

Pervasive Encryption for z/VM and Linux on Z

TechU



Brian W. Hugenbruch, CISSP
IBM Z Security for Virtualization & Cloud
z/VM Development Lab: Endicott, NY

 **@Bwhugen**



Data protection and compliance are business imperatives

***“It’s no longer
a matter of if,
but when ...”***

28%



Likelihood of an organization
having a data breach in the next 24
months ¹

European Union General Data
Protection Regulation (GDPR)



Payment Card Industry Data Security
Standard (PCI-DSS)

Of the **9.7 Billion** records
breached since 2013

only **4%** were encrypted ³



Health Insurance
Portability and
Accountability
Act (HIPAA)



\$3.6M

Average cost of a data breach in
2017 ²

1, 2 Source: 2017 Ponemon Cost of Data Breach Study: Global Overview -- <http://www.ibm.com/security/data-breach/>

3 Source: Breach Level Index -- <http://breachlevelindex.com/>

Implementing encryption can be complex

Comprehensive data protection requires a huge investment to deploy point solutions and/or enable encryption directly in the applications.



Organizations struggle with questions such as:

What

data should be encrypted?

Where

should encryption occur?

Who

is responsible for encryption?

Pervasive encryption: A paradigm shift in data protection

Protecting only enough data to achieve compliance should be the bare minimum, not a best practice.

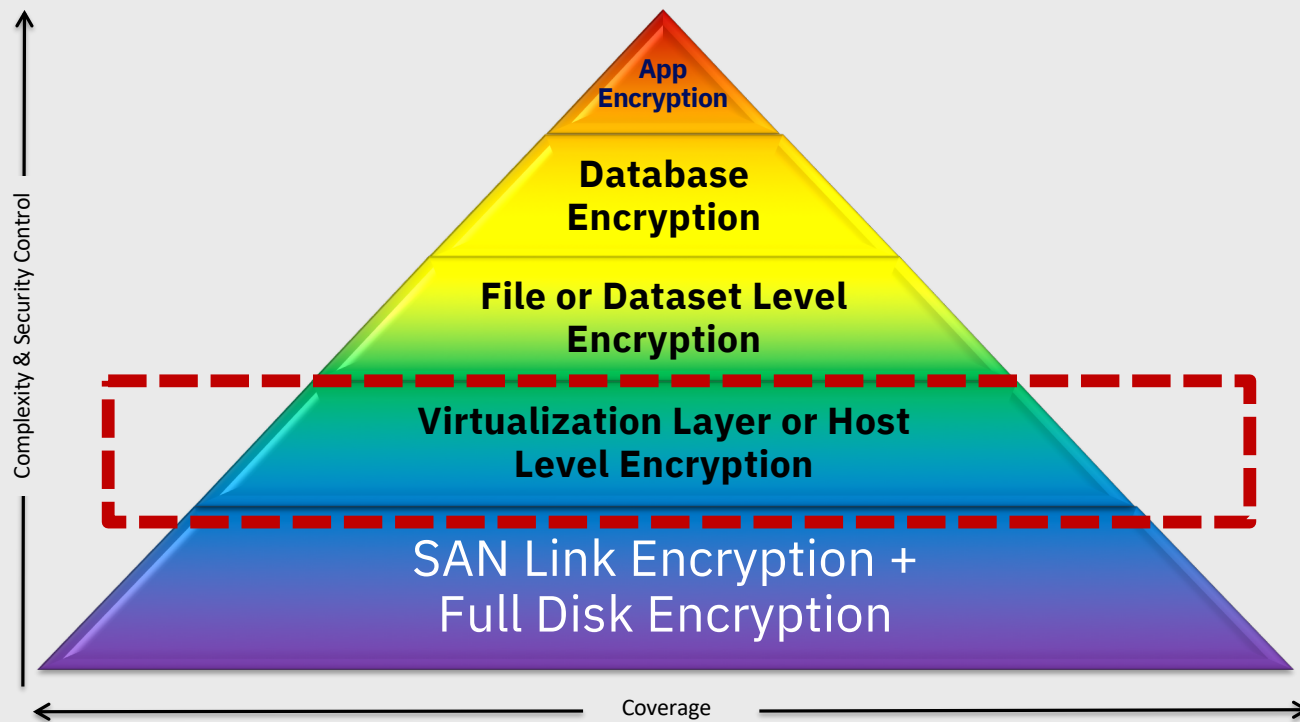
Focus on eliminating barriers:

- Decouple encryption from classification
- Extensive application changes
- Encryption of database indexes and/or key fields
- High cost associated with processor overhead



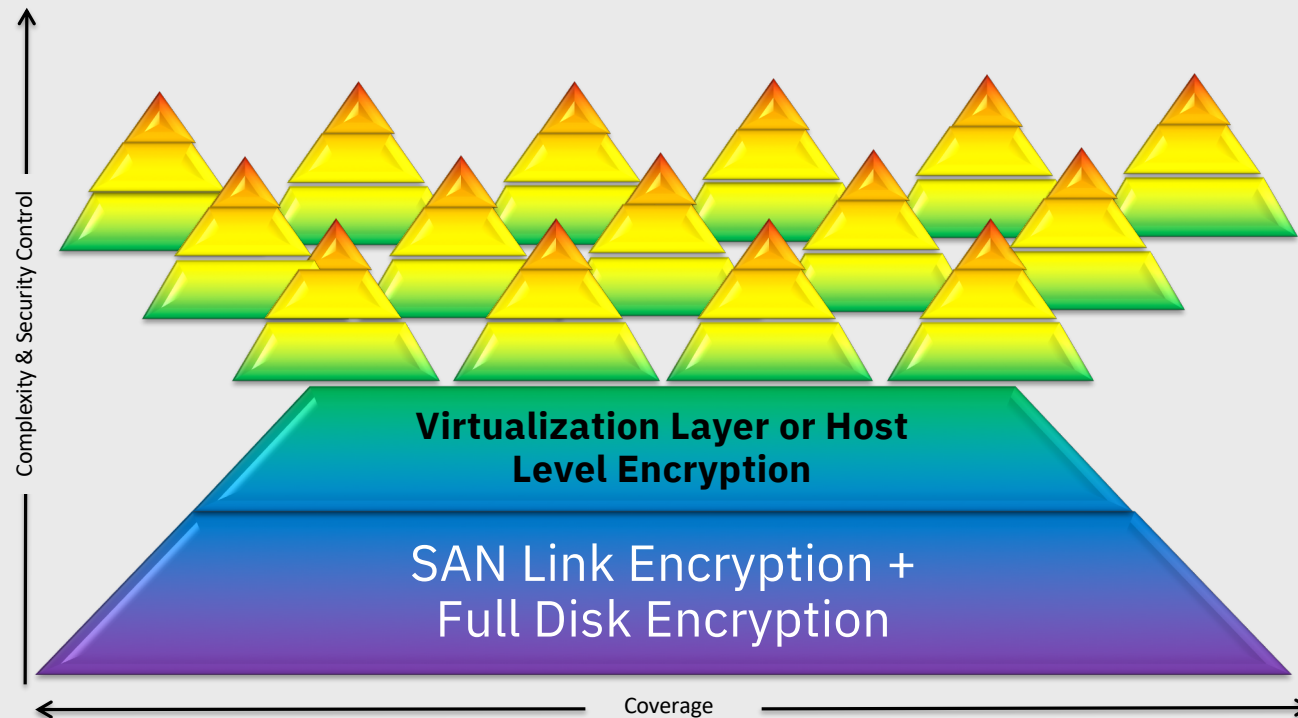
IBM Z Pervasive Encryption

From a Virtualization Point of View



IBM Z Pervasive Encryption

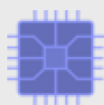
From a Virtualization Point of View



Pervasive Encryption with IBM Z and IBM LinuxONE

Enabled through tight platform integration

Integrated Crypto Hardware



Hardware accelerated encryption on every core, CPACF performance improvements of 7x
Crypto Express6S – PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor

Data at Rest



Broadly protect Linux file systems using policy controlled encryption that is transparent to applications and databases

Network



Protect network traffic using standards based encryption from end to end to ensure that 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

Pervasive Encryption for z/VM and Linux on IBM Z

IBM Z hardware – Designed for Pervasive Encryption

CPACF – Dramatic advance in bulk symmetric encryption performance

Crypto Express – Doubling of asymmetric encryption performance for TLS handshakes

z/VM – Virtualizing Encryption for Linux

Virtualization of IBM Z Crypto Hardware and **Dynamic Crypto management**

Crypto Express **acceleration** for encrypted data in flight

Encrypted Paging for z/VM

Linux on IBM Z – Full Power of Linux Ecosystem plus z14 Capabilities

dm-crypt – Transparent file & volume encryption using industry unique CPACF protected-keys

Network Security – Enterprise scale encryption and handshakes using z14 CPACF and SIMD

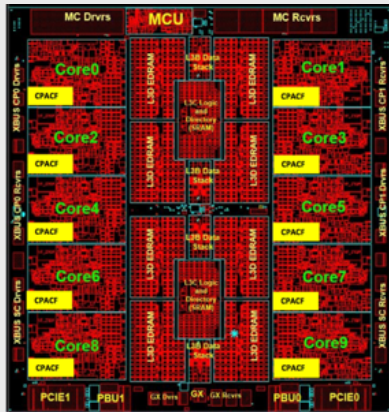
Secure Service Containers – Automatic protection of data and code for virtual appliance

