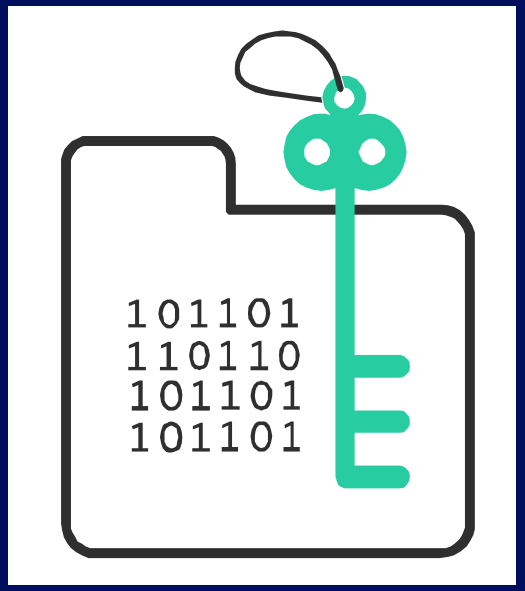
Encrypted Paging for z/VM 6.4: Deep Dive



Stephanie Rivero
z/VM Development Lab: Endicott, NY
srivero@us.ibm.com

IBM

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

BladeCenter*	FICON*	OMEGAMON*	RACF*	System z9*	zSecure
DB2*	GDPS*	Performance Toolkit for VM	Storwize*	System z10*	z/VM*
DS6000*	HiperSockets	Power*	System Storage*	Tivoli*	z Systems*
DS8000*	HyperSwap	PowerVM	System x*	zEnterprise*	
ECKD	IBM z13*	PR/SM	System z*	z/OS*	

* Registered trademarks of IBM Corporation

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.

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.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and

Linux is a registered trademark of Linus Torvalds 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.

OpenStack is a trademark of OpenStack LLC. The OpenStack trademark policy is available on the OpenStack website.

TEALEAF is a registered trademark of Tealeaf, an IBM Company.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

Worklight is a trademark or registered trademark of Worklight, an IBM Company.

UNIX is a registered trademark of The Open Group in the United States and other countries.

* Other product and service names might be trademarks of IBM or other 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 from 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 from 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.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g., zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

First

What is Pervasive Encryption, and why do we care?

Then

An explanation of IBM z14 hardware cryptography. (This will help explain why the rest of it matters.)

Followed by

Encrypted Paging for z/VM: what is it? What does it do?

And finally …

How to’s, interesting questions, performance considerations, and concluding thoughts.

The Value of Data

Today, data is one of the most valuable assets of many companies.

In particular sensitive data must be protected against unauthorized access to avoid

- losing customer trust
- losing competitive advantages
- being subject to fines

Data encryption is the most effective way to protect data outside your system be it in flight or at rest.

But encrypting data is not easy

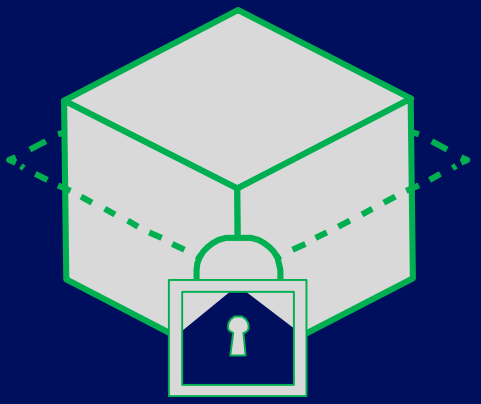
- requires the introduction of new policies
- complicates data management
- requires to securely manage keys
- costs computing resources

The IBM Z Pervasive Encryption Strategy

Extensive use of encryption is one of the most impactful ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

However, implementing encryption can be a complex process …

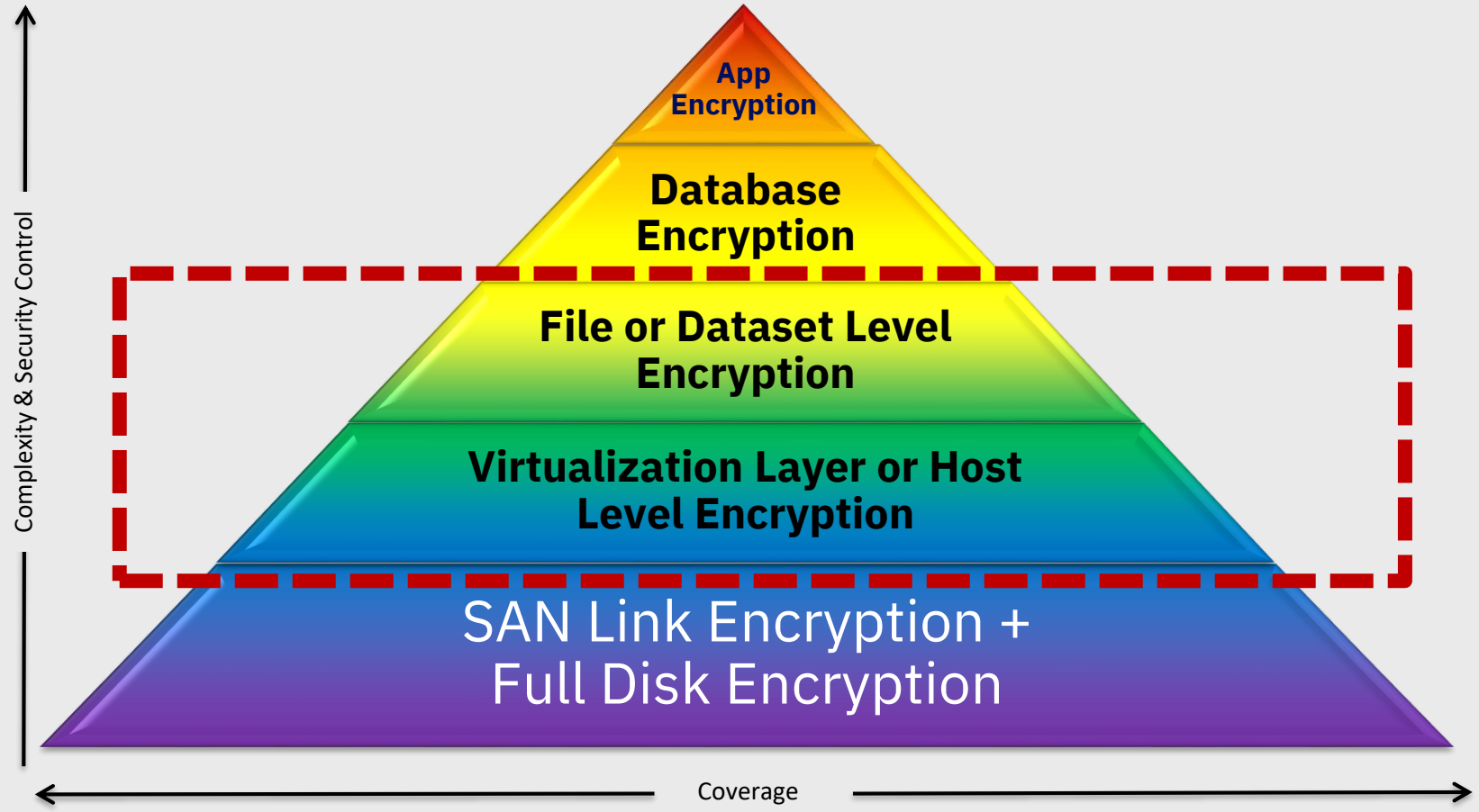
1. What data should be encrypted?
2. Where should encryption occur?
3. Who is responsible for encryption?



