Managing IBM Z Cryptography with z/VM
(Keys to the Kingdom)

Steven Horvath
IBM z/VM I/O and Crypto Development
Steven.Horvath@ibm.com

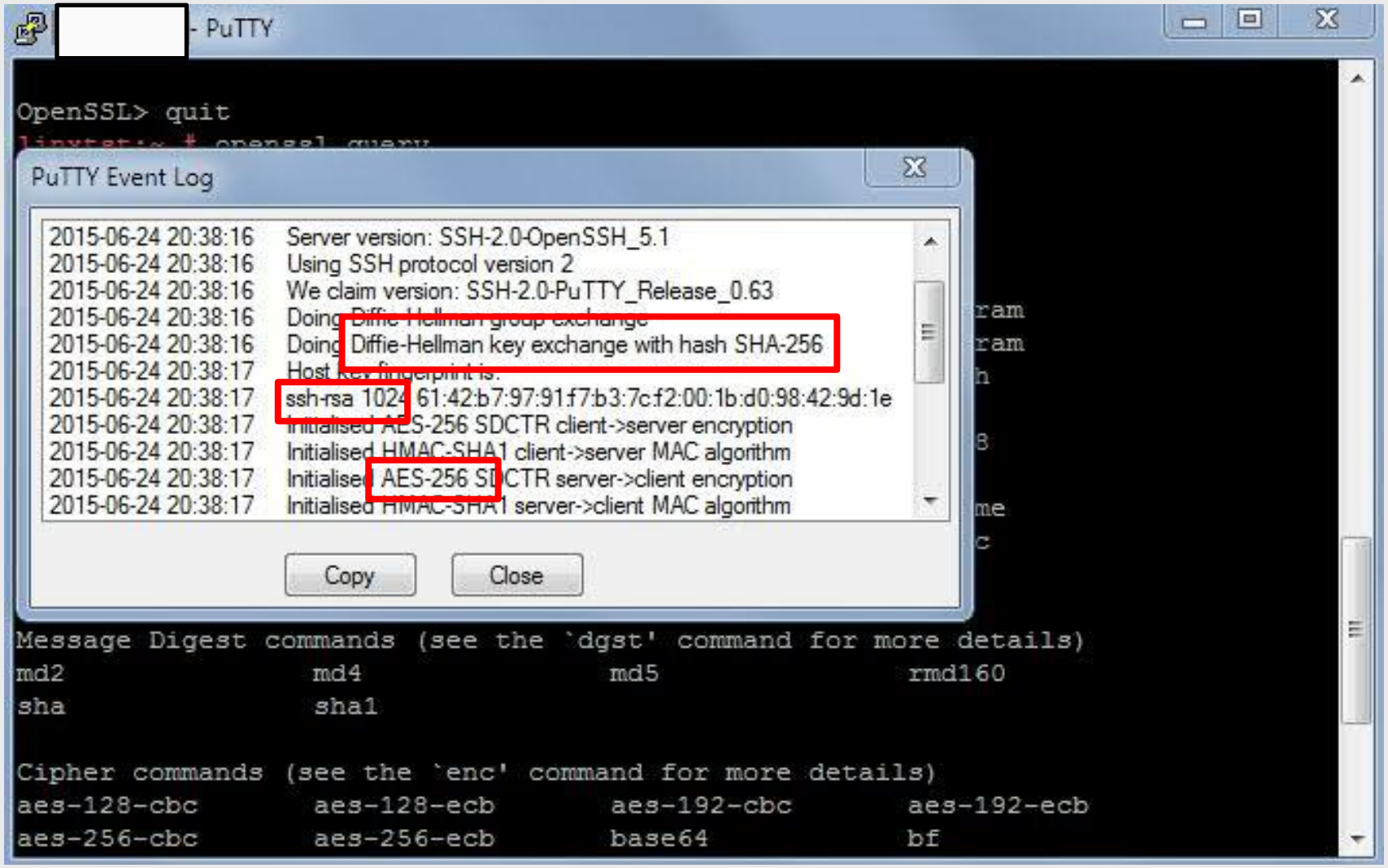
Brian W. Hugenbruch, CISSP
z/VM Security & Cryptography Product Owner
bwhugen@us.ibm.com

v7.5.1.a – May/June 2026

Who are we?