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

Suited for high speed bulk symmetric encryption



Crypto Express6S

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

Suited for high value transactions, key protection and asymmetric acceleration

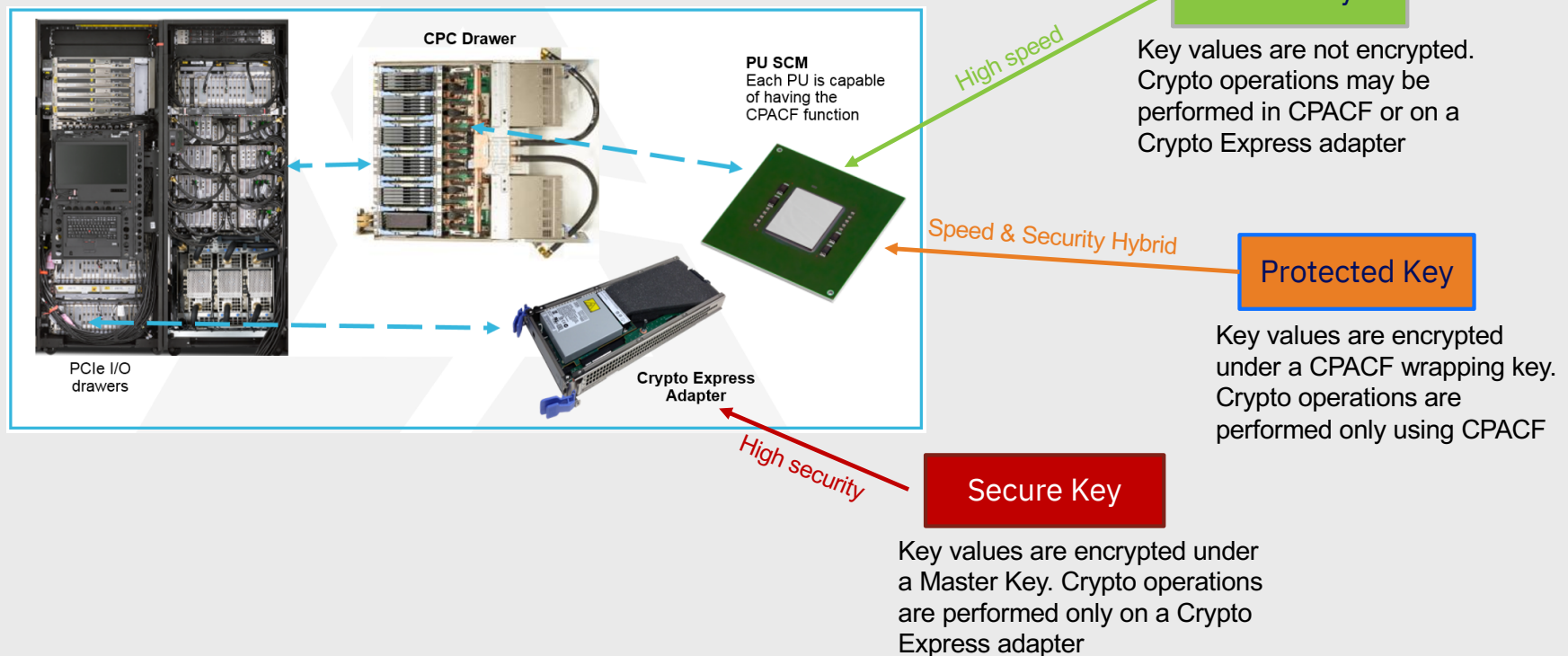
Why is it valuable:

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

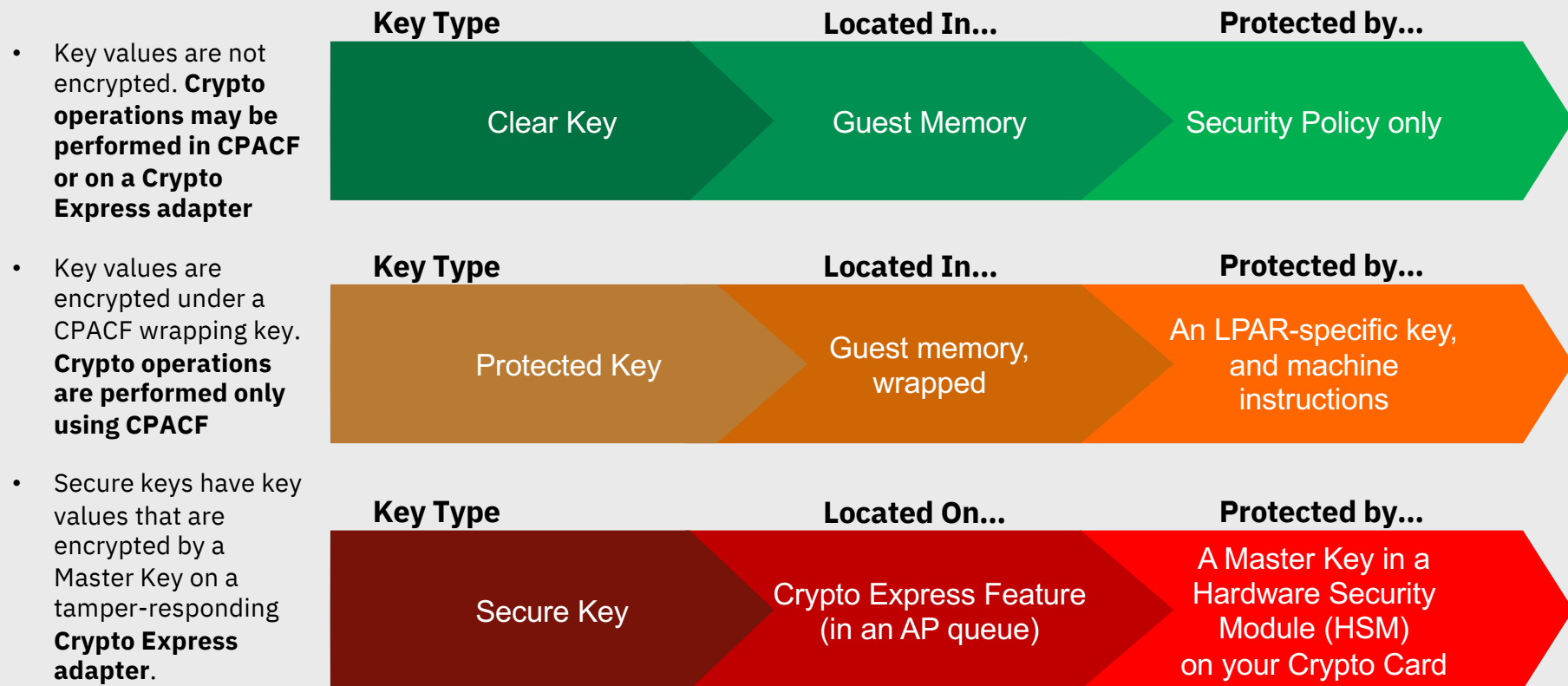


What are clear, secure and protected keys?

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



IBM Z Operational Keys: Explaining Clear, Protected, Secure



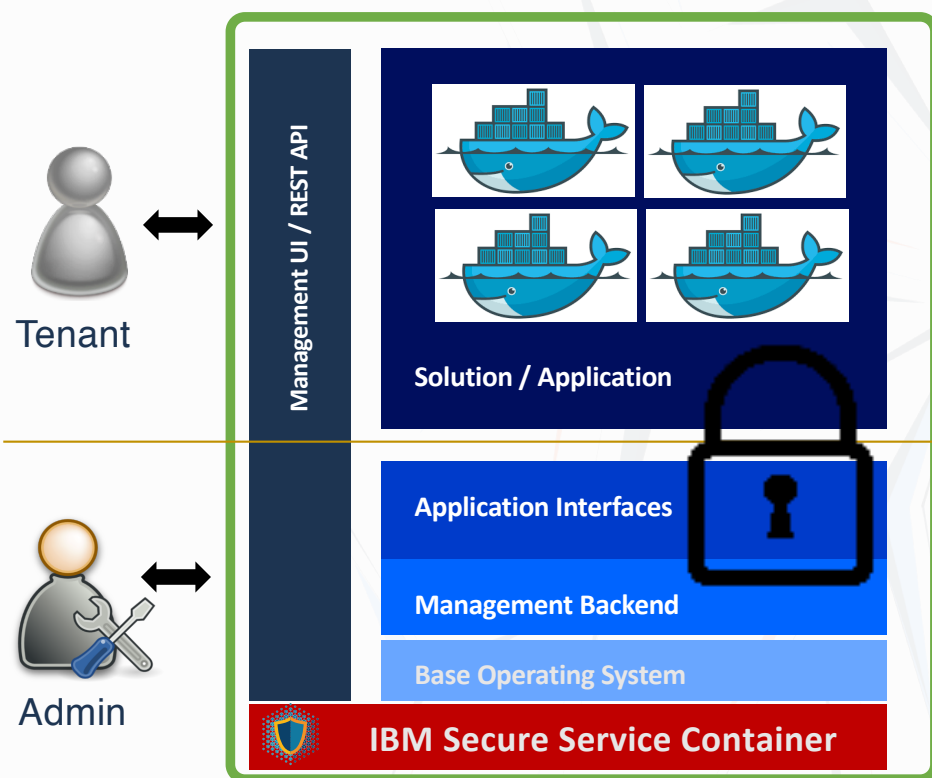
Secure Service Containers

IBM Secure Service Container (SSC)

- ✓ Platform-enforced **Confidentiality and Security** for the cloud
- ✓ Built-in tamper **resistance** and **pervasive encryption**
- ✓ Locks out **privileged users** for protection against abusive use of system admin or root user credentials

- Data and code in-flight, in-use and at-rest are inherently and pervasively encrypted by hypervisor
- Keys are held and managed in firmware
 - The System Admin is not required to be trusted
- No code changes to apps required
- Tamper proof application install
- No direct host or OS level interaction
 - Only well-defined bound and auditable interfaces

IBM Secure Service Container Appliance



IBM Secure Services Container

Secure Enclaves on LinuxONE

IBM Cloud Hyper Protect Services

- Mandatory encryption at rest, and transport
- Memory access disabled at firmware level
- Remove root access attack vector: no SSH

Crypto Services

Secure key storage: the industry's only cloud FIPS 140-2 Level 4 compliant service

DBaaS

MongoDB EE or PostgreSQL for secure data storage

Containers

Managed Kubernetes environment for applications

IBM Corporation www.ibm.com/cloud/hyper-protect-services



Secure Service Container for IBM Cloud Private

- Secure Service Containers now available on premise with IBM Cloud Private
- Deploy cloud-native workloads to Secure Service Containers



www.ibm.com/us-en/marketplace/secure-service-container



Secure Service Container Set-Up (at Partition Level)

<https://www-01.ibm.com/support/docview.wss?uid=isg2bb79df265313634d85258088005188e3&aid=1>

Configure partition
Configure logon
Configure networks
Activate partition

Customize Image Profiles: RACKSE27:ZAWARE2 : ZAWARE2 : SSC

RACKSE27:ZAWARE2

- ZAWARE2**
 - General
 - Processor
 - Security
 - Storage
 - Options
 - Crypto
 - SSC**

Boot selection:

- ☒ Secure Service Container installer
- ☐ Secure Service Container

Master user ID:

Master password:

Confirm master password:

Host name:

Network Adapters

--- Select Action ---

Select	CHPID	VLAN	IP address	Mask/Prefix

Default gateway:

DNS Servers

--- Select Action ---

Select	IP address

Cancel Save Copy Profile Paste Profile Assign Profile Help

Secure Service Container Set-Up (at Partition Level)

<https://www-01.ibm.com/support/docview.wss?uid=isg2bb79df265313634d85258088005188e3&aid=1>

Configure partition
Configure logon
Configure networks
Activate partition

New Partition - RACKPR27

Welcome

- Name
- Processors
- Memory
- Network
- Storage
- Accelerators
- Cryptos
- Boot
- Summary

Provide a name and description for the partition.