Transparent and consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates

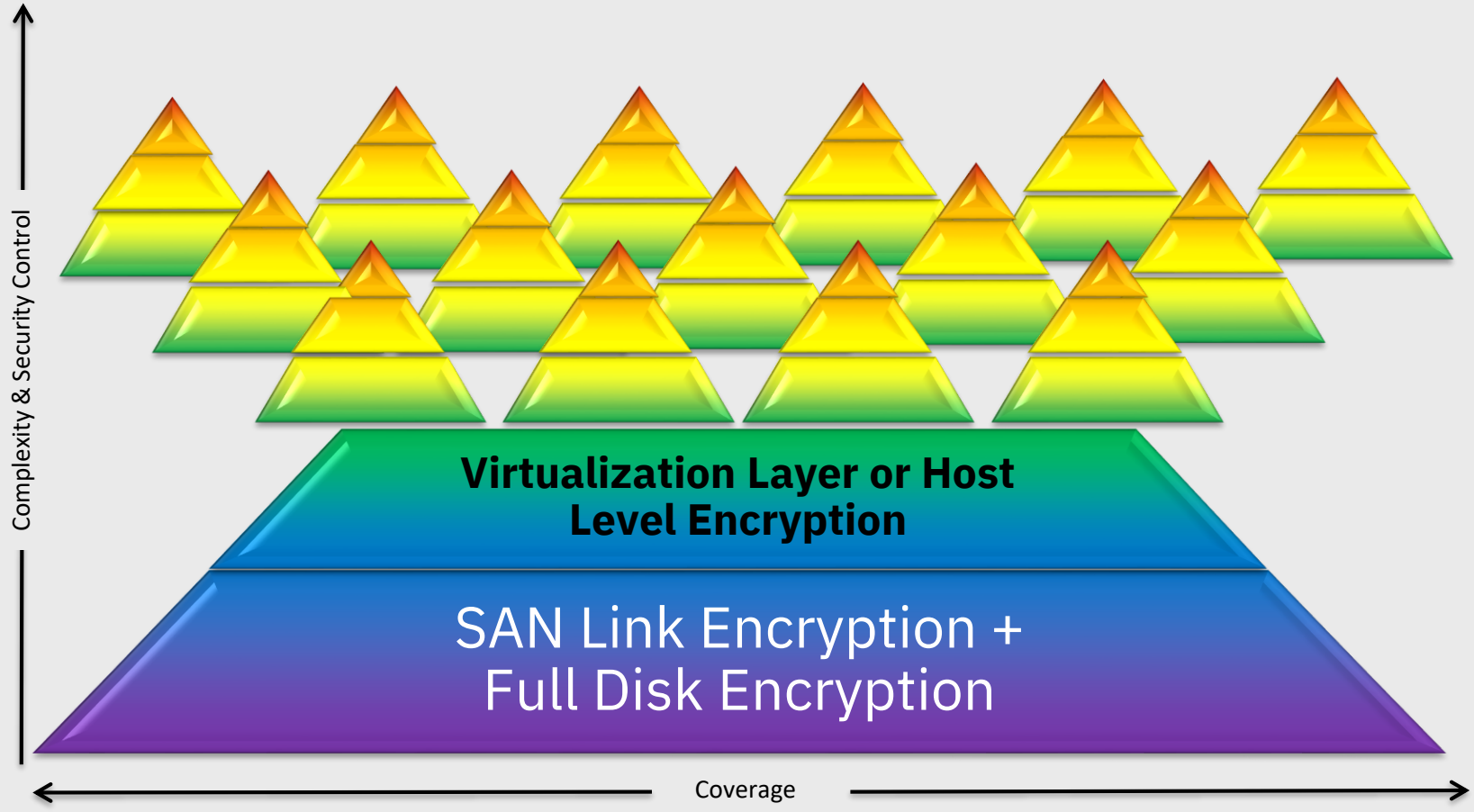
IBM Z Pervasive Encryption

From a Virtualization Point of View



IBM Z Pervasive Encryption

From a Virtualization Point of View



Pervasive Encryption for z/VM and Linux on IBM Z

z14 – Designed for Pervasive Encryption

- **CPACF** – Dramatic advance in bulk symmetric encryption performance
- **Crypto Express6S** – Doubling of asymmetric encryption performance for TLS handshakes

z/VM – Virtualizing Encryption for Linux

- **Virtualization** of IBM Z Crypto Hardware (**updated August 2017**)
- Crypto Express **acceleration** for encrypted data in flight (**available March 2017**)
- **Encrypted Paging** for z/VM (**available 4Q2017**)

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

- **LUKS 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

IBM Z Cryptographic Features

IBM z Systems provide two flavors for offloading and accelerating cryptographic operations which help you to

- Move cryptographic workload away from central processors
- Heighten your security level by protecting and securing keys
- Accelerate encryption and decryption

CP Assist for Cryptographic Function (**CPACF**)

Support for **symmetric** and hashing algorithms included in every CP and IFL
Pseudo-random number generator

Crypto Express *features*

Asymmetric and hashing algorithm offload
Host master-key storage
Hardware RNG
PKCS #11 cryptographic support

CP-Assisted Cryptographic Facility (CPACF)

CPACF Support (No-Charge Licensed Feature 3863)

Available on all modern IBM Z hardware but it must be explicitly ordered and enabled

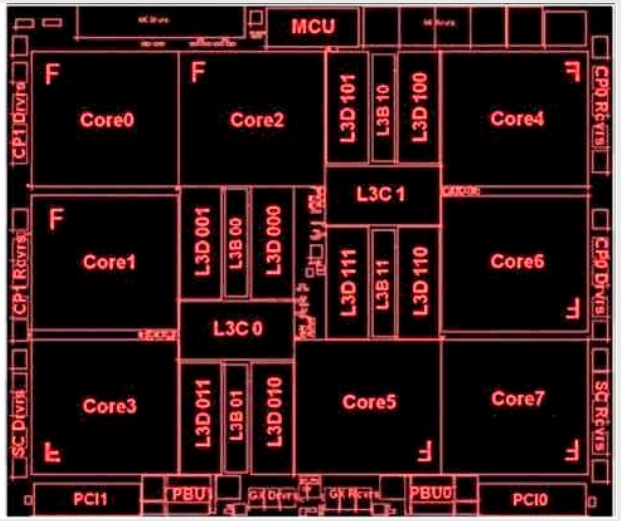
Provides on-CPU cryptographic processing ***at a higher throughput***