- **Steven Horvath**
  - z/VM I/O Development
  - Guitar player and fan of metal \m/
  - Appreciates red ales
- **“Sir Brian, Wielder of the Security Hammer”**
  - Former lead singer for the z/VM Band
  - NCAA Div 1 Varsity Fencer
  - Fan of doppelbocks

Security looks complicated, and it happens quickly.



What just happened?

SSH connections and TLS connections use:

- **Asymmetric** key exchange to establish a connection
- **Symmetric** keys to encrypt bulk traffic
- **Hashing** to validate content integrity between source and target

That's a lot of math ... and it's processing power that adds up

- Happens for every secure operation (connection, application math, etc.)
- The bigger (more secure) the keys, the longer it takes
- Costs time, money

Why Use IBM Z and LinuxONE Hardware Cryptography?

- **Maximize Trust & reliability**
- **Minimize Cost**
  - Save money: offload expensive CPU workload
  - Save time: Faster crypto algorithms
- **Industry-leading security**
- **Regulatory compliance** starts at hardware

How should I configure my IBM Z and LinuxONE Crypto
(or: why you‘re here)

Let me counter with a few questions:

- *What workload are you running?*
- *What are your security requirements?*
  - *“Know your rules”*
  - *This changes if you’re running a cloud*
  - *This changes if you’re supporting multinational customers*
- *What are your mobility requirements?*
  - *Do you need z/VM Live Guest Relocation?*
  - *Do you have other plans for failover, planned outages, and HA/DR?*
  - *Who’d win in a fight – your business continuity team, or security team?*

Today’s Topics

IBM Z and LinuxONE Hardware Cryptography
(the parts of it, why it matters, what it means)

z/VM Virtualization of IBM Z and LinuxONE Cryptography
(and how to use it)

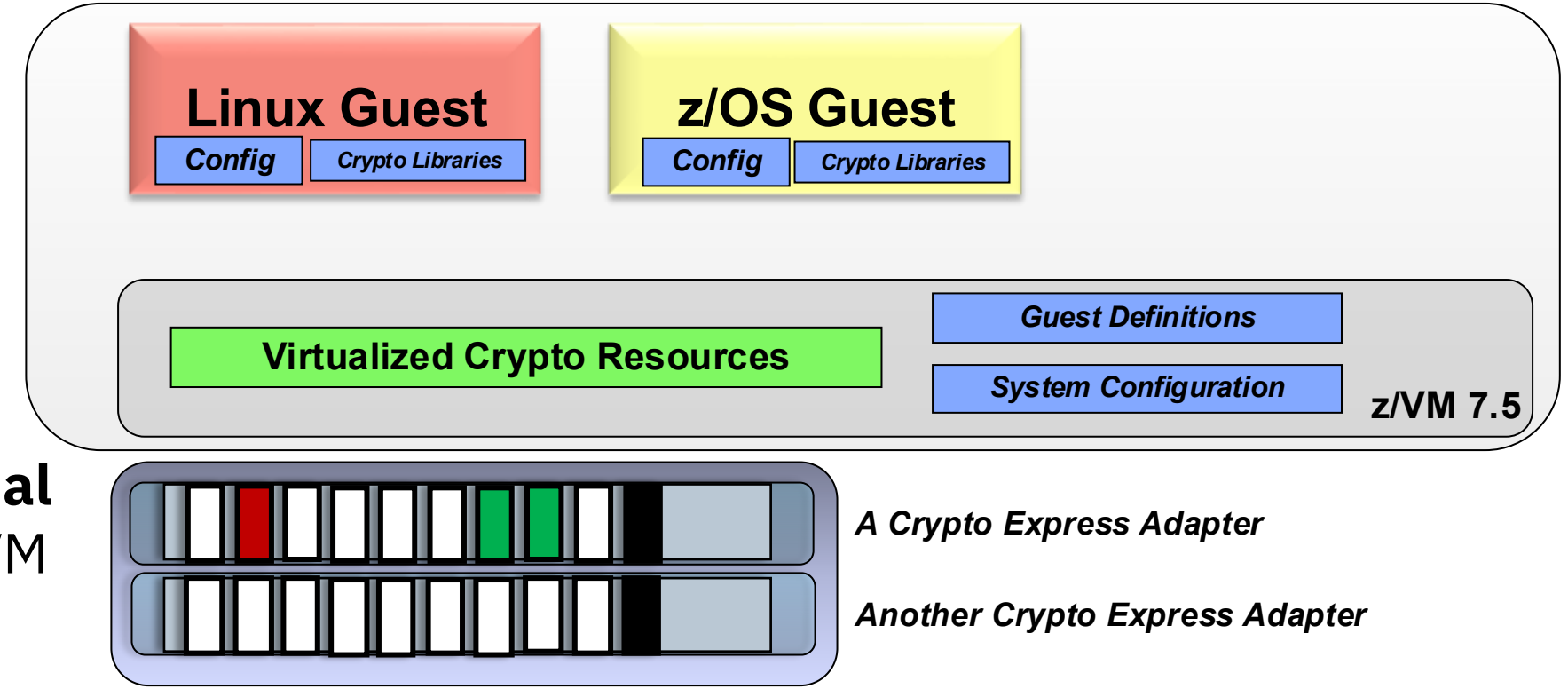
Guest Support: Operating Systems Running on z/VM