• Name:

Description:

Partition Type:

Provide a master user ID and password to use when logging in to the SSC web interface.

• Master User ID:

• Master Password:

• Confirm Master Password:

Secure Service Container Management (Sample Web UI)

<https://www-01.ibm.com/support/docview.wss?uid=isg2bb79df265313634d85258088005188e3&aid=1>

Login


Welcome to IBM HyperProtect Cryptographic Services (ACSP)

Please login with your credentials.

User ID*

Forgot your password?


Login





This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license


IBM HyperProtect Cryptographic Services (ACSP) V2.0.12


admin Log out



CryptosCard



Log



Networks


Security


Storage


Ex-/Import


Dumps


Maintenance

Invoke Installer

Reboot to the Installer to install new Appliances or update an existing installation. The current Appliance will be overwritten. This will interrupt Appliance operation.

Important: To login to the Installer after reboot you have to connect to the UI with the network settings and credentials provided by your system administrator.

Installer

Secure Service Container Management (Sample Web UI)

<https://01.ibm88e38>

CryptoCard

Log

Networks

Security

Storage

Ex-/Import

Dumps

Maintenance

Network Connections

Filter

Name	Status	Type	Device
vlan001a0.503	<div></div>	vlan	vlan001a0.503
enc1a0	<div></div>	802-3-ethernet	enc1a0

Total: 2 Selected: 0

1

CryptoCard

Log

Networks

Security

Storage

Ex-/Import

Dumps

Maintenance

Users

Groups

Roles

Requests

Configured Users

Filter

[administrator_acsp](#)

User Details

Name: administrator_acsp

Roles

Groups

Explicitly assigned:
ACSP Administrator

Inherited from groups:
Groups Roles

CryptoCard

Log

Networks

Security

Storage

Ex-/Import

Dumps

Maintenance

Cryptographic Devices

Filter

Total: 2 Selected: 0

1

CryptoCard

Log

Networks

Security

Storage

Ex-/Import

Dumps

Maintenance

Capabilities of Crypto Card

Crypto Card

Domain Name
card02.0000

Card Type
CEX6C

Card Mode
CCA-Coproc

Hardware type
12

Hardware function facilities
0x92800000

Enabled capabilities of crypto card

RSA 4K Clear Key

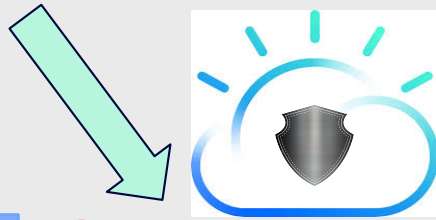
CCA Secure Key (full function set)

Long RNG

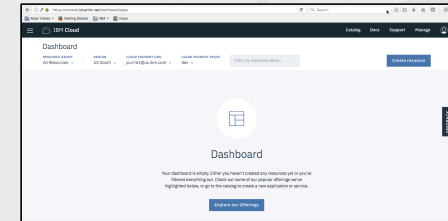
IBM Z services now offered through IBM Cloud

“Hyper Protect Platform Services”

IBM Z differentiation in the IBM Cloud.



IBM Cloud Dashboard



Customer Experience

Developer Experience (e.g. - Developer Starter Kit, Mobile, etc)

Platform Services



Security Services
(e.g. - Hyper Protect Crypto Services and Key Management)



mongoDB



PostgreSQL

Data Services
(e.g. – Hyper Protect DBaaS)



Docker and Kubernetes

Cloud Native Application
(e.g. Hyper Protect Containers Including Runtimes)

Infra

Hyper Protect Compute Services – Deployed globally in IBM Cloud



Create an HSM as a Service

IBM Cloud

← View all

Hyper Protect Crypto Services

Lite

Experimental

Attention: This service is experimental. It might not yet be stable and might change in ways that make it incompatible with earlier versions. This service is not recommended for production environments.

IBM Cloud Hyper Protect Crypto Services is a complete set of encryption and key management services backed by IBM Z technology. These services bring the security and integrity of IBM Z to the cloud. The same state of the art cryptographic technology relied upon by banks and financial services is now offered to cloud users via IBM Cloud. The network addressable Hardware Security Module provides safe and secure PKCS#11 cryptography via industry standard open source application programming interfaces. It supports secure key operations and random number generation via IBM Z cryptographic hardware, FIPS-140-2 level 4 certified technology. This is the industry's first and only FIPS 140-2 Level 4 certified technology in the public cloud market today and is the same technology that is the backbone of the IBM Enterprise Blockchain solution.

[View Docs](#) [Terms](#)

AUTHOR

IBM

PUBLISHED

05/30/2018

TYPE

Service

Service name:

MyHSM

Choose a region/location to deploy in:

US South

Select a resource group:

Default

Pricing Plans

Monthly prices shown are for country or region: [Germany](#)

PLAN	FEATURES	PRICING
✓	<div>Hyper Protect Crypto Services - 10 Crypto Slots Lite Plan</div> <div>This Lite Plan enables you to use Hyper Protect Crypto Services for free as an Experimental offering</div> <div>Lite plan services are deleted after 30 days of inactivity.</div>	Free

Need Help?

[Contact IBM Cloud Sales](#)

Estimate Monthly Cost

[Cost Calculator](#)

Create

Hyper Protect Crypto Services

IBM Cloud Hyper Protect Crypto Services provides cryptographic functions from a high level of security.

Lite

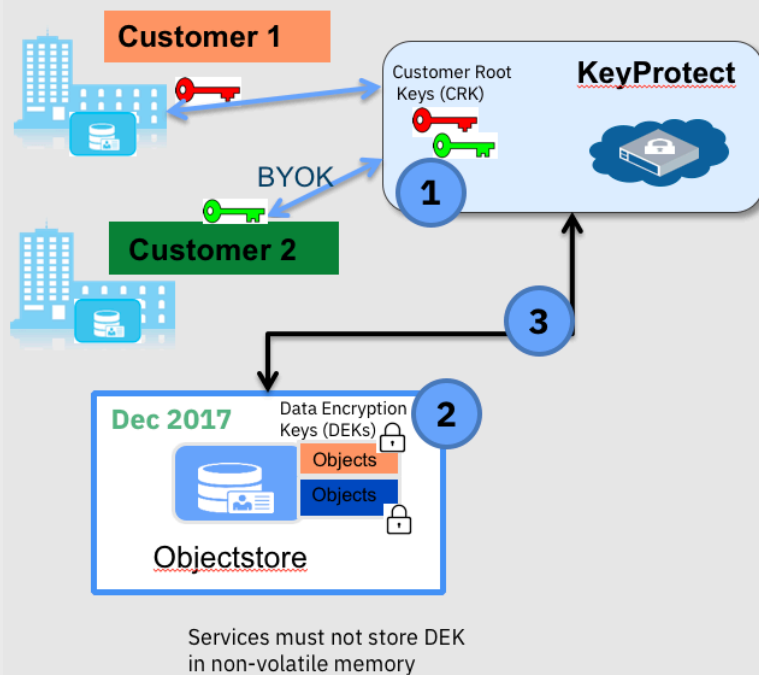
Experimental

FEEDBACK

Managing Keys in IBM Cloud: Key Protect

Encryption Keys Used for Integration with Storage and Data Services









All crypto operations performed within HSM



1. **CRK (Customer Root Key)**: generated by the customer and imported or generated by Key Protect. CRKs are always encrypted when stored outside of HSM. It is not in clear text outside the HSM. All crypto operations involving this customer key happens within the HSM boundary
2. **DEK (Data Encryption Key)**: used by data/storage services to encrypt customer data. This is always stored in encrypted form - encrypted with CRK.
3. Through **envelope encryption**, services request Key Protect to wrap or unwrap their DEKs with the CRK
4. Services can safely store wrapped DEKs along with their encrypted data and destroy the original unwrapped DEK

With Secure Service Container technology ...

What does it cost to plan, configure, implement and/or maintain?

High Cost								
Medium Cost								
Low Cost	 People	 Skills	 Ongoing maintenance	 Application lifecycle	 Application outages to implement encryption	 Updates for regulatory changes	 Key management	 New business requirements

z/VM Encrypted Paging



Bringing Pervasive Encryption to z/VM

Bringing Pervasive Encryption to z/VM involves

Ease of use needs to be mandatory

Client interviews and feedback a must

Enablement of **hardware facilities for guest usage**

z/VM is a virtualization platform first and foremost.

Encryption of security-pertinent hypervisor components

... but which ones?