Supports the following algorithms:

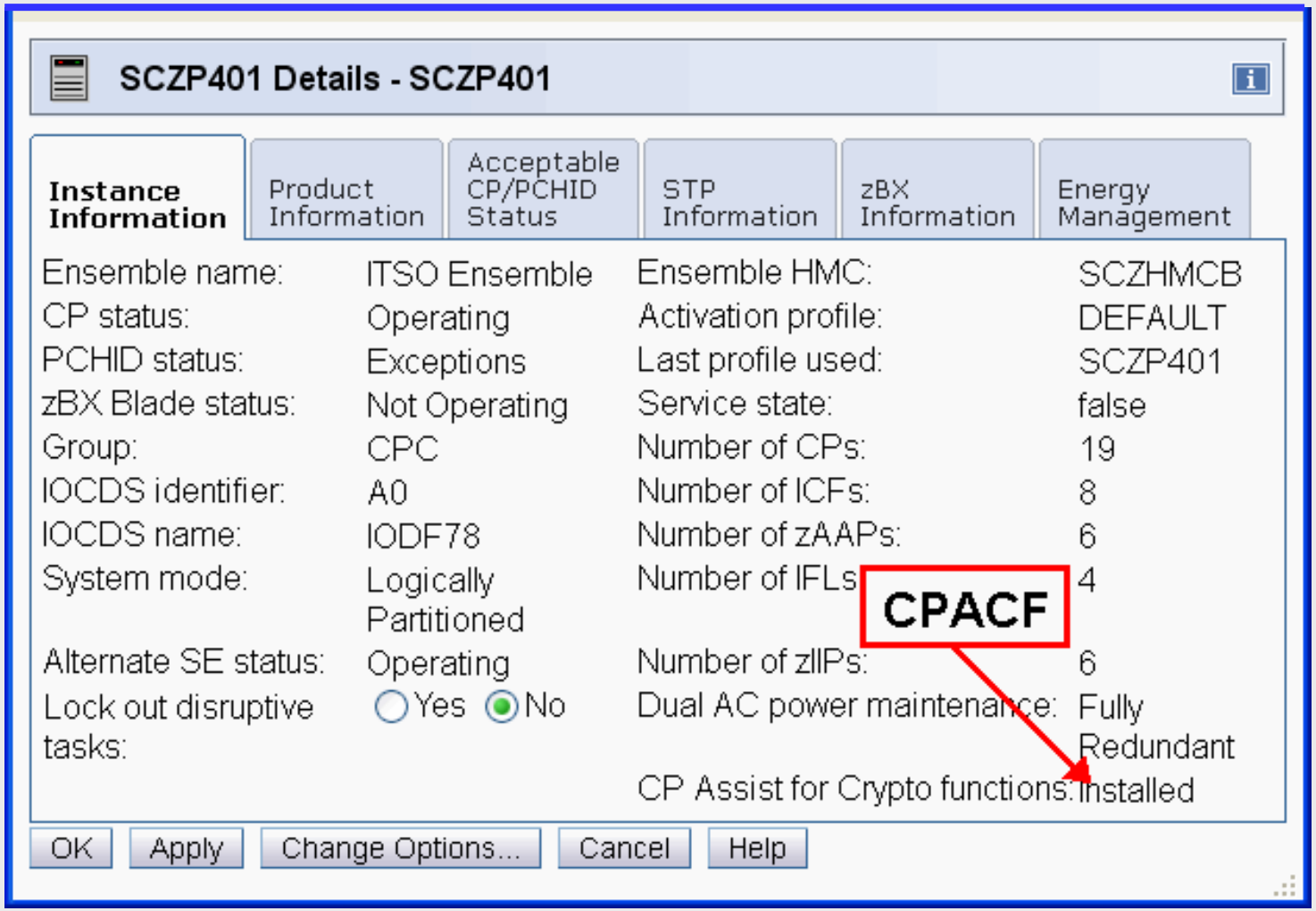
- DES
- TDES
- AES-128
- AES-256 (z10 onward)

- SHA-1
- SHA-224 and SHA-256
- SHA-384 and SHA-512 (z10 onward)

- Single-length key MAC
- Double-length key MAC

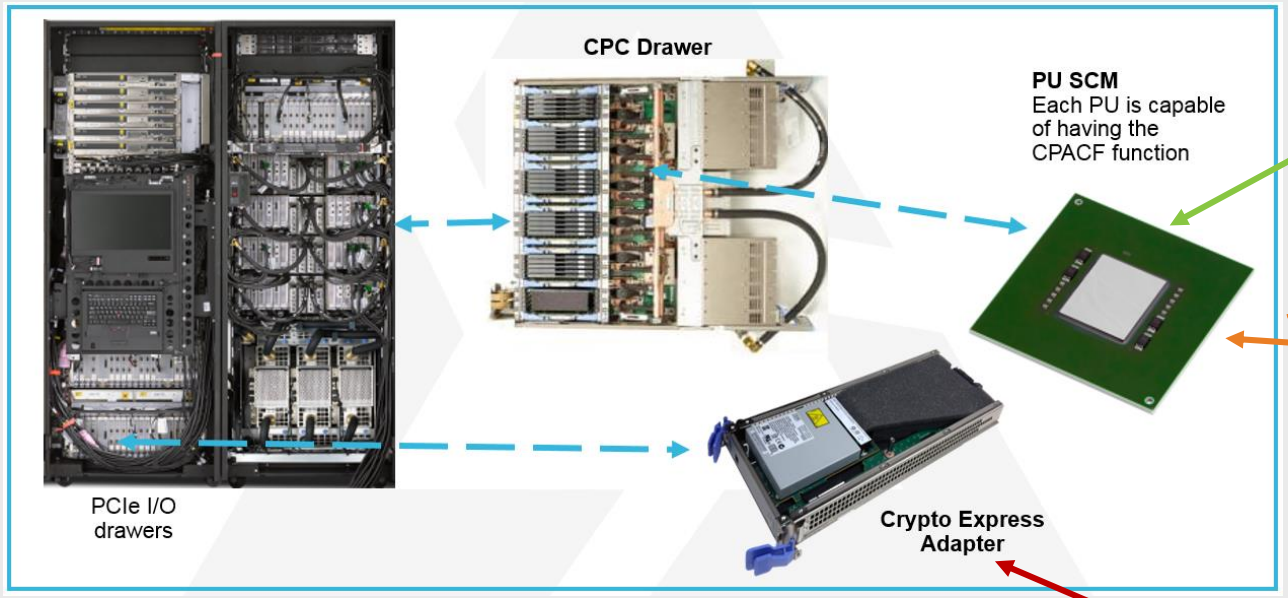


CP-Assisted Cryptographic Facility (CPACF)



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.



