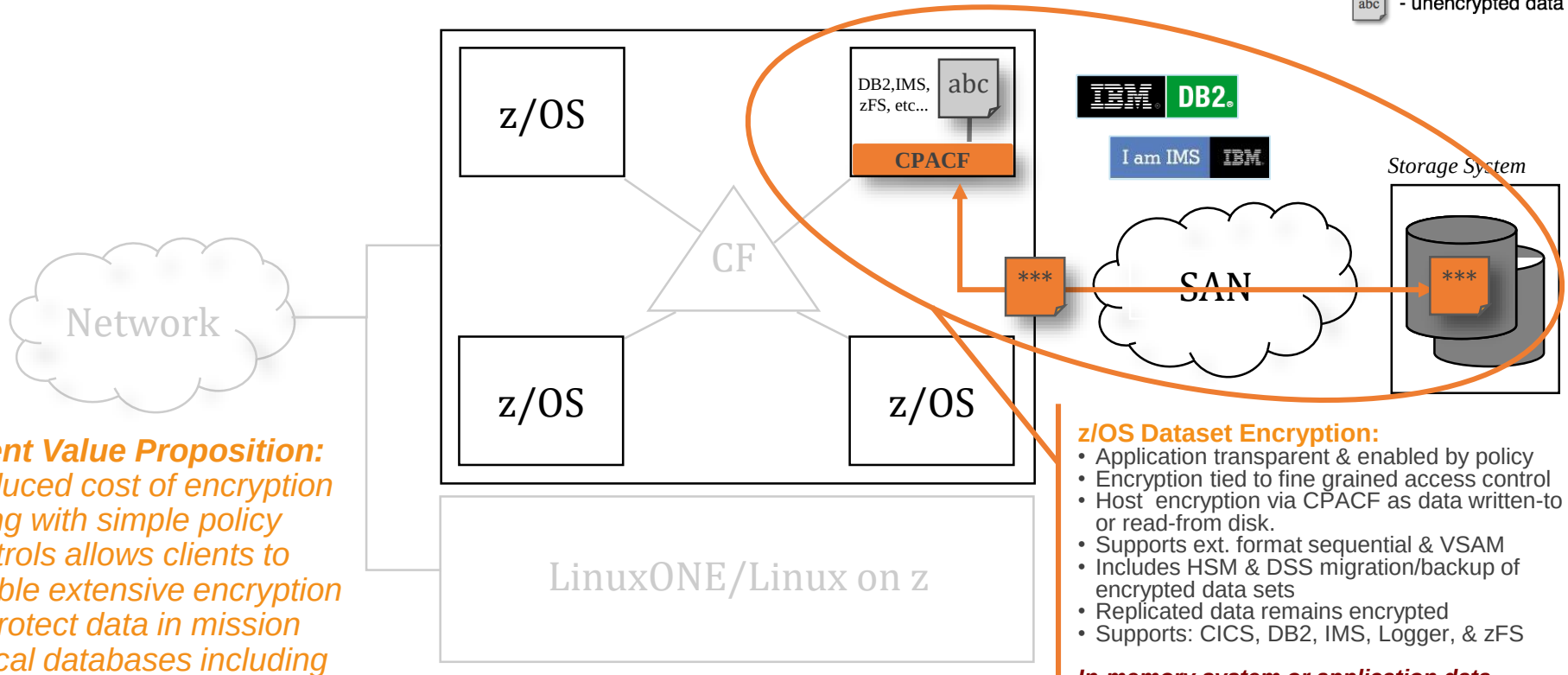
Only protected keys created from secure keys should be used for Pervasive Encryption.

Note: With z/OS data set encryption, protected keys are implicitly created from secure keys.

z/OS 2.2 & 2.3

Data Protection // z/OS Dataset Encryption

Protection of data at-rest



Client Value Proposition:
Reduced cost of encryption along with simple policy controls allows clients to enable extensive encryption to protect data in mission critical databases including DB2, IMS and VSAM

z/OS Dataset Encryption:
- Application transparent & enabled by policy
- Encryption tied to fine grained access control
- Host encryption via CPACF as data written-to or read-from disk.
- Supports ext. format sequential & VSAM
- Includes HSM & DSS migration/backup of encrypted data sets
- Replicated data remains encrypted
- Supports: CICS, DB2, IMS, Logger, & zFS