Question of **security policy** vs. **performance** vs. **risk**

z/VM Support of z14 Cryptographic Hardware

PTF for APAR VM65942

New CPACF facilities and Crypto Express6S orderable features

- CPACF now includes TRNG and AES GCM
- Some fantastic performance benefits over previous hardware

Elliptic Curve Cryptography for Shared Crypto Domains ("APVIRT")

- All domains assigned to the CP-managed queues must be CCA coprocessors
- No change to dedicated crypto domains – those function as before
- Accelerates use of elliptic curve crypto for Linux or z/OS guests

– For more information, see the z14 Announce Letter at:

<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS117-044&appname=USN>

z/VM Support of z15 Cryptographic Hardware

PTF for APAR VM66248 -- refer to <http://www.vm.ibm.com/service/vmreqz15.html>

New CPACF facilities and
Crypto Express7S orderable
features

Service implications when
operating in an SSI with
multiple z/VM release levels
and/or hardware levels

z/VM APAR table

APAR	z/VM 6.4	z/VM 7.1	Description
VM66248	✓	✓	Support for new hardware facilities
VM66283	✗	✓	z/VM System recovery boost
PI99085	✓	✓	TCP/IP support for OSA-Express7S Adapter
VM66239	✓	✓	IBM z15 HCD support
VM66318	✓	✓	LinuxONE III HCD support
VM66206	✓	✓	Fix for AP Crypto messages may be lost during relocation
VM65976	✓	7.1 base	LGR Support for ESA/390 removal
VM65952	✓	✓	EREP/VM support
VM65266	✓	7.1 base	z/VM support of a 3906 processor
VM65598	✓	✓	VMHCM support
VM66240	✓	✓	z/VM IOCP update
PH00902	✓	✓	New HLASM hardware instructions
PI46151	✓	✓	ICKDSF Stand alone version z/Architecture support

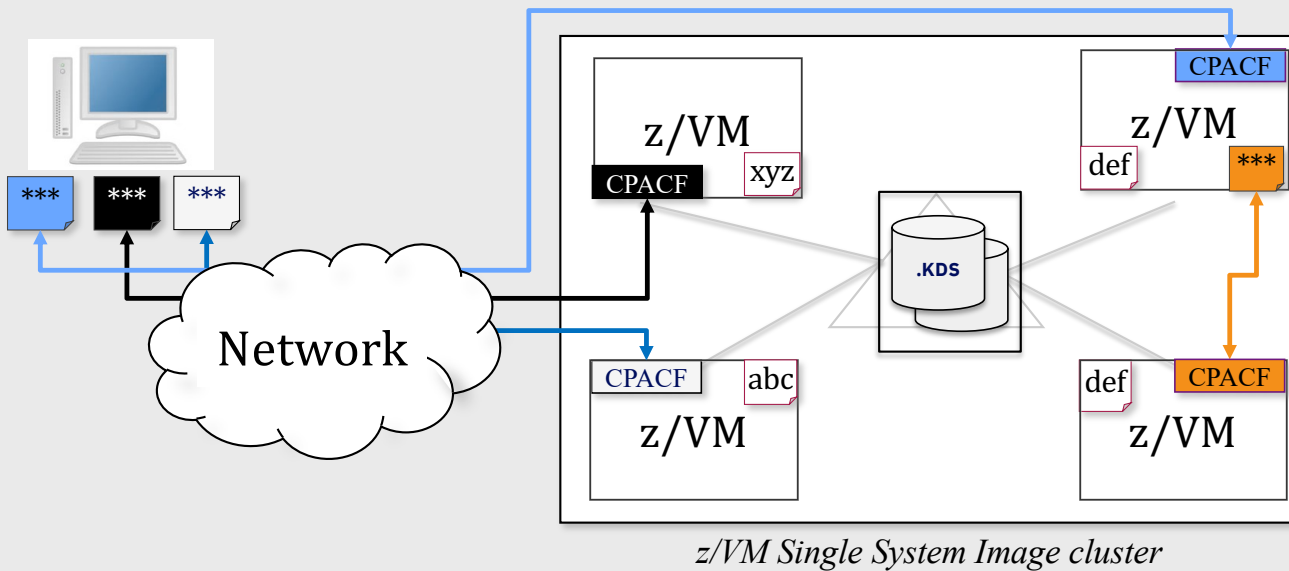
Data Protection // z/VM Network Security

Protection of data in-flight

z/VM 6.4
PTF for APAR PI72106

Legend:

*** - encrypted data
abc - unencrypted data



z/VM Secure Communications

- **Threat:** disclosure of sensitive data in flight to the hypervisor layer
- **Solution:** encrypt traffic in flight.

Notes:

- Automatic use of CPACF for symmetric algorithms
- One-line change to enable automatic use of Crypto Express features for acceleration of asymmetric algorithms
- Built on System SSL and ICSFLIB for z/VM

Client Value Proposition:

Not all organizations use host-based network encryption today ... reduced cost of encryption enables broad use of network encryption

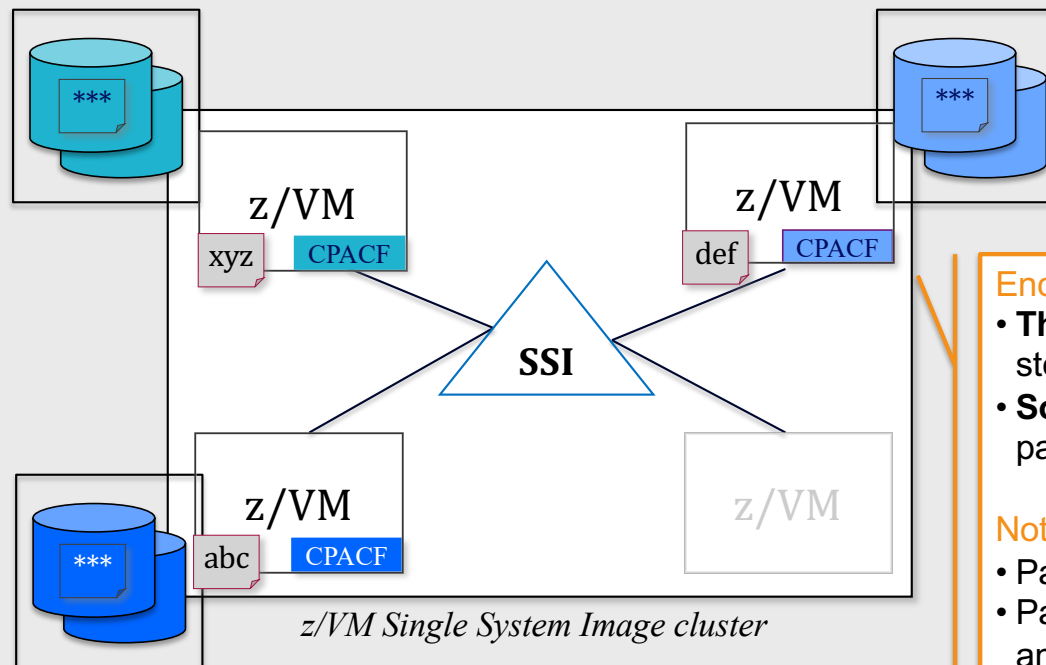
Data Protection // z/VM Encrypted Paging

Protection of data at-rest

z/VM 6.4
PTF for APAR VM65993

Legend:

*** - encrypted data
abc - unencrypted data



Client Value Proposition:

*Protect guest paging data from administrators
and/or users with access to volumes*

Encrypted Paging

- **Threat:** access to sensitive data when stored on CP owned disk
- **Solution:** encrypt guest data on page-out.

Notes:

- Paging is not SSI-relevant
- Paging data does not need to survive an IPL
- Ephemeral CPACF protected-key stored in CP (not on disk somewhere)
- AES encryption
- Very low overhead via CPACF

Using Encrypted Paging for z/VM (1/2)

new ENCRYPT Statement in System Configuration file

- `ENCRYPT PAGING ON ALGORITHM AES256`

new QUERY/SET ENCRYPT

- `SET ENCRYPT PAGING {OFF | ON | REQUIRED}`

- ALGORITHM selection when first enabled (AES 128, 192, 256)

Note: **REQUIRED** may cause complications with DR sites

- System will not IPL on earlier hardware, **or if missing z14 CPACF enablement**
- Recommendation: keep a backup System Configuration file for SALIPL emergencies
- Recommendation: use sysname keywords in System Configuration to specify ENCRYPT by system or node
- Recommendation: IPL your system with `ENCRYPT PAGING ON <algorithm>`
 - `SET ENCRYPT PAGING REQUIRED` via AUTOLOG1 or via a COMMAND Statement
 - Audit trail demonstrates encryption was never “off.”

Using Encrypted Paging for z/VM (2/2)

Auditing with MONITOR Records

- D1R4 – System Configuration and current status thereof
- D3R2 – Change record for status (SET ENCRYPT), with userid
- ***new*** D1R34 – Pages encrypted/decrypted, CPU utilization for encryption

If moving from ON to OFF, pages will still be decrypted when read into guest memory

Only way to ensure 100% compliance is to IPL your z/VM system with

- **ENCRYPT PAGING ON ALGORITHM AES256**

Auditing with SMF Records

- Auditing in RACF automatically covers new CP commands, per above
- Just enable tracking in your VMXEVENT profile

Dynamic Crypto Support for z/VM

http://www.vm.ibm.com/newfunction/#dynamic_crypto

z/VM 7.1
PTF for APAR VM66266

Dynamic Crypto support enables changes to the z/VM crypto environment without requiring an IPL of z/VM or its guests (e.g. Linux on Z).

This allows:





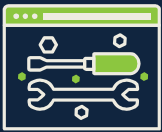



- Less disruptive addition or removal of Crypto Express hardware to/from a z/VM system and its guests
- Less disruptive maintenance and repair of Crypto Express hardware attached and in-use by a z/VM system
- Reassignment and allocation of crypto resources without requiring a system IPL or user logoff/logon
- Greater flexibility to change crypto resources between shared and dedicated use.