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

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")

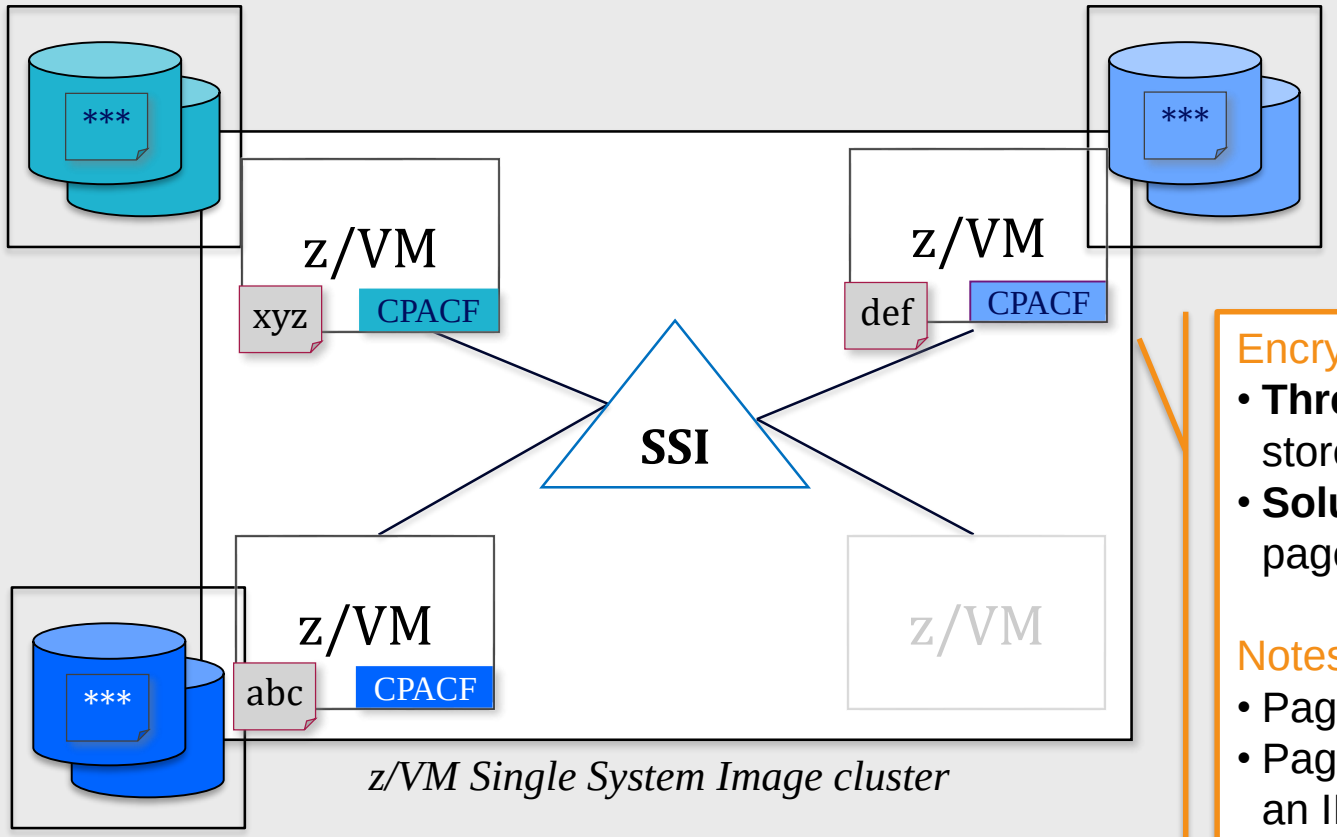
- All domains assigned to the CP-managed queues must be CCA coprocessors
- No change to dedicated crypto domains – those function as before
- Accelerates use of elliptic curve crypto for Linux or z/OS guests

– 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

Data Protection // z/VM Encrypted Paging

Protection of data at-rest

z/VM 6.4
PTF for APAR VM65993



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

Client Value Proposition:
Protect guest paging data from administrators and/or users with access to volumes

Getting Started with Encrypted Paging

How Do I Get Value?

z/VM Encrypted Paging

1. Starting point: z/VM partition on a z14 with CPACF enabled
2. Select configuration in System Configuration file (can modify it dynamically later, if you change your mind)
3. Generate an ephemeral *n*-bit AES encryption key during IPL process
4. If ENCRYPT PAGING is ON, then pages are encrypted as they move to/from paging volumes.
5. Use monitor records to determine performance impact for workloads

Relevant Hills: SUB-HILLS 1 & 3
Relevant Sponsor User Roles: Data Owner, Security Admin, Auditor
Security Admin Products: z/VM

Getting Started with Encrypted Paging: What's Encrypted?

This function encrypts data moved from active memory *to a paging volume owned by CP*

– ECKD, SCSI, or native FBA

Encryption is limited to guest pages and VDisk pages written by the CP paging subsystem

The following types of pages will **not** be encrypted:

– Spool files

– Directory pages

– Minidisk data to a mapped minidisk pool

– Minidisk cache pages

– CP page tables (PGMBKs)

Details on Encrypted Paging – How To Use

1. Make sure CPACF is enabled on your z14 system.
   - Support requires CPACF (no-charge Feature 3863) to be enabled on z14 hardware or later
2. Set **ENCRYPT PAGING ON** in System Configuration or use **CP SET ENCRYPT PAGING**
3. Protected ephemeral key (of selected algorithm) generated by CP for system lifetime, for all guests
   - No key rotation mechanism in this PTF
4. Support comes in **OFF** (default), **ON**, and **REQUIRED** modes
   - Per sponsor feedback on priorities, changing algorithm in first deliverable will require an IPL
5. To prevent against timing attacks, TRSOURCE not be permitted in keygen section of the IPL processes
6. One key per z/VM partition – no SSI dependencies
   - Performance considerations for guest relocation: re-enciphering paging data
7. A mandate for 100% encryption should use 'ENCRYPT PAGING ON' (at minimum) at IPL
   - ENCRYPT PAGING ON gives function but can be dynamically toggled
   - ENCRYPT PAGING REQUIRED comes with some usability concerns (more on this later)
   - Dynamic support can enable compliance, but **proving it** is difficult (draining volumes)