Extra: Frequently Asked Questions (if you don't ask them first)

IBM Z and LinuxONE Hardware Crypto Support

How To: Configure your Crypto on IBM Z and LinuxONE

1. Install the **features**
2. Configure **adapters** on HMC/SE
3. Configure your **hypervisor**
4. Configure your **virtual machines** at the z/VM level
5. Configure your **guest operating system(s)**



IBM Z and LinuxONE Integrated Cryptographic Hardware

CP Assist for Cryptographic Functions (CPACF)

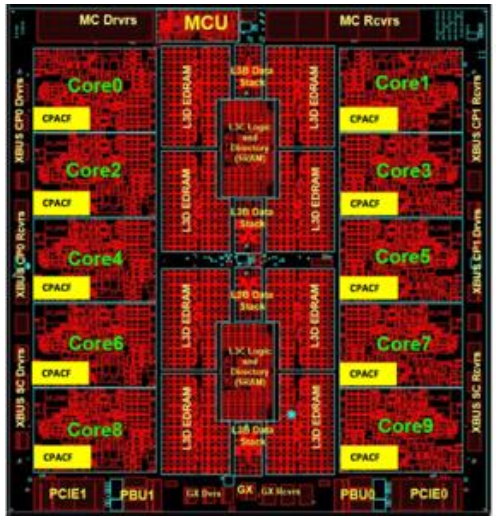
- Hardware accelerated encryption on every microprocessor core

Suited for high-speed bulk symmetric encryption

Crypto Express8S

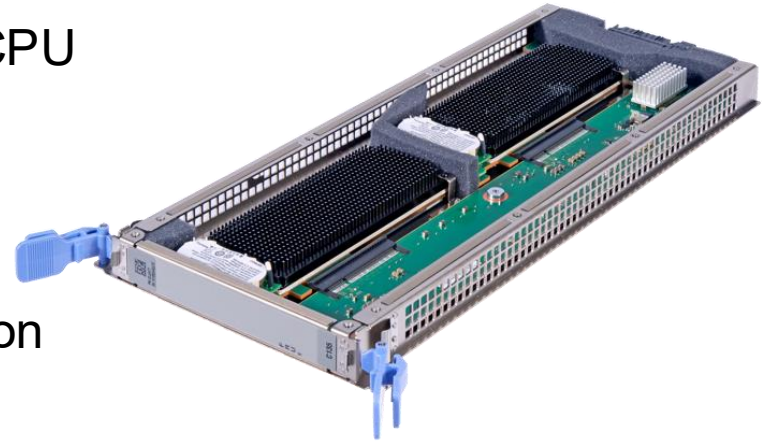
- PCIe Hardware Security Module (HSM)
- Industry leading FIPS 140-2 Level 4 Certification