In-memory system or application data buffers will not be encrypted

z/OS Data Set Encryption

Hardware and Operating System Support

Product/Feature	Required Level	Description
Hardware		
Minimum HW	z196 CPACF	Minimum HW for AES-XTS (MSA-4)
	Crypto Express3	Minimum HW for Secure-key/Protected-key CPACF[1]
Recommended HW	z14 CPACF	AES-XTS CPACF performance improvements
	z14 Crypto Express6s	Crypto express performance improvements
Operating System – Base Support		
DFSMS	z/OS 2.3	Full support
	z/OS 2.2 + OA50569 PTFs	
	z/OS 2.1 + OA50569 PTFs	*Toleration only –read/write, cannot create encrypted data sets.*
RACF	z/OS 2.3	DFP segment key label and conditional access checking
	z/OS 2.1, 2.2 + OA50512 PTFs	
ICSF	HCR77C0 or HCR77C1	Protected-Key Read
	HCR77A0–B1 + OA50450 PTFs	

[1] – *Secure-key is STRONGLY RECOMMENDED for production environments. Clear-key may be used for dev/test.*

z/OS Data Set Encryption

Exploitation

Product/Feature	Required Level	Description
	Software Exploitation	
DB2	DB2 v12 + PTFs	Base exploitation + user interface enablement
	DB2 v11 + PTFs	Base exploitation
IMS	IMS v14	FF VSAM DB & OLDS - *test only no code changes expected*
	IMS v15	FP DEDB VSAM & WADS enablement support
CICS	*Supported CICS versions*	Test-only for user, CICS TS, and TD data sets
MQ	*NA*	*Recommendation for MQ - Advanced Message Security*
zSecure	zSecure 2.3	zSecure Audit & Admin support for z/OS data set encryption
zBNA	zBNA x.y.z	zBatch Network Analyzer support for z/OS data set encryption
	z/OS Exploitation	
zFS	z/OS 2.1 & 2.2	Toleration support
	z/OS 2.3	User Interface & data conversion support
System Logger	z/OS 2.3 w/RB 2.2 & 2.1	Media Manager enablement for logger data sets

Data Protection // Coupling Facility Encryption

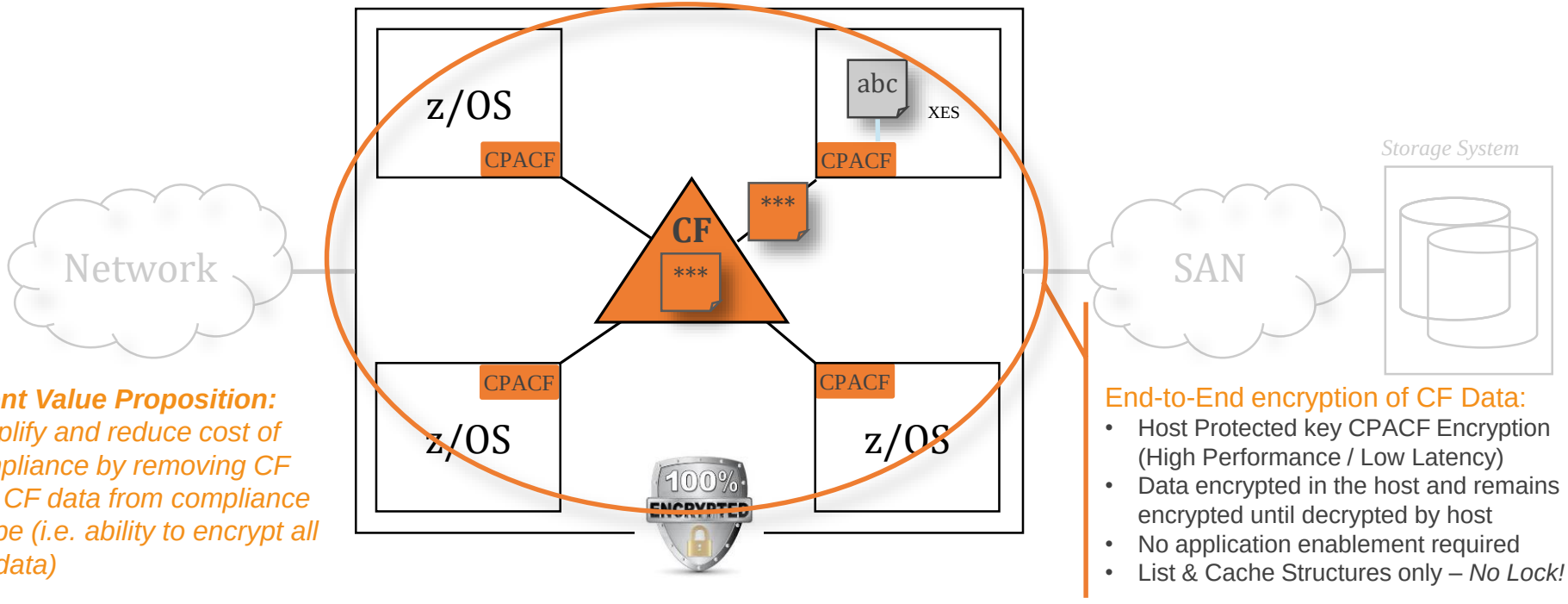
Protection of data in-flight and in-use (CF)

z/OS 2.3

Legend:

*** - encrypted data

abc - unencrypted data



Client Value Proposition:
Simplify and reduce cost of compliance by removing CF and CF data from compliance scope (i.e. ability to encrypt all CF data)

End-to-End encryption of CF Data:

- Host Protected key CPACF Encryption (High Performance / Low Latency)
- Data encrypted in the host and remains encrypted until decrypted by host
- No application enablement required
- List & Cache Structures only – *No Lock!*

CF Structure Encryption Requirements

z/OS V2.3:

Product/Feature	Required Level	Description
Hardware		
z/OS: Minimum HW	zEC12	Minimum supported for z/OS 2.3
	Crypto Express3	Required for Protected-key CPACF
z/OS: Recommended HW	z14	AES-CBC CPACF encrypt/decrypt performance improvements
CF: Recommended HW	z14	Simplified recovery for sysplex-wide CF reconciliation scenarios when using a new/changed CFRM couple dataset
Operating System – Base Support		
z/OS	z/OS 2.3	z/OS XCF/XES support for CF encryption
Additional Support		
zSecure	zSecure 2.3	zSecure Audit support for CF encryption
zBNA	zBNA	zBatch Network Analyzer support for CF encryption

Data Protection // z/OS Network Security

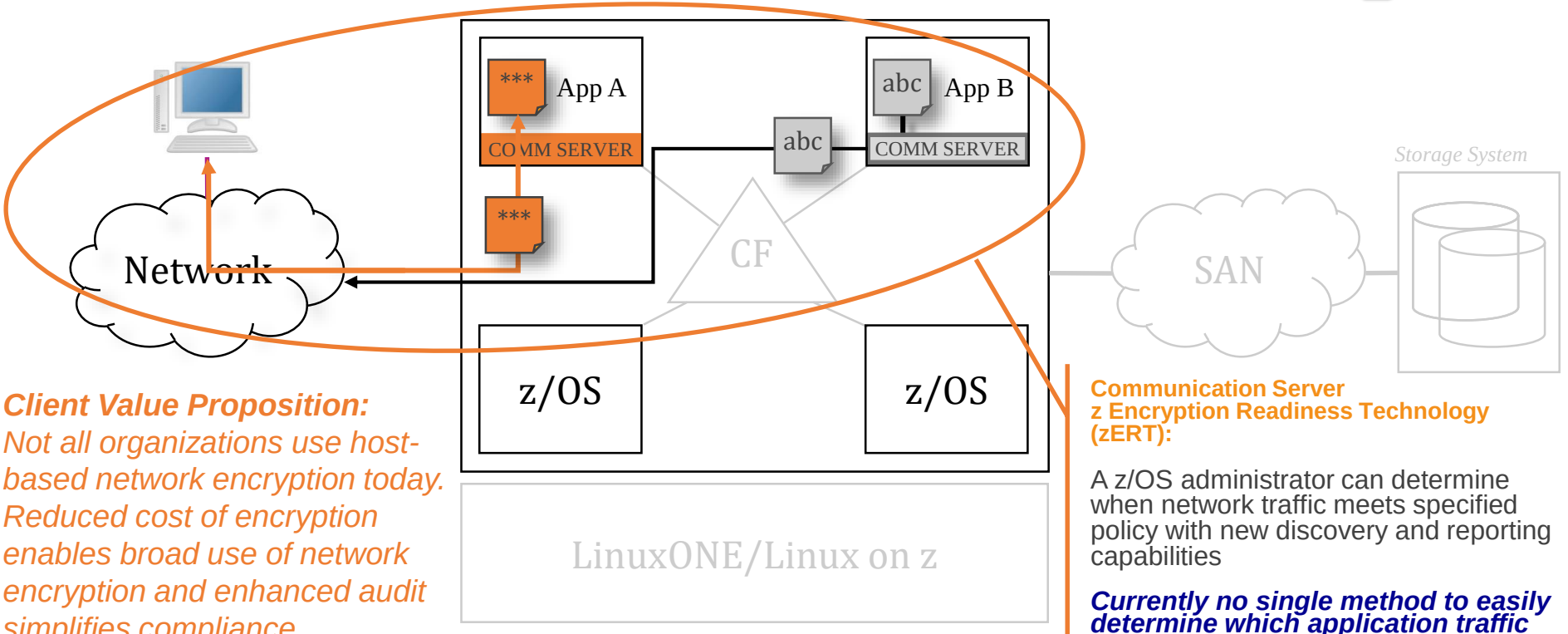
Protection of data in-flight

z/OS 2.3

Legend:

*** - encrypted data

abc - unencrypted data



Client Value Proposition:

Not all organizations use host-based network encryption today. Reduced cost of encryption enables broad use of network encryption and enhanced audit simplifies compliance.