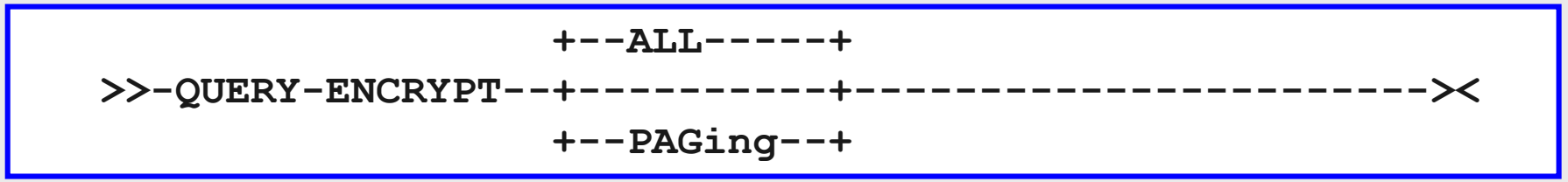
QUERY ENCRYPT
(Privilege Class A, C, or E)

Validate current encryption configuration, and compare against setting at time of IPL.

(Does not notify user if required hardware facilities are available.)

>> QUERY ENCRYPT PAGING

```
Encrypt Paging settings:
     Currently: Required AES256
     At IPL: Off
Ready;
```

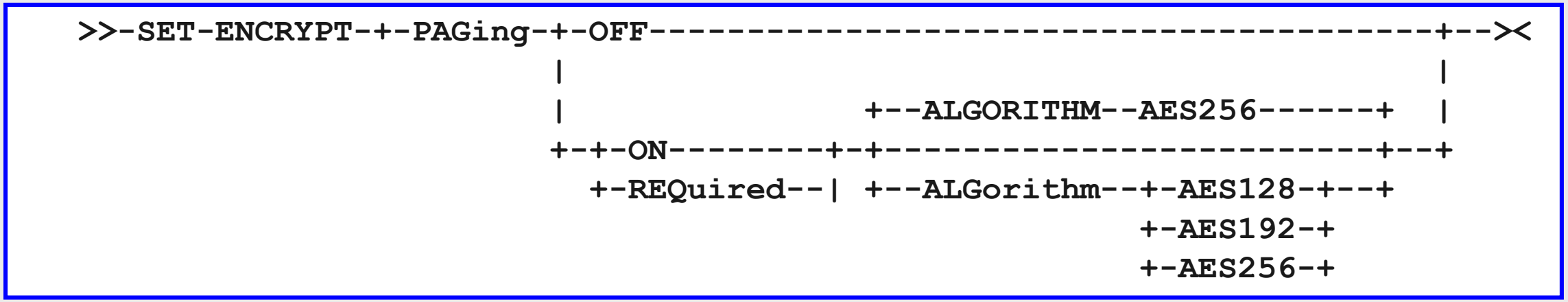


SET ENCRYPT
(Privilege Class A)

Modify the encryption setting for a particular CP host capability.

>> SET ENCRYPT PAGING ON ALGORITHM AES128

```
Encrypt Paging settings:
     Currently: Required AES128
     At IPL: Off
Ready;
```



Using SET ENCRYPT

- When specifying ON or REQUIRED, the default ALGORITHM is always AES256.
- The algorithm value may only be selected when Encrypted Paging is enabled for the first time. This may be either via SET or in the System Configuration file.
- Algorithm value cannot be changed without a re-IPL:

```
HCP1391E: Encryption algorithm previously set to ALGORITHM; no change made
```

- The System Operator is notified of changes to primary setting, e.g.

```
HCPENC1394I Encryption of paging changed from OFF to ON, with algorithm AES256,
by user ALTMARKA
```

- SET ENCRYPT cannot be used when missing hardware support:

```
HCPENC1390E Encrypt Paging cannot be enabled due to missing hardware support
```

- If set to REQUIRED, changes cannot be made without a System IPL.

```
HCPENC1390E Encrypt Paging is required; no change made
```

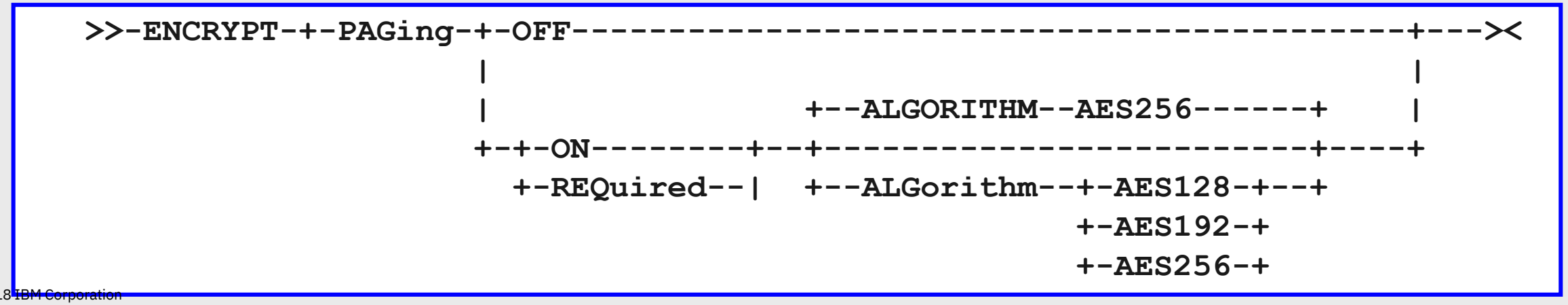
ENCRYPT Statement
(System Configuration file)

Establish the default ENCRYPT value for a CP host function.

```
ZVMSYS01: ENCRYPT PAGING ON
/* Default AES256 */

ZVMSYS02: ENCRYPT PAGING REQUIRED ALG AES192
/* not taking chances */

ZVMSYS03: ENCRYPT PAGING OFF
/* This system IPL's on a z12 EC. */
```



Using the ENCRYPT Statement

If OFF, no change – no problem. This is the default behavior, even after PTF is applied.