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

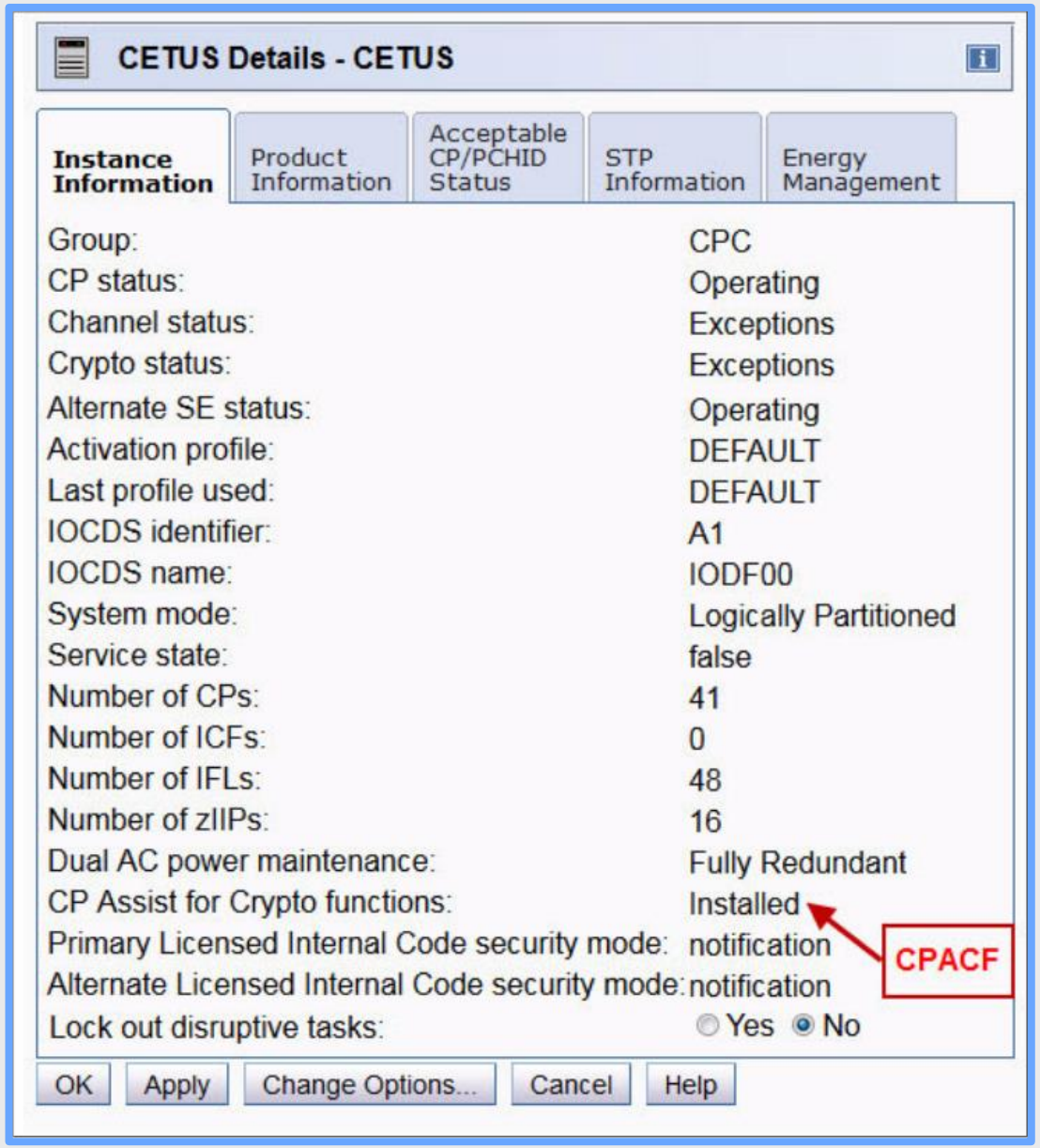


CP-Assisted Cryptographic Facility (CPACF)