Additionally, there are RAS benefits for shared-use crypto resources:

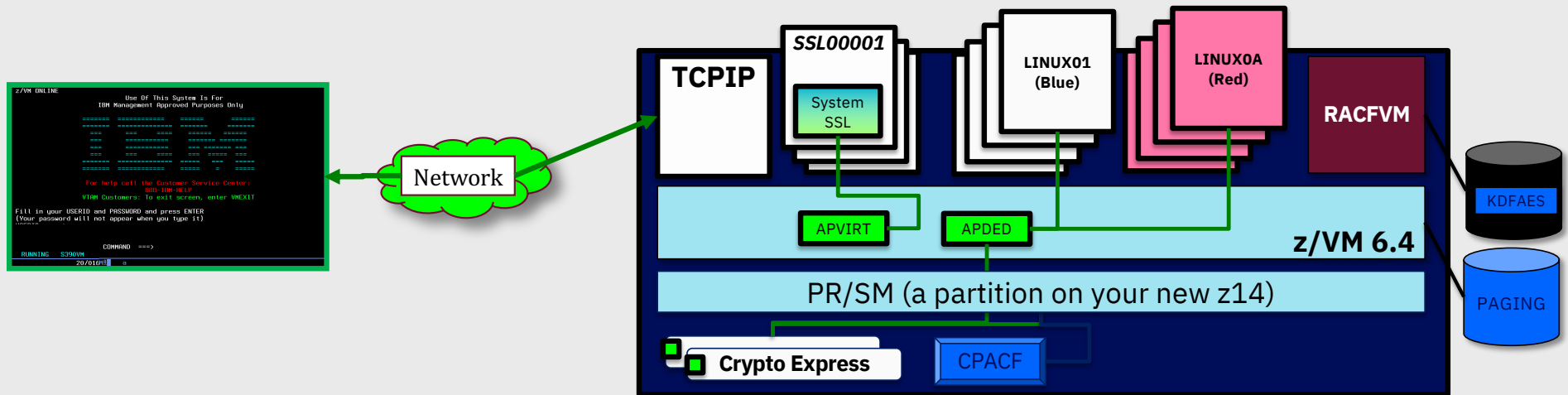
- Better detection of Crypto Express adapter errors with "silent" retrying of shared pool requests to alternative resources
- Ability to recover failed Crypto Express adapters
- Improved internal diagnostics for IBM service
- Improved logoff and live guest relocation latency for users of shared crypto.

With z/VM Pervasive Encryption ...

What does it cost to plan, configure, implement and/or maintain?

High Cost						
Medium Cost	 Key management		 Updates for regulatory changes			
Low Cost	 People	 Skills	 Ongoing maintenance	 Application lifecycle	 Application outages to implement encryption	 New business requirements

Summary: z/VM and Pervasive Encryption



Protection for guest operating systems

- Encryption needs to exist in virtual environments, too!

Protection of data in flight

- Modernized software crypto library
- Crypto Express acceleration for hypervisor traffic

Protection for data at rest

- Encrypted Paging as the first step
- More to come ...

Simplification and ease of use

- Security and cryptography should not be an impediment to business

But why stop there?

With Continuous Delivery, z/VM is providing early access to the crystal ball and allowing you – yes, **you** – to be involved with the design and development process.



Disclaimer

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Target dates shared here are not formal commitments, but meant to assist in your planning purposes. Because of the likelihood of changes, we highly recommend [subscribing to the notifications](#) for this page.

For more information, visit: <http://www.vm.ibm.com/newfunction/>

Data at Rest for Linux on Z

Linux on Z Crypto Libraries

Crypto Libraries supporting Crypto Express

libica

- clear key RSA

libcsulcca

- CCA coprocessor

openssl with ibmca (libcrypto API)

- clear key RSA

openCryptoki (PKCS #11 API)

- ica token: clear key RSA
- cca token: CCA coprocessor
- ep11 token EP11 coprocessor

GSKit

- via openCrxtoki using PKCS #11 API

IBM Java IBMPKCS11Impl (JCE API)

- via openCryptoki using PKCS #11 API

IBM Java IBMJCECCA (JCE API)

- CCA coprocessor

Crypto Libraries supporting CPACF

libica

- latest release supports z14 CPACF

openssl (libcrypto API)

- option: configure ibmca engine
- z14 GCM support via ibmca engine

openCryptoki (PKCS#11 API)

- with ica token (calls libica)

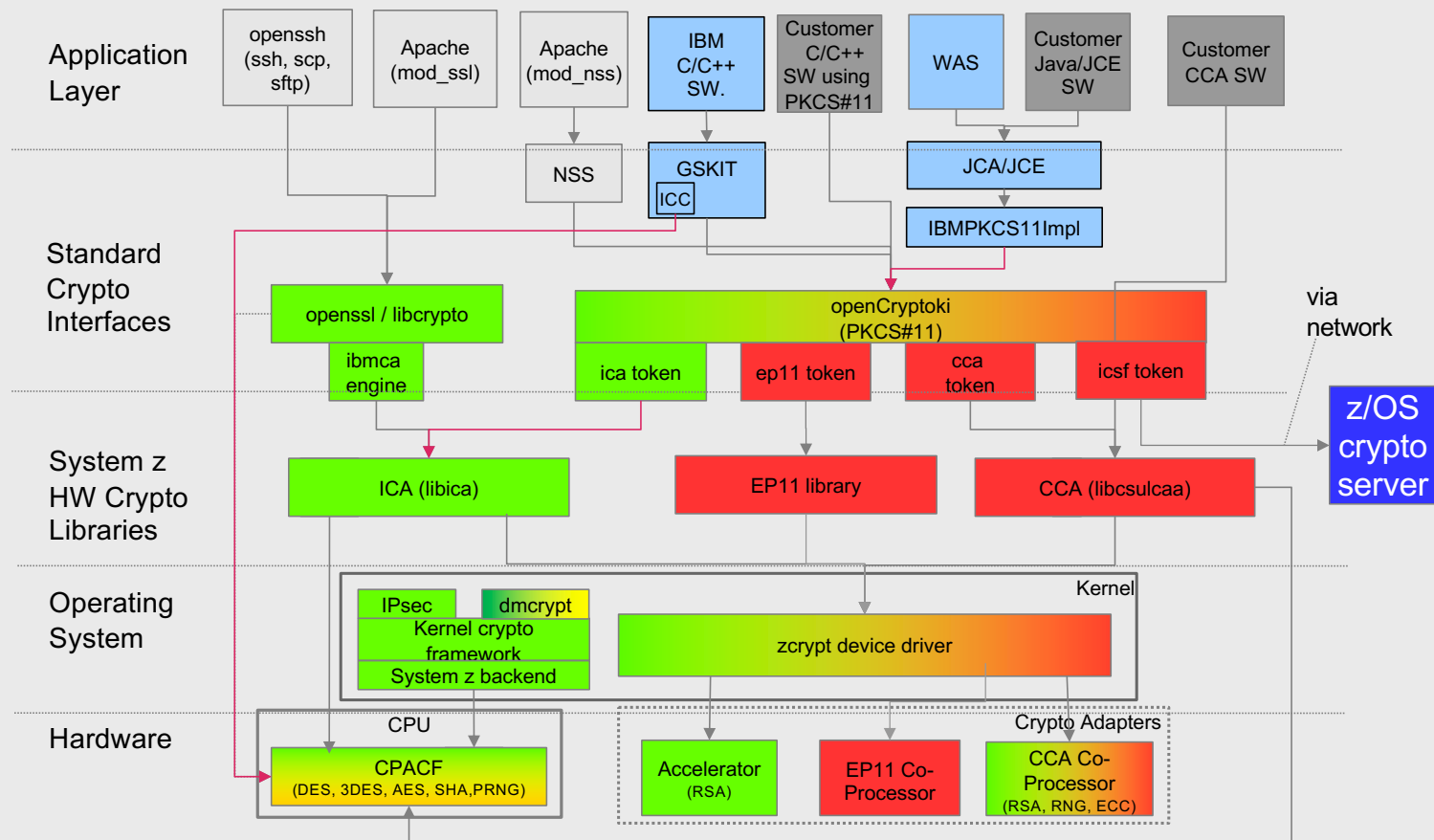
GSKit

- used by IBM software
- latest release supports Z14 CPACF

IBM Java 8 IBMJCE (JCE API)

- latest release supports Z14 CPACF

Linux on Z Cryptographic Infrastructure



Bringing Pervasive Encryption to Linux on Z

Bringing Pervasive Encryption to Linux on Z involves ...

Pushing crypto modifications upstream

Taking advantage of z14 hardware for both acceleration and protection

Extending crypto usage both for data-in-flight and data-at-rest

Key usage and cryptographic access should be as transparent to the administrator as possible

Data Protection // Linux on Z File Encryption

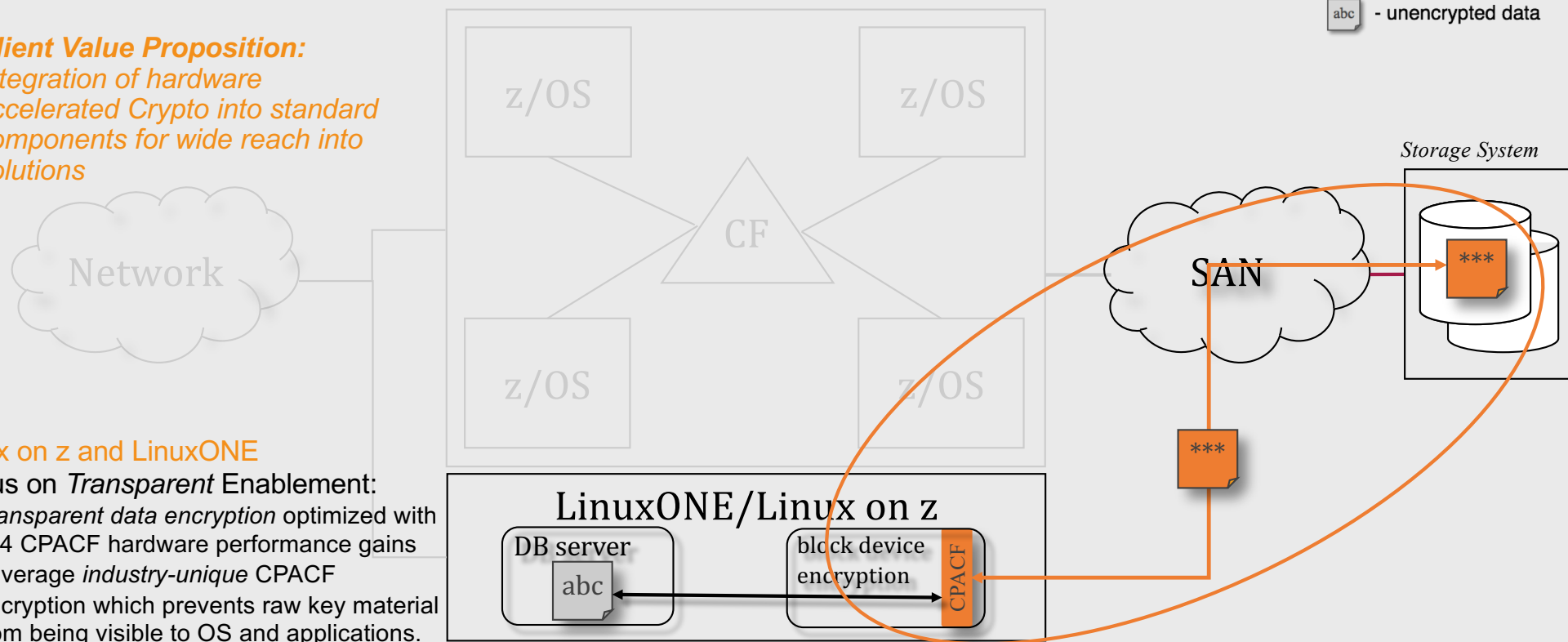
Protection of data at-rest

Client Value Proposition:
Integration of hardware accelerated Crypto into standard components for wide reach into solutions

Linux on z and LinuxONE

Focus on *Transparent Enablement*:

- Transparent data encryption optimized with z14 CPACF hardware performance gains
- Leverage *industry-unique* CPACF encryption which prevents raw key material from being visible to OS and applications.