If ON and (missing or low-level CPACF) then

```
HCP1390E Encrypt Paging Not Available due to missing hardware support
(IPL processing continues)
```

If REQUIRED and (missing or low-level CPACF) then

```
HCP1393W Encrypt Paging Not Available due to missing hardware support, specified
as Required
(wait state)
```

Using REQUIRED (1/2)

Please note that **REQUIRED** means **REQUIRED.**

- Cannot be changed, cannot be broken
- Meant to assure 100% compliance for the administrators who need it

If you have configured **REQUIRED** on a system which does not support the feature, ***your system will not IPL***

- Double-check system labels in an SSI cluster – exclude back-level systems
- CPACF not enabled on new CEC – turn on CPACF
- z13 and earlier hardware – not supported
- May be a problem for DR sites

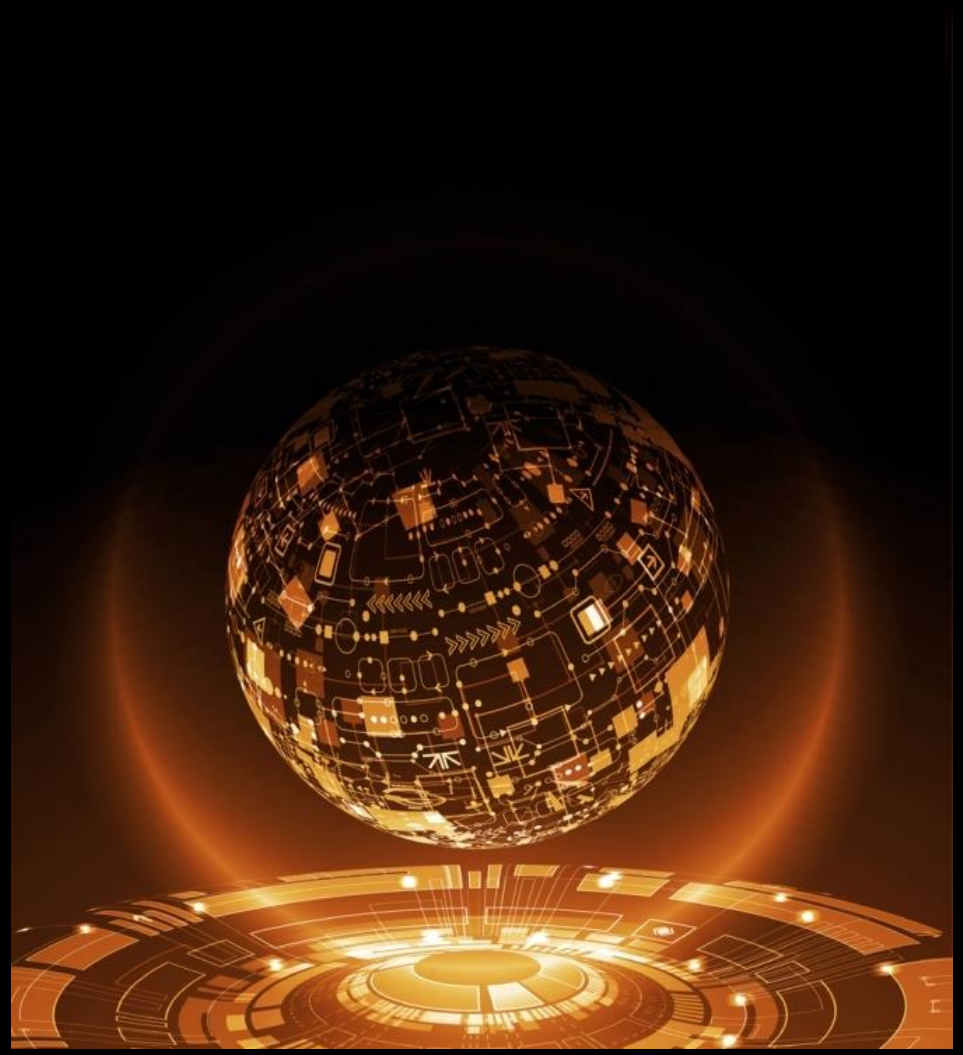
Using REQUIRED (2/2)

IBM recommends:

1. Test Encrypted Paging with **ON** before switching to **REQUIRED**

2. Consider either:
   a) Switching from **ON** to **REQUIRED** in AUTOLOG1 (during System IPL)
   b) Putting **SET ENCRYPT PAGING REQUIRED** on a COMMAND statement for OPERATOR

3. Have a back-up System Configuration file (with setting **ON**) for emergency purposes
4. Double-check DR plans for hardware availability of z/VM systems

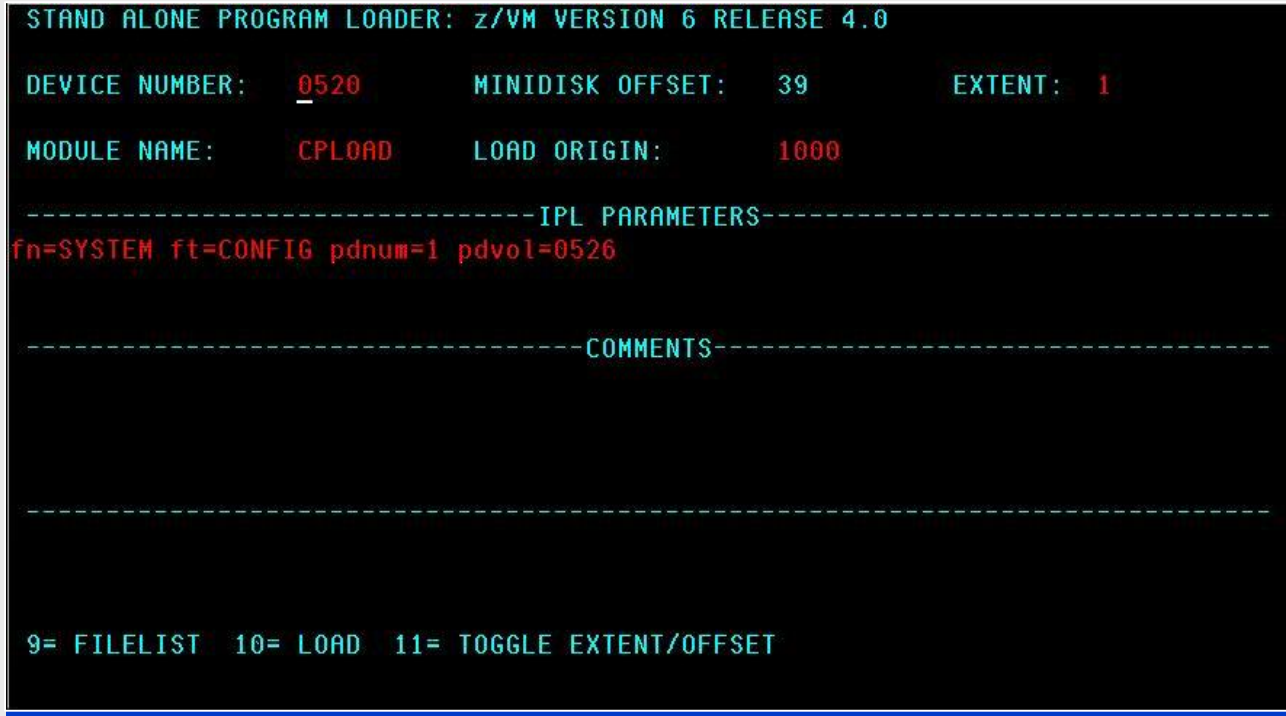


How do I specify an alternate SYSTEM CONFIG file, anyway?