No-charge feature on IBM Z and LinuxONE hardware (Feature 3863)

On-chip cryptographic acceleration and operations

Enablement required to use the Crypto Express hardware



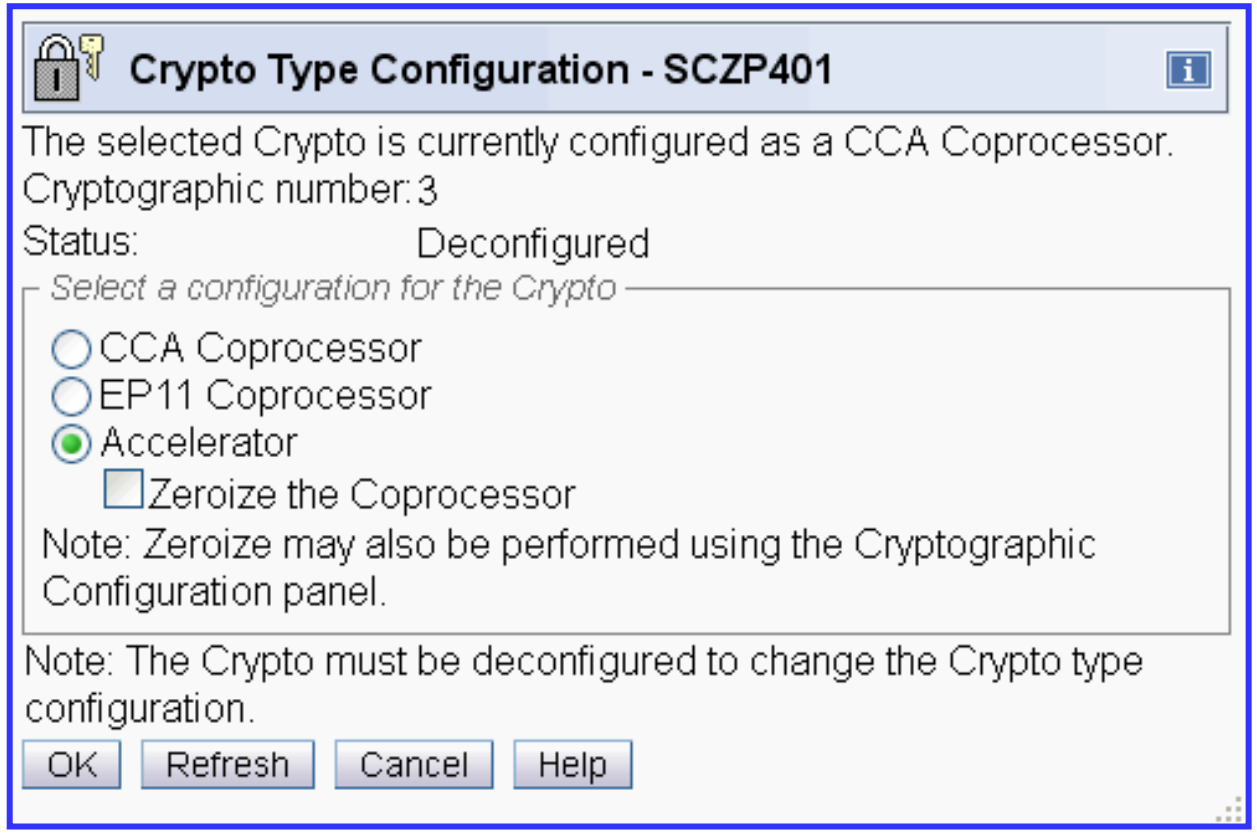
Setting Operational Mode for a Crypto Express Adapter (1/2)

Configuration for a Crypto Express feature is done on the **Hardware Management Console (HMC)**

– **Step 1**: Make sure CPACF is enabled.

– **Step 2**: Select adapter, then choose the operational mode