Submitted Upstream

Legend:

*** - encrypted data
abc - unencrypted data

Status: dm-crypt enhancements for CPACF protected-key submitted upstream

Pervasive Encryption for Data at Rest

End-to-End Encryption

dm-crypt: block device / full volume encryption

- uses kernel crypto
- granularity: disk partition / logical volume
- new protected key option

ext4 with encryption option: file system encryption

- uses kernel crypto
- granularity: file, directory, symbolic link

Spectrum Scale (GPFS) with encryption option: file encryption

- uses GSKit or Clic
- granularity: file

DB2 native encryption: data base encryption

- uses GSKit

Network Encryption

NFS v4 with encryption option: encryption of file transport

- uses kernel crypto

SMB v3.1: encryption of file transport

- uses kernel crypto

kernel crypto
automatically uses
CPACF for AES if the
module aes_s390 is
loaded

GSKit and latest
versions of Clic use
CPACF for AES

End-to-End Data at Rest Encryption

The complete I/O path outside the kernel is encrypted: HV, adapters, links, switches, disks

dm-crypt

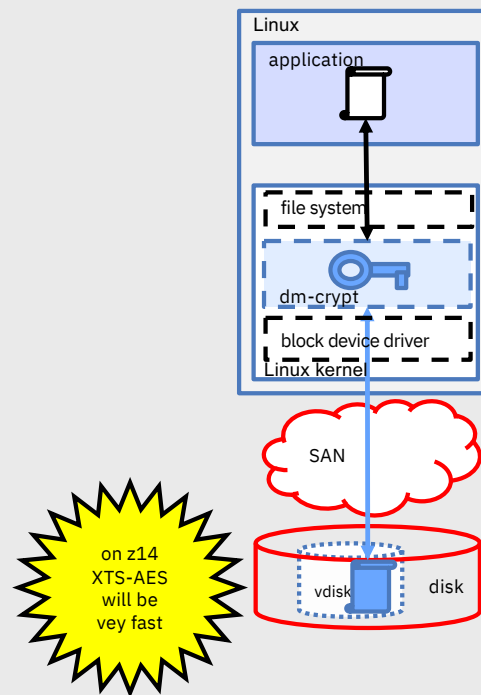
- a mechanism for end-to-end data encryption
- data only appears in the clear in application

Linux kernel component that transparently

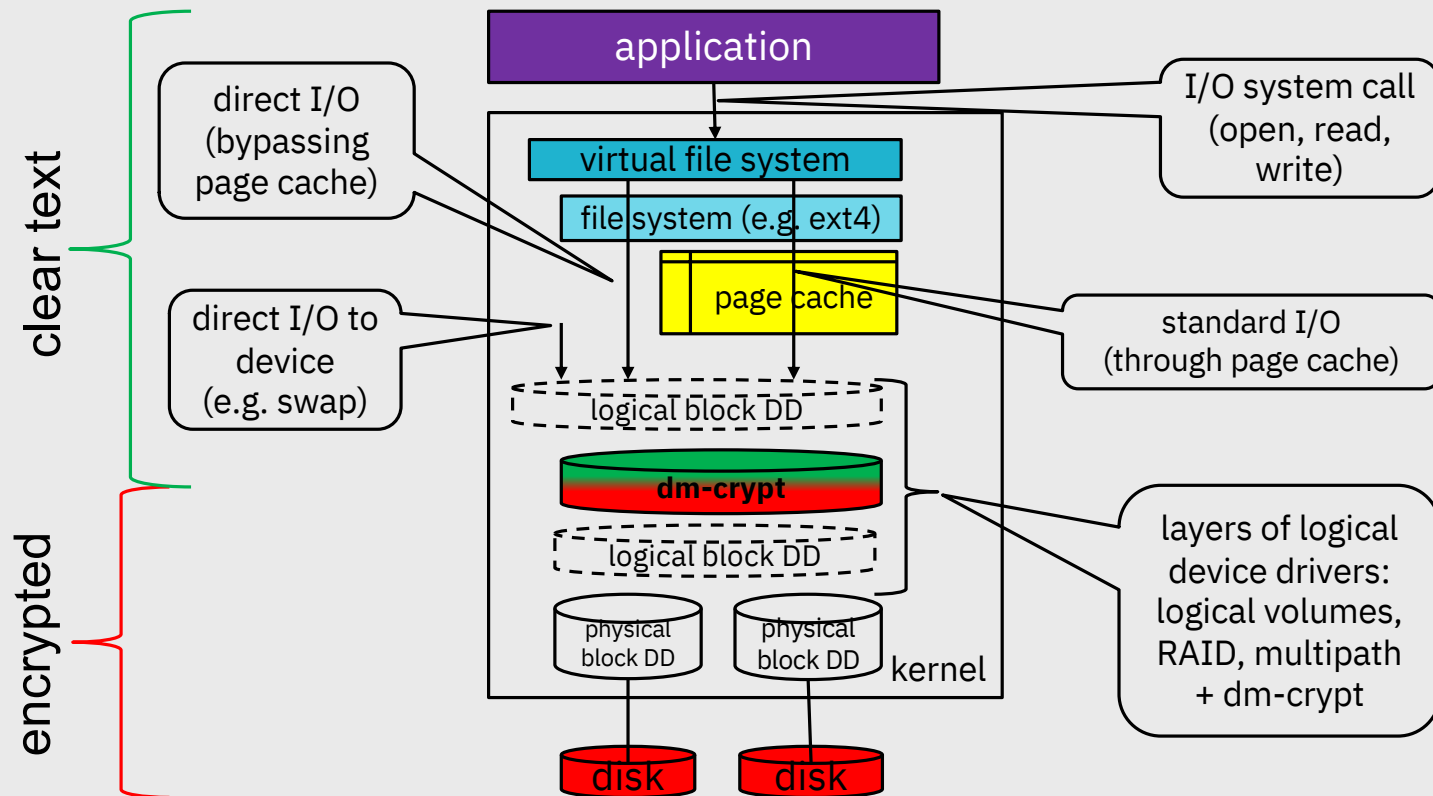
- for all applications
- for a whole block device (partition or LV)
 - encrypts all data written to disk
 - decrypts all data read from disk

Uses LUKS and in-kernel crypto operations

- LUKS: encryption keys stored on disk (partition, LV) header
- LUKS: encryption keys on disk are protected by passphrases
 - passphrases must be provided when disk is “opened”
- can use IBM Z CPACF for symmetric crypto operations:
 - AES-CBC
 - XTS-AES (recommended)



Linux File System Stack with dm-crypt



dm-crypt: Linux Unified Key Set-up (LUKS)

Plain

- No header
- **No formatting required**
- **Key & cipher name must be supplied with every open**
 - Key must be stored in a file in the file system

LUKS1

- Header on disk
 - Fixed binary header format
- **One-time formatting required**
- **Key & cipher name contained in the header**
 - Key is wrapped by a key derived from a passphrase
 - Up to 8 key slots

LUKS2

- Header on disk
 - Flexible header format (JSON)
 - Redundancy of metadata
 - Detection of metadata corruption
 - Automat repair from metadata copy
- **No formatting required**
- **Key & cipher name must be supplied with every open**
 - Key is wrapped by a key derived from a passphrase
 - Up to 32 key slots

What volumes can be encrypted by dm-crypt?

Yes: block devices

- Disks
 - SCSI disks
- Partitions of:
 - ECKD DASD
 - SCSI disks
- Multipath devices
- (LVM2) Logical volumes
- Loopback devices
- Other device mapper devices

No:

- Full ECKD DASD volumes
- Network file systems like NFS
 - But: you can create a loopback device based on a file in a network file system



E2E Data at Rest Encryption with Protected Keys

Protected keys?