Communication Server
z Encryption Readiness Technology (zERT):

A z/OS administrator can determine when network traffic meets specified policy with new discovery and reporting capabilities

Currently no single method to easily determine which application traffic patterns are protected

z/OS Communications Server

Hardware and Operating System Support

Product/Feature	Required Level	Description
Hardware		
Recommended HW	z14 CPACF	AES-GCM CPACF performance improvements
Operating System – Base Support		
z/OS Comm Server	z/OS 2.3	Provides zERT function
z/OS Exploitation		
System SSL	z/OS 2.3	zERT-enabled cryptographic protocol provider
OpenSSH	z/OS 2.3	zERT-enabled cryptographic protocol provider
Software Exploitation		
Connect:Direct	z/OS 2.3 + PTFs	Exploits SIOCSHSNOTIFY ioctl
zSecure	*TBD*	*Working with zSecure to be a consumer of zERT SMF records*
ISV Support		
ISVs	*As required by ISV*	*ISV enablement/compatibility support*

Sizing : Estimating CPU Cost of Data Protection

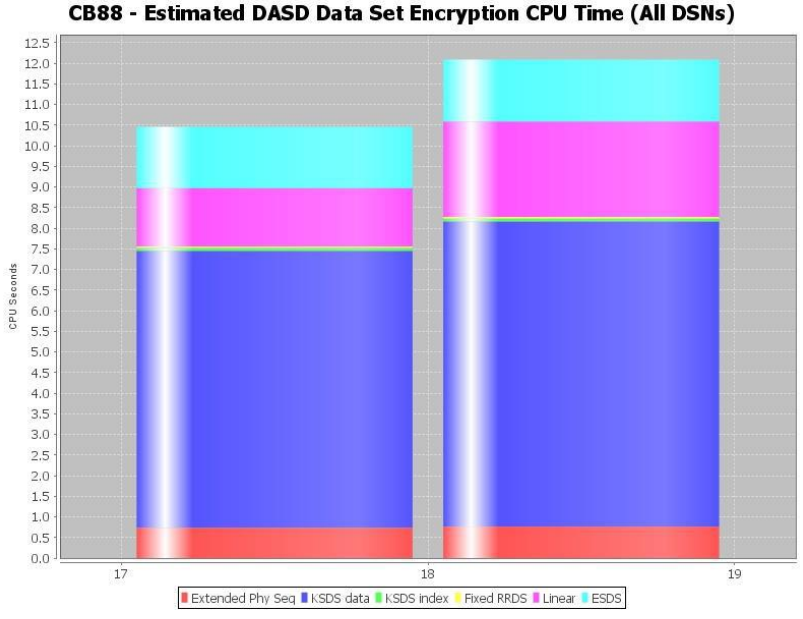
z Batch Network Analyzer (zBNA)

Background:

- A no charge, “as is” tool originally designed to analyze batch windows
- PC based, and provides graphical and text reports
- Available on techdocs for customers, business partners, and IBMers
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132
- Previously enhanced for zEDC to identify & evaluate compression candidates

Encryption Enhancements:

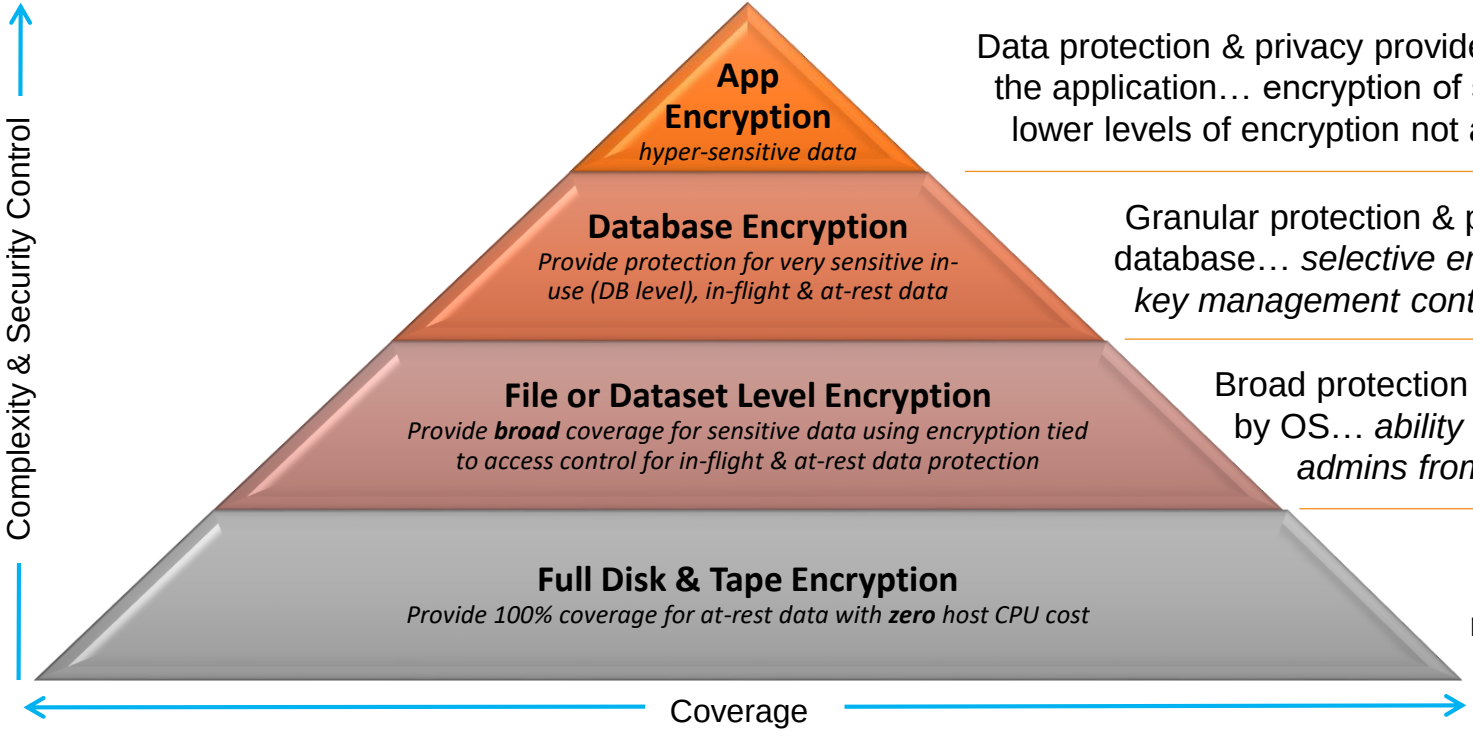
- zBNA will be further enhanced to help clients estimate encryption CPU overhead based on actual client workload SMF data
- Ability to select z13 or z14 as target machine (no EC12 !)
  - for z14 estimations APARs OA53718, OA53664 required
- Support will be provided for
  - z/OS data set encryption (DFSMS SMF 42.6 for pervasive encryption)
    - z/OS V2.1 and V2.2 require **OA52132**,
    - z/OS V2.3 requires **OA52734**
  - Coupling Facility encryption
    - z/OS V2.2 requires APAR OA51879 and APAR OA52003



There are three Data Set Encryption graphs.
Projected Data Set Encryption CPU Cost
Projected Data Set Encryption MIPS
Projected Data Set Encryption Gigabytes per Hour

Note: z/OS Capacity Planning tool zCP3000 also updated to provide encryption estimates
http://w3-03.ibm.com/support/americas/wsc/cpsproducts.html

Multiple Layers of Encryption for Robust Data Protection



Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Protection against intrusion, tamper or removal of *physical* infrastructure

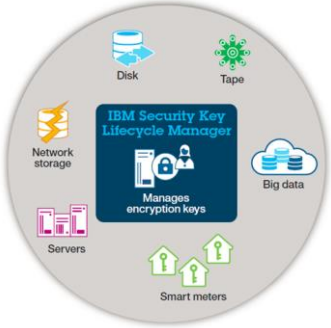
IBM Key Management Landscape…

ICSF

- Provides secure key storage with HSM protected keys (CKDS, PKDS, TKDS)
- Integrated with High Availability and Disaster Recovery Solutions
- Basic key *administration* primitives
- New ICSF CKDS Browser (HCR77C1)

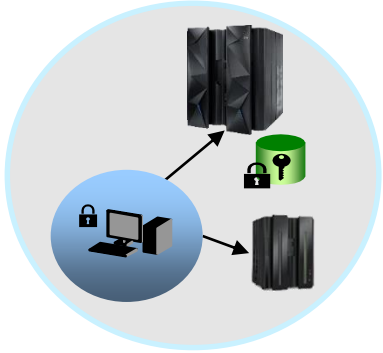
ISKLM - IBM Security Key Lifecycle Manager

- Primarily used for serving keys to storage devices (e.g. disk, tape)
- Supports IBM Proprietary Protocol (IPP) and OASIS Key Management Interoperability Protocol (KMIP)
- Available on z and distributed platforms
- Limited ability to manage keys in z Systems hardware key stores