Answer: IPLPARLMS in SAPL

- `Fn=<filename>  /* default SYSTEM */`
- `Ft=<filetype>  /* default CONFIG */`
- `PDNUM  /* parm disk # */`
- `PDVOL  /* parm disk address */`

Can use FILELIST option to double-check filenames / to validate which CONFIG files might be available (if pointing at correct volume).



For more information, see:

z/VM System Operation, Chapter 2 (“Using the Stand-Alone Program Loader”):

- “Passing IPL Parameters”

The System Configuration file is generally on PMAINT.CF0, but check your local configuration to confirm this detail.

Tracking Changes to ENCRYPT PAGING

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

Encrypted Paging: SSI and LGR Implications

Encrypted paging does not need to be enabled on all members of a Single System Image cluster

Ephemeral keys are not shared; there is one ephemeral key per member

– When relocating a guest
  - Its pages are decrypted before they are relocated to the target member
  - Target member re-encrypts the guest's pages using its own ephemeral key

Relocation domains may be defined based on guests' security requirements, such as

– Access to hardware facilities such as z14 CPACF

– Encrypted paging in the hypervisor (requires z14 partitions)

Encrypted Paging: Frequently Asked Questions (1/2)

Can I turn it on and/or off after IPL?

– *Yes! But bear in mind that we won't automatically decrypt previously encrypted pages until it's time to page the data in (and read it).*

Why does Encrypted Paging require z14?

– *In order to generate ephemeral keys, z/VM needs the TRNG now available on z14 CPACF. Keys generated with PRNG would not have been reasonably secure.*

What do I do if I lock myself out?

– *We recommend you keep a back-up system configuration file available and specify that on your SALIPL screen in case of emergencies.*

Encrypted Paging: Frequently Asked Questions (2/2)

What about Single System Images and Live Guest Relocation?

- *One ephemeral key per member system where enabled*
- *Guest relocation will need to decrypt pages before relocating them to target system*
- *Relocation domains based on security rather than architecture*
- *No, we're not encrypting CTCs – they're closed physical channels.*

Why paging? Why not minidisks?

- *"Minimum Viable Product."*
  (If Brian H. is on stage, he'll ramble for a while here.)

And of course, the big question ...

“How much does it cost me?”

Answer (say it with me):
“It depends.”

… but probably not as much as you think.

- **Goal was +3%-6% CPU time per operation**
- **In line with pervasive encryption on the rest of the platform**
- **Encrypted paging on IBM z14 still costs “less” than clear paging on the IBM z13.**

Performance Key Findings

As cipher strength increased, total CPU used on encryption and decryption increased

- CPU time used to encrypt a page increased
- CPU time used to decrypt a page decreased

On average, encryption costs more than decryption

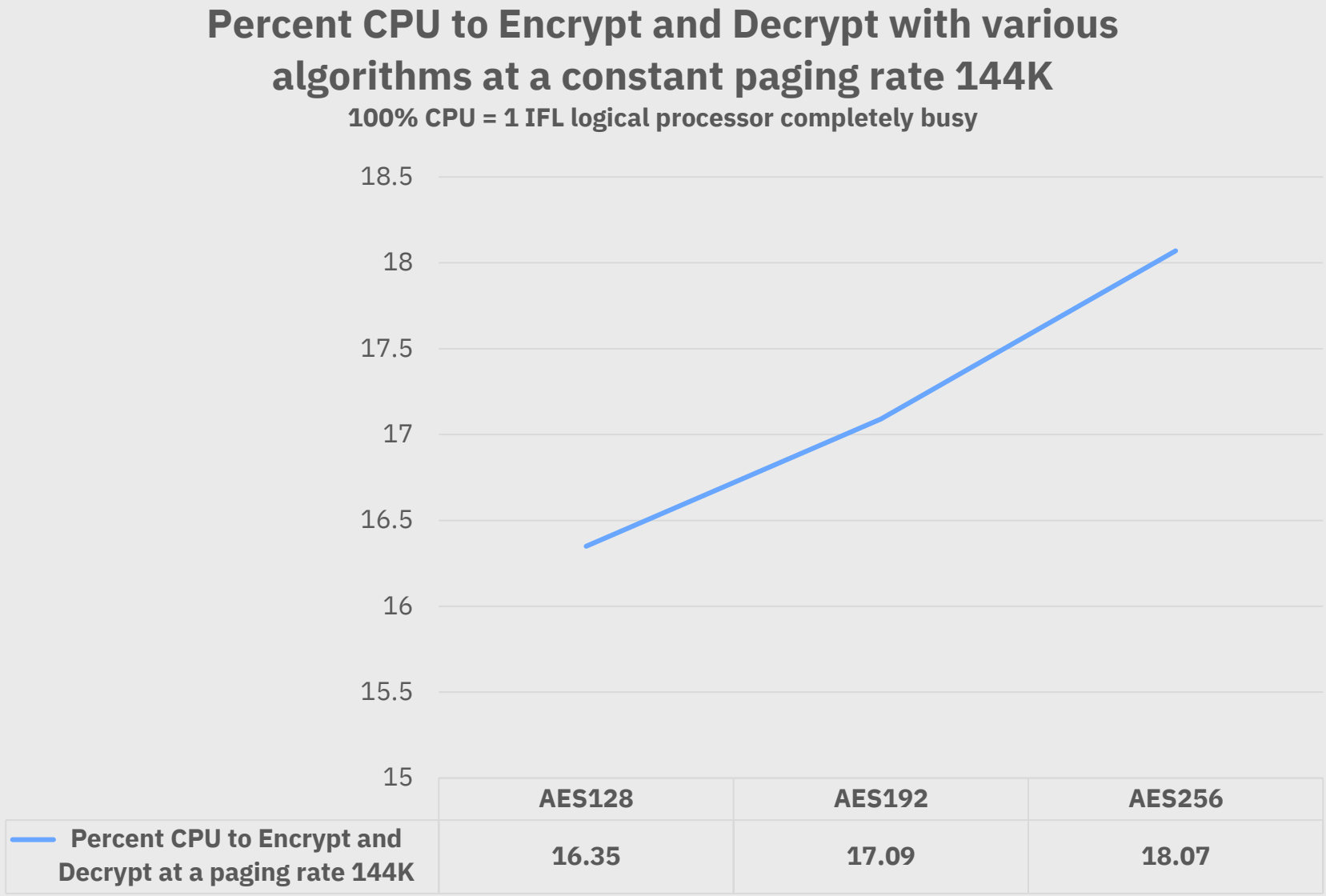
- ***This is a function of CPACF AES-CBC, and true no matter what you're doing with it.***
- This translates to the CPU penalty for page writes being greater than the CPU penalty for page reads

Despite the extra cost of encryption, the z14 with encrypted paging enabled performed better when compared back to a z13 (measured one test case)

CPU cost of encrypted paging is a function of the paging rate rather than the LPAR size.