- never stored in plain text in OS memory
- wrapped by system key accessible to CPU only
- ephemeral since system key recycled with every IPL
- extend **lifespan** of protected keys with Crypto Express adapters
- functionally similar to secure keys but much faster
 - implemented on CPU (CPACF)
 - no I/O required

New kernel support for protected key

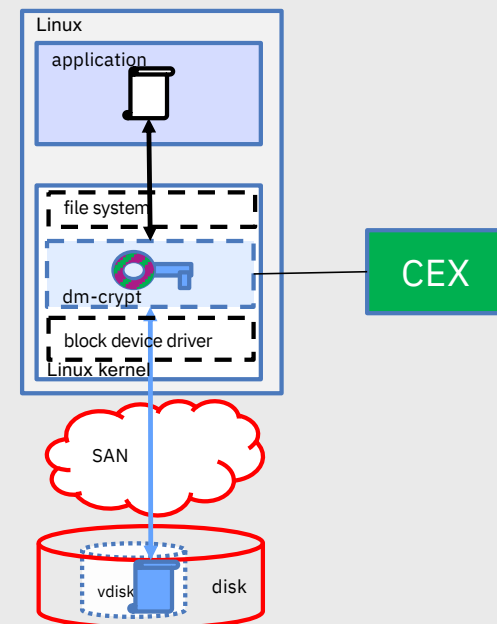
- module to support managing protected keys
 - transform secure key into protected key
- module to support PAES cipher (protected key AES)
 - takes a secure key and caches the associated protected key

dm-crypt

- can use **PAES** cipher to protect data with XTS-AES

New tools to manage volume encrypted using **PAES**

- support of LUKS format (work in progress)



LUKS/dm-crypt with Protected Keys

Components

new *pkey* kernel module for protected key management

- generate secure key
- transform secure key into protected key

new *paes* kernel module to perform protected key encryption-decryption

- introduces *paes* cipher

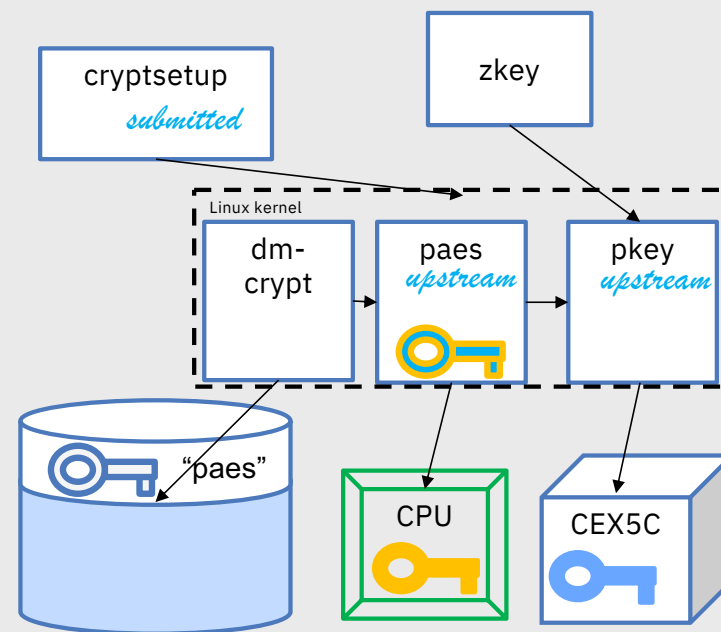
dm-crypt kernel module (unchanged)

extended *dm-crypt* management tool *cryptsetup*

- recognizes *paes* cipher
- stores secure key into LUKS header

new *zkey* tool to

- generate and manage secure keys
- re-encipher secure key



Key Management Tool for Protected Key dm-crypt

zkey tool released with s390tools 2.4.0

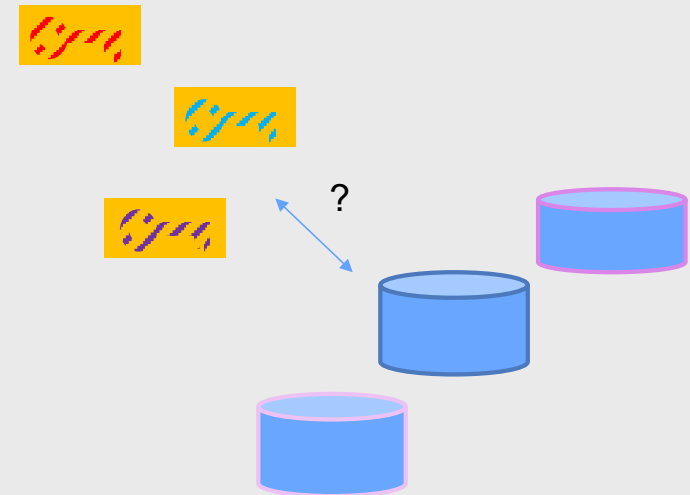
- stores secure keys (to be transformed into protected keys)
- associating keys with
 - with volumes encrypted by that key
 - cryptographic modes used
- allows key generation, repository management (list, add, delete)
- generation of opening commands for plain format volumes
- backup of repository easily possible with Unix tools (e.g. tar)

zkey tool extension to be released soon

- **adds LUKS2 volume type**
- allows generation of formatting commands for LUKS2 volumes

zkey-cryptsetup tool to be released soon

- support for master key changes for LUKS2 volumes **using protected keys**



Best Practices with (Protected Key) dm-crypt

use /etc/cryptsetup

- to configure automated opening of volumes

use dm-crypt volumes as LVM physical volumes

- allows transparent data migration

for production use

- Back up the dm-crypt superblock
 - to deal with superblock corruption
- Utilize back-up adapters with same master keys
 - to deal with HSM loss
 - Alternately:
 - - generate secure key from clear key in clear room environment
 - - and store clear key in safe

Current State of Pervasive Encryption for Linux

-- Data at Rest --

dm-crypt support for 4kB sectors

- upstream with kernel 4.12 and cryptsetup 2.0.0
- being included in all new distribution releases since beginning of 2018

	512b	4kB
z13 / Emperor	1	1.5
z14 / Emperor II	4	13

relative AES GCM/XTS
in-memory performance

dm-crypt support for protected key AES for volumes in plain format

- upstream with kernel 4.11
- being included in all new distribution releases since beginning of 2018

dm-crypt support for protected key AES for volumes in LUKS2 format

- upstream with kernel 4.11 and cryptsetup 2.0.3
- being included in all new distribution releases in 2H 2018

tool to manage key repository for secure keys used with protected key dm-crypt

- upstream with s390 tools 2.4.0
- being included in all new distribution releases in 2H 2018

Data in Flight for Linux on Z

Data Protection // Linux on Z Network Security

Protection of data in-flight

Submitted Upstream

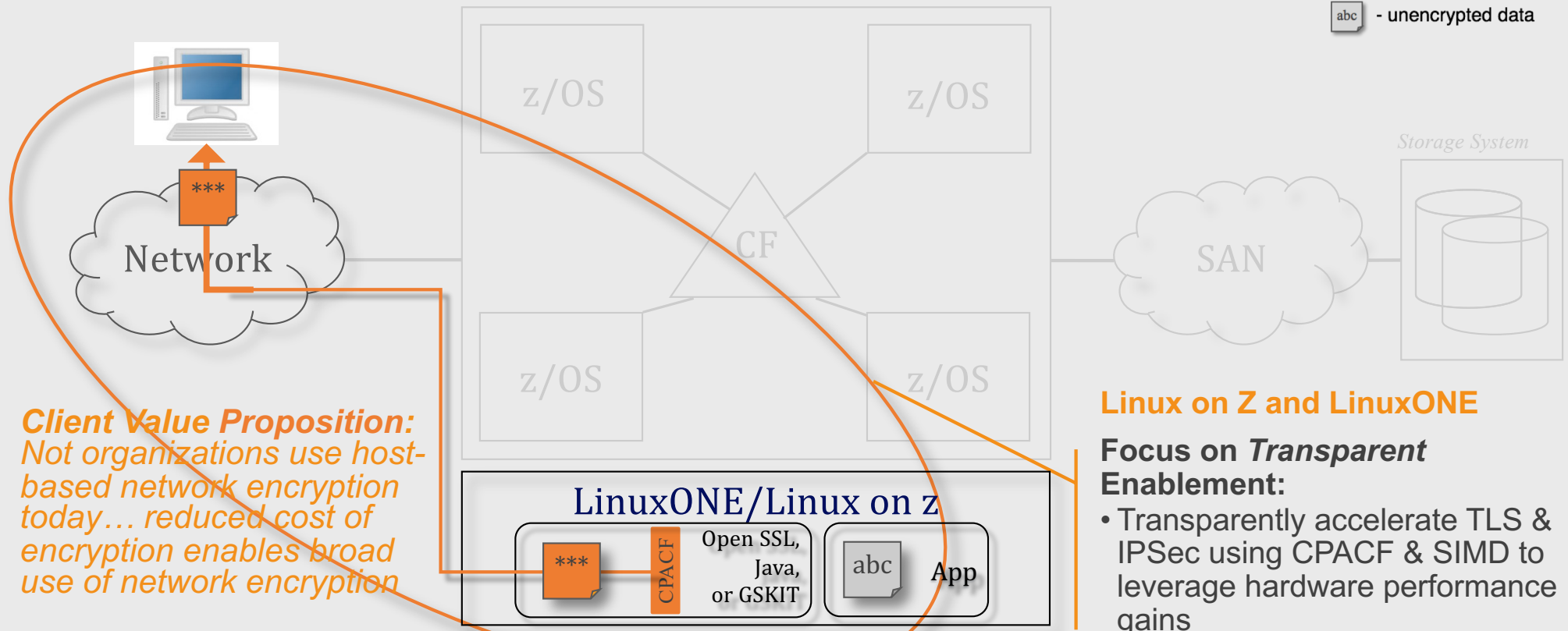
Legend:



- encrypted data



- unencrypted data



Client Value Proposition:
Not organizations use host-based network encryption today... reduced cost of encryption enables broad use of network encryption

Linux on Z and LinuxONE

Focus on *Transparent Enablement*:

- Transparently accelerate TLS & IPSec using CPACF & SIMD to leverage hardware performance gains