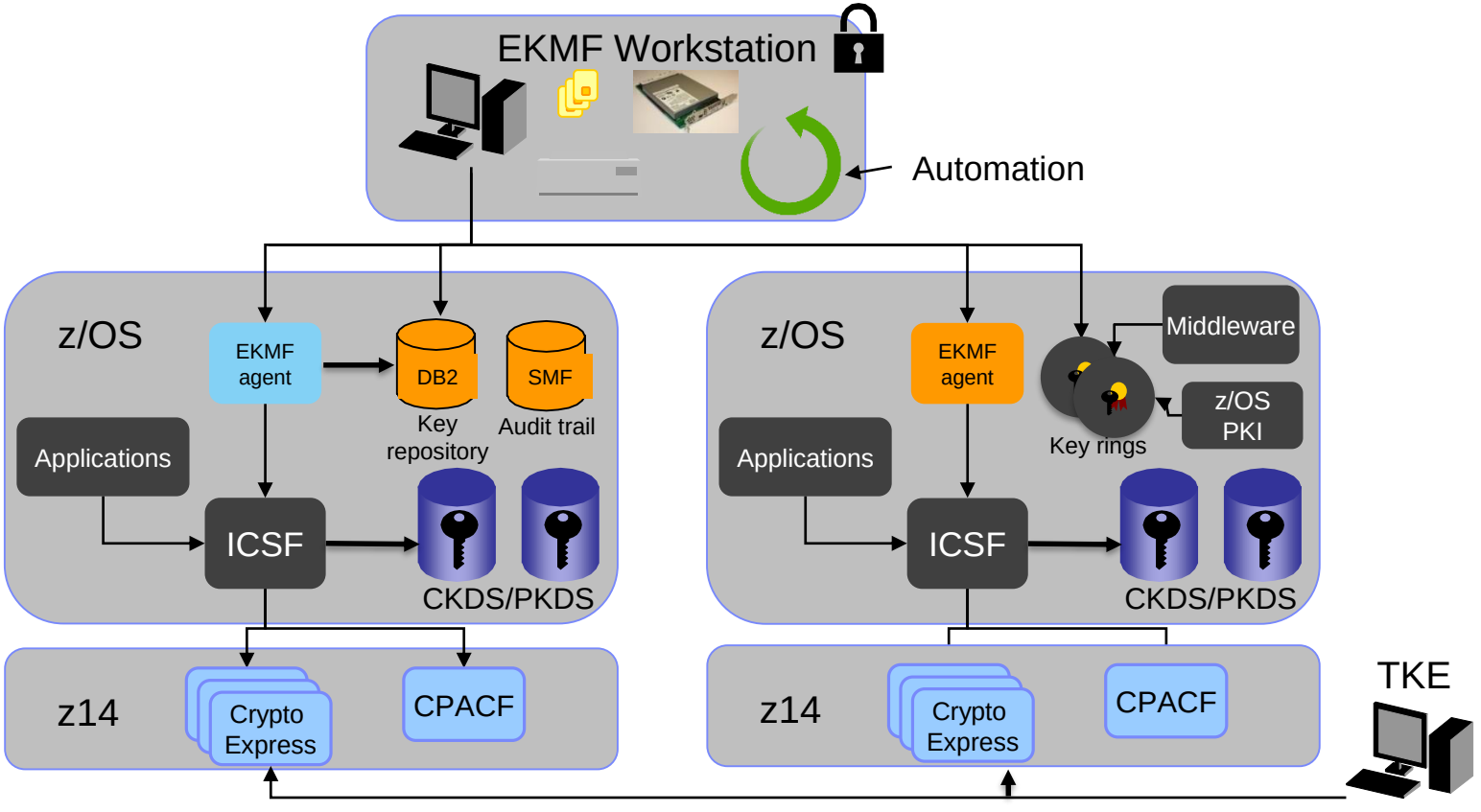


EKMF – IBM Enterprise Key Management Foundation

- Geared toward Banks, payment processors and other financial services
- Provides Multi-platform, multi-site & multivendor support key management
- Rich integration with z Systems hardware cryptography and key stores
- Robust backup and recovery capabilities
- Supports proprietary protocol for key distribution
- Delivered as a services offering



Architectural Overview – EKMF and zSystems crypto ecosystem



Data Protection // Secure Service Container

Extending the value of Z hardware crypto

Client Value Proposition:

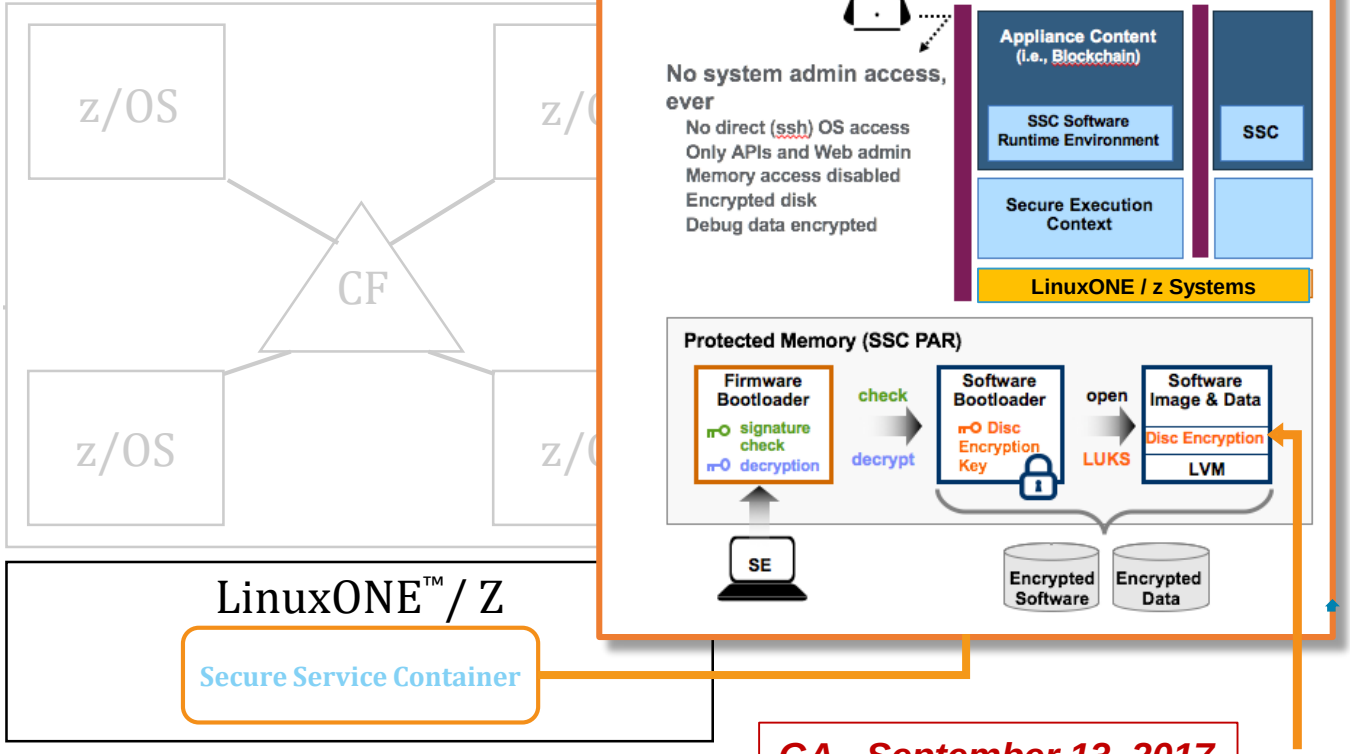
Simplified, fast deployment and management of packaged solutions

Tamper protection during Appliance installation and runtime

Confidentiality of data and code running within the Appliance both at flight and at rest

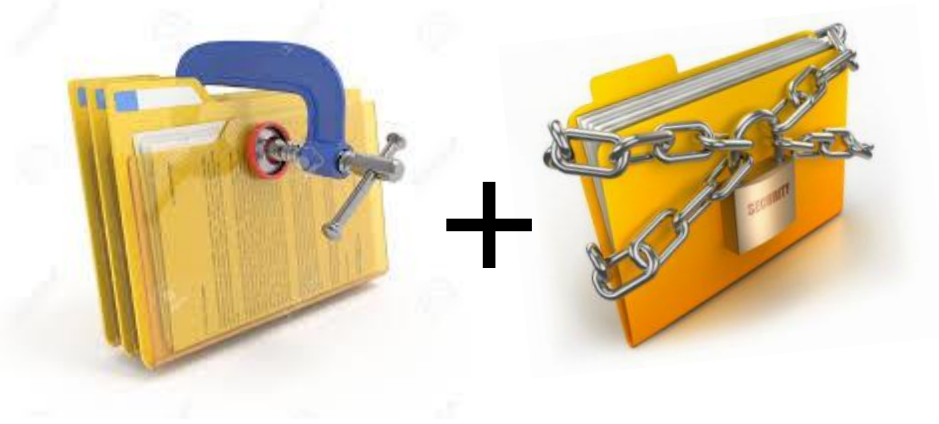
Restricts administrator access to workload and data

Secure Service Container architecture builds on the value z systems hardware crypto using a runtime environment designed to help clients reduce risk.



GA - September 13, 2017

Compression and Encryption



Encrypted data does not compress!