Performance Report: http://www.vm.ibm.com/perf/reports/zvm/html/640EP.html

Performance Key Findings



D3R2EC Tool

Name: Domain 3 Record 2 Encrypted Counters

Reduces the encrypted paging counter monitor D3 R2 sample records

Tracks how many pages are being encrypted and decrypted, bytime and per logical processor

Tracks how much CPU is being used for encryption and decryption by time and per logical processor

The tool requires a monitor file with Encrypted Paging enabled as the input

Produces a filetype $D3R2EC

Useful information on D3R2EC:
http://www.vm.ibm.com/perf/tips/d3r2ec.html

D3R2 Encrypted paging report for file: A1TYA170 MONDATA

Interval			<------- Rate of Pages -------->			<------ Percent CPU busy ------>		
__Ended_	Type	LPU_	_Enc+Dec__	Encrypted_	Decrypted_	_Enc+Dec__	__Encrypt_	__Decrypt_
>>Mean>>	IFL	0	21540.75	14312.00	7228.75	2.82595	2.08754	0.73840
>>Mean>>	IFL	1	16604.04	8337.06	8266.98	2.05002	1.20734	0.84268
>>Mean>>	IFL	2	16889.88	8456.90	8432.97	2.08686	1.23022	0.85664
>>Mean>>	IFL	3	16890.18	8582.90	8307.29	2.10518	1.25280	0.85237
>>Mean>>	IFL	4	17028.51	8580.36	8448.14	2.11193	1.24691	0.86502
>>Mean>>	IFL	5	18559.72	8828.98	9730.74	2.27496	1.28750	0.98746
>>Mean>>	IFL	6	18855.95	8928.82	9927.13	2.30543	1.30089	1.00453
>>Mean>>	IFL	7	18504.28	8780.39	9723.88	2.26575	1.27842	0.98732
>>Total>	....	8	144873.30	74807.41	70065.89	18.02607	10.89163	7.13444

This is a **by-time** report and **per logical processor** report

The top of the file includes an average over the whole monitor interval report.

Over the whole monitor interval, this workload was **encrypting and decrypting over 144K pages/sec** and used a little over 18% of one logical processor

- 10.89% CPU of one logical processor for Encryption
- 7.13% CPU of one logical processor for Decryption

$D3R2EC

Sample Output File

PKEPESTM EXEC Estimator

Takes a PERFKIT file and predicts amount of CPU needed based on paging rate
FCX143 – PAGELOG

Estimated CPU to be used on Encryption and Decryption

Note: 100% CPU = 1 IFL logical processor completely busy

Interval	% CPU Encrypt	% CPU Decrypt
>>Mean>>	11.51	8.59
15:07:51	9.20	7.96
15:08:21	12.04	9.45
15:08:51	15.33	7.38
15:09:21	13.43	8.03
15:09:51	12.40	8.46
15:10:21	11.56	8.20

PKEPESTM EXEC Estimator

Checks the model-type in FCX180 – SYSCONF

If model-type **is not** a 3609-M05 then the tool bails

Why?
Because the tool is based the measurements completed on the 3690-M05

```
Ready; T=0.01/0.01 09:35:27
PKEPESTM A10YA17X PERFKIT  T
Processor Model is not a 3609-M05
An estimation was not calculated
Ready(00001); T=0.20/0.22 09:35:33
```

Questions?

Best Practices with z/VM Encrypted Paging

System Configuration: **Use ON** and not REQUIRED

- Safer for DR scenarios
- Prevents accidental lockout
- Switch to REQUIRED in AUTOLOG1 (before RACF is IPL'd)

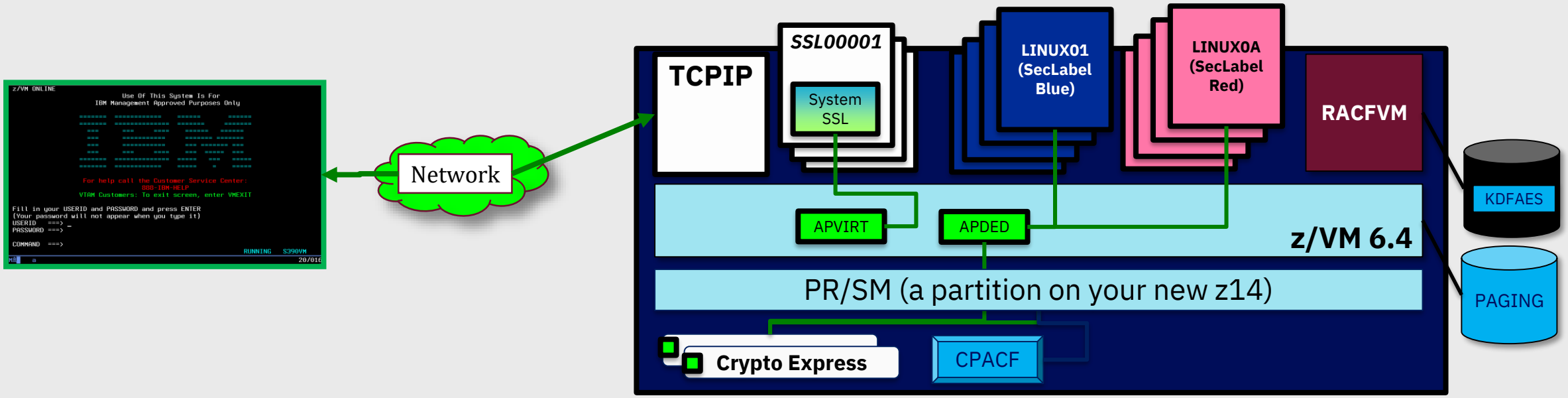
Test your workloads vs. ephemeral key size

- Read the Performance Guidance from IBM z/VM
- Find the encryption strength which works best for you
- Consider your security needs when enabling encryption at one level vs. another

Audit your Encryption

- Monitor records – monitor your usage
- SMF records – monitor access controls and changes

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

For More Information …

IBM z14 Technical Guide:
http://www.redbooks.ibm.com/redpieces/abstracts/sg248451.html?Open

IBM Z Hardware Crypto Synopsis:
https://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100810

IBM Z Crypto Education Community:
https://www.ibm.com/developerworks/community/groups/community/crypto

z/VM Security:
http://www.vm.ibm.com/security

Linux on z Security:
https://www.ibm.com/support/knowledgecenter/linuxonibm/liaaf/security.html

Contact Information:

Stephanie Rivero
z/VM Memory Management Component and Function Test
srivero@us.ibm.com

Contact Information:

CISSP®

Brian W. Hugenbruch
IBM Z Security for Virtualization & Cloud
bwhugen at us dot ibm dot com
@Bwhugen