Status: dm-crypt enhancements for CPACF protected-key submitted upstream

The new Linux on Z openssl Strategy

Original Linux on z strategy

put Z specific code in the ibmca engine (only)

pro: all Z specific user space crypto in libica

cons: engines must be configured

New Strategy

all CPU dependent code (SIMD, CPACF) in **libcrypto**

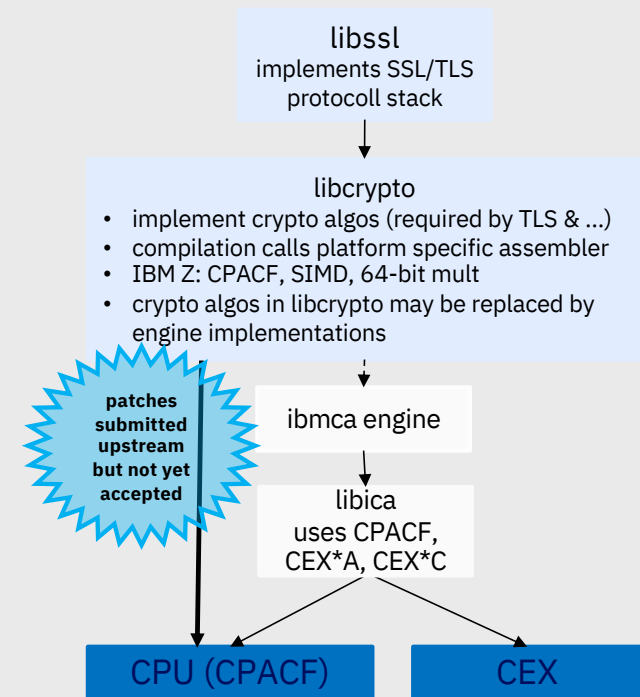
CryptoExpress dependent code in ibmca

no config needed for

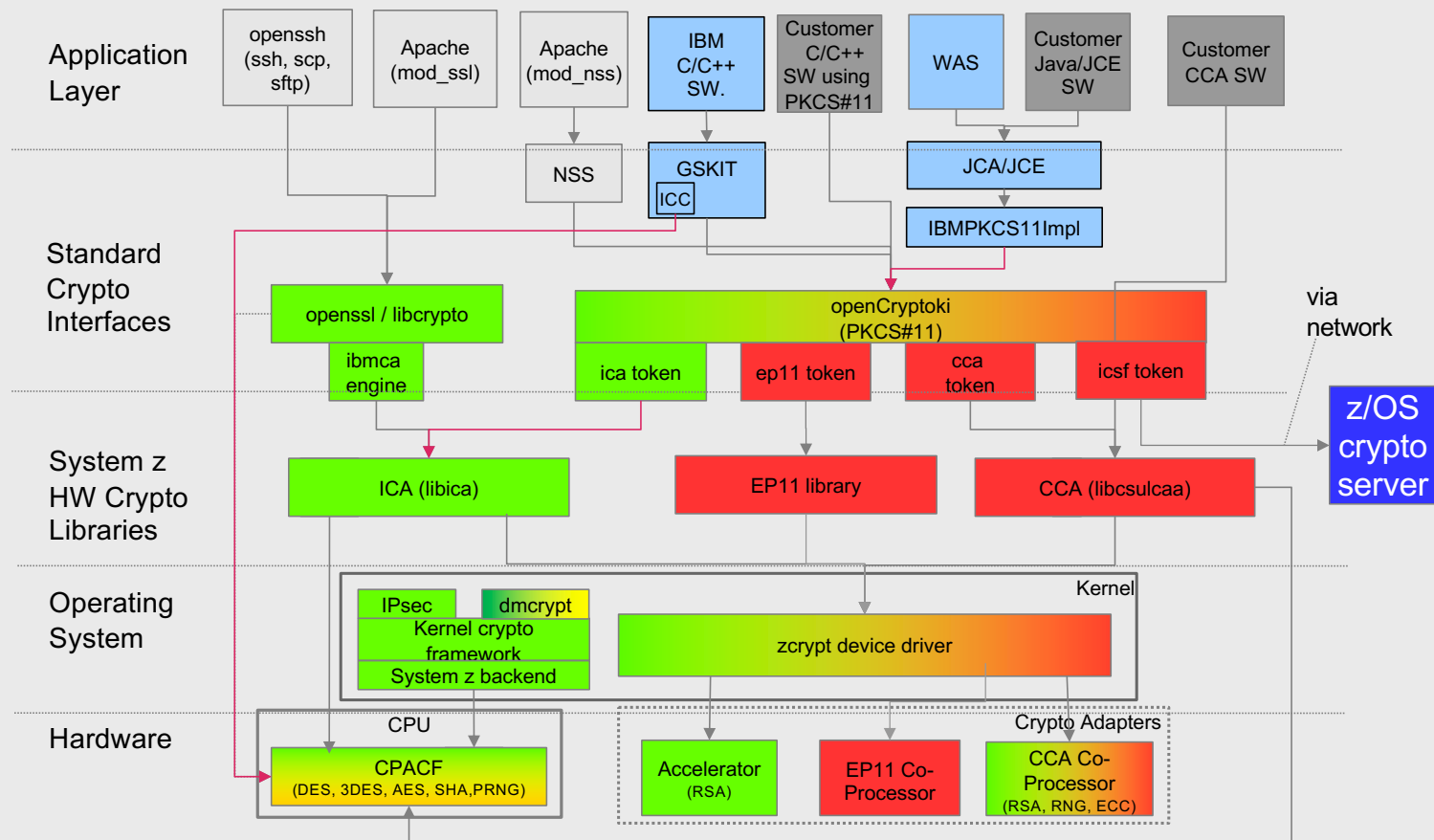
- hashes (SHA1, SHA2)
- AES (ECB, CBC, OFB, CFB, XTS, CTR, GCM, CCM)
- chacha20, poly1305
- Outlook: RSA, & ECC acceleration via SIMD arithmetic

ibmca engine config needed for

- offload/acceleration of RSA, DH, DSA, ECC, (3DES) via Crypto Express adapters
- configure engine to not support AES or hashes



Linux on Z Cryptographic Infrastructure



Pervasive Encryption: Data in Flight

openSSL and libcrypto

- de-facto standard TLS & crypto libraries
- used by many open source projects (including Apache, node.js, MongoDB)
- exploitation of IBM Z CPACF and SIMD code by libcrypto (w/o ibmca engine)
- focus on TLS 1.2 and 1.3 ciphers
- no IBM Z specific configuration required
- first patches (including AES-GCM support) accepted for openssl version 1.1.1-alpha2

IPsec

- bulk encryption and authentication implemented by kernel crypto
- transparently uses CPACF
- kernel 4.15 and later uses new CPACF instructions

GSKit

- IBM C library for TLS and crypto
- e.g. used by IBM HTTP Server (IHS)
- uses IBM Z CPACF
- release 8.0.50.82 and later use new z14 CPACF instructions

Java 8 / JCE

- exploitation of IBM Z CPACF and SIMD code
- Java 8 service refresh 5 and later use z14 CPACF instructions

Current State of Pervasive Encryption for Linux

-- Data in Flight --

TLS: CPACF support for AES GCM

- openssl/libcrypto upstream with version 1.1.1 beta
 - also supports AES ECB/CBC/CFB/OFB/CTR/XTS/CCM
 - being included in all new distribution releases since beginning of 2018
 - CPACF support for GCM backported to openssl 1.0.2 if required by distribution
- GSKit version 8.0.52.82
- Java 8 service refresh 5

IPSec: CPACF support for AES GCM

- upstream with Kernel 4.15
- being included in Ubuntu 18.04 and new distribution releases in 2H 2018

Questions?

IBM Z and LinuxONE – Security by Design, Architecture & Integration

Security is architected into IBM Z at all levels

- Processor
- Firmware
- Hypervisors
- Network
- Operating systems
- Applications & Middleware



IBM Z security innovation and leadership:

- Identity and access management
- Hardware and software encryption
- Communication security capabilities
- Extensive security event logging and reporting capabilities
- Extensive security certifications including EAL5+ (e.g., Common Criteria and FIPS 140)

“...our (infrastructure) is almost impossible to secure. We have added on three different applications and appliances in an effort to make it safer, but the add-on pieces have created their own difficulties and vulnerabilities. We are about ready to pull these services off of this platform and move it to a more secure platform, like our mainframe (z System). That platform at least is secure and does not act like an information sieve to hackers.”

– CISO, A Large Insurance Company



Security integration provides a more seamless solution, serves to reduce attack points, and yields a more robust security model.

Resources



Redbook: Getting Started with Linux on Z Encryption for Data At-Rest Redbook ***new***
<http://www.redbooks.ibm.com/abstracts/sg248436.html?Open>

Redbook: Security and Linux on z Systems
<http://www.redbooks.ibm.com/abstracts/redp5464.html?Open>

New: IBM Z pervasive encryption landing page
<https://izswebpage.mybluemix.net/>

IBM Z pervasive encryption solution guide (Knowledge Center)
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.izs/izs.htm

IBM Z pervasive encryption FAQ:
<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSQ03116USEN>

IBM Crypto Education page: <https://ibm.biz/BdiAah>


zPET Test Reports:
<https://www.ibm.com/developerworks/community/groups/service/html/communitystart?communityUuid=43ea8e78-acbe-49f5-9290-379e4f4569cb>

MOP demo white paper:
<http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102734>

Youtube Videos:

- Data Set Encryption: <https://www.youtube.com/watch?v=zdSXRUSmkb4>
- CF Encryption: <https://www.youtube.com/watch?v=lTmsFWuJwJU>
- zERT: https://www.youtube.com/watch?v=1CgEcCTX_o8
- MOP MPL Bank: <https://www.youtube.com/watch?v=EP488nLdGts>

Thank you!

Brian Hugenbruch 

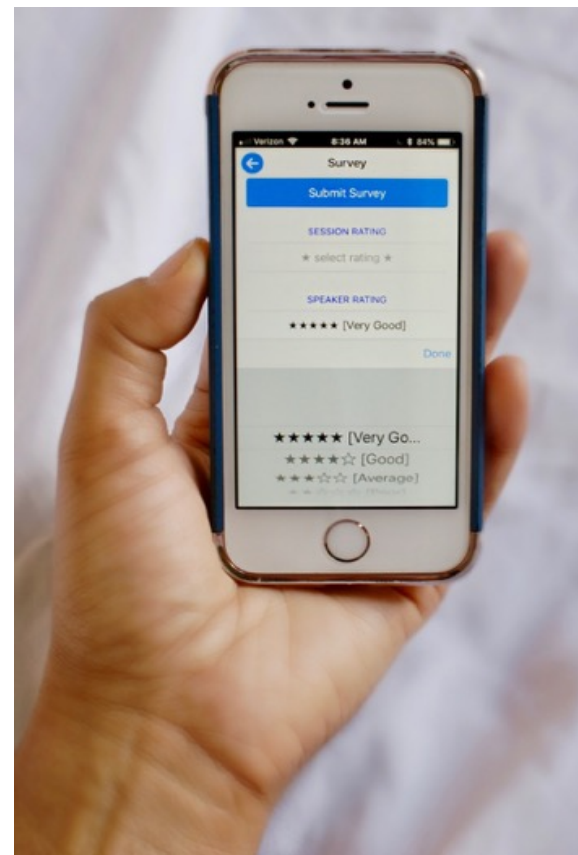
IBM Z Security for Virtualization & Cloud

bwhugen@us.ibm.com

 @Bwhugen

www.vm.ibm.com/devpages/hugenbru

Please complete the Session Evaluation!



Notices and disclaimers

- © 2019 International Business Machines Corporation.
No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.**
IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of 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. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.
- .