- Any compression downstream from encryption will be ineffective
- Where possible compress first, and then encrypt

z/OS data set encryption

- DFSMS™ will compress first (generic, tailored, enhanced, and zEDC) then encrypt
- Data sets will remain encrypted during HSM and DSS migration and backup processing
- Data sets will remain encrypted during hardware based data replication services

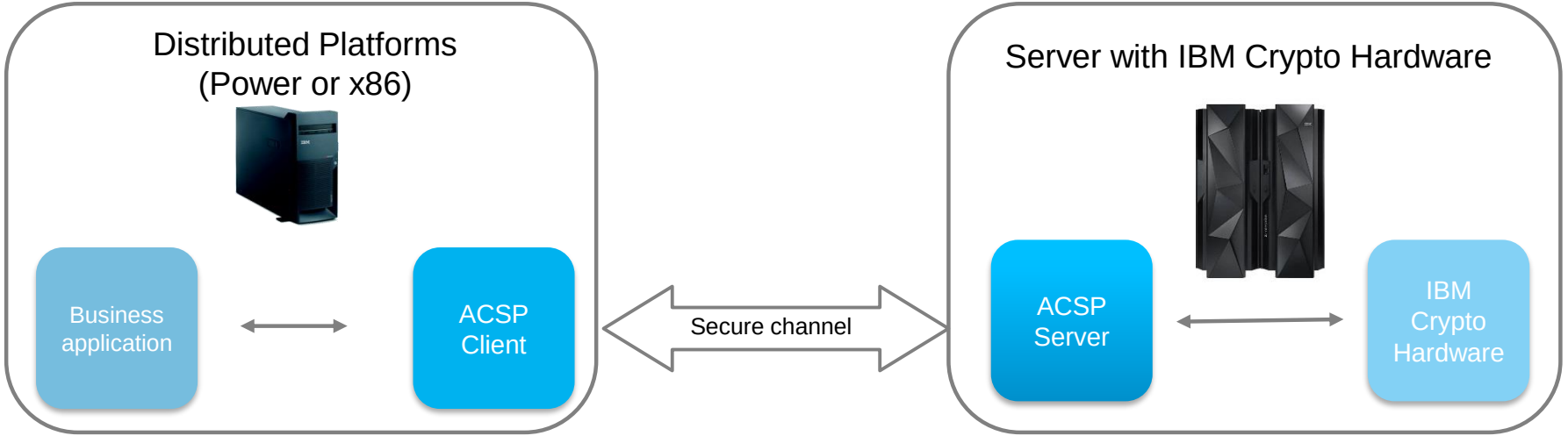
zEDC is expected to significantly reduce the CPU cost of encryption

- Great compression ratios (5X or more for most files)
- Less data to encrypt means lower encryption costs
- Compressed data sets use large block size for IO (57K)
- Applicable to QSAM, and BSAM access methods

Advanced Crypto Service Provider - ACSP

Capitalize on an existing scalable infrastructure and add security to new applications and platforms

- Mainframe centric security



More information

- IBM z Systems Security
  - http://www.ibm.com/systems/z/solutions/enterprise-security.html
- Redbooks
  - http://www.redbooks.ibm.com/
  - SG24-8410-00 Getting Started with z/OS Data Set Encryption
- Crypto Competency Center
  - http://www.ibm.com/security/cccc/
- Announcement Info
  - www.ibm.com/systems/zsolutions
- Demo Pervasive Encryption
  - https://www.youtube.com/watch?v=EP488nLdGts

More information

- Wiki mit div. Self Learning Elementen zu Crypto, TKE und z. B. dataset encryption
  - https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W7df80301055d_495b_bb88_a0a2f84757c5/page/Pervasive%20Encryption%20-%20zOS%20Data%20Set%20Encryption

- A technical document about the installation and configuration of data set encryption on z/OS.
  - This document (especially for beginner) starts from the configuration of the crypto card via the HMC to the final customization (PARMLIB, ICSF…)
  - http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102734

- YouTube video to explain all the process of the different keys involved in the data set encryption process
  - https://www.youtube.com/watch?v=TdGoTNIC-lc

- A power point presentation to explain the keys process. This presentation is the support of the video
  - http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5376

- Transporting AES encrypted data keys
  - http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102736

NEW Pervasive Encryption self-paced configuration walk-through

Available to you via the IBM Client Demonstration portal

The highly detailed step-by-step, fully illustrated documentation guides you through a pervasive encryption configuration. You become the IBM Z programmer and step through the configuration steps. Load a crypto card with your master key and use it to protect datasets of your choice. You will have an isolated z/OS LPAR with the necessary authority to perform the pervasive encryption configuration. Once configured, use a non-privileged userid to simulate real-world access violations and prove that pervasive encryption is properly configured.

Schedule the demonstration here.

https://www.ibm.com/systems/clientcenterdemonstrations/faces/dcDemoView.jsp?demoId=2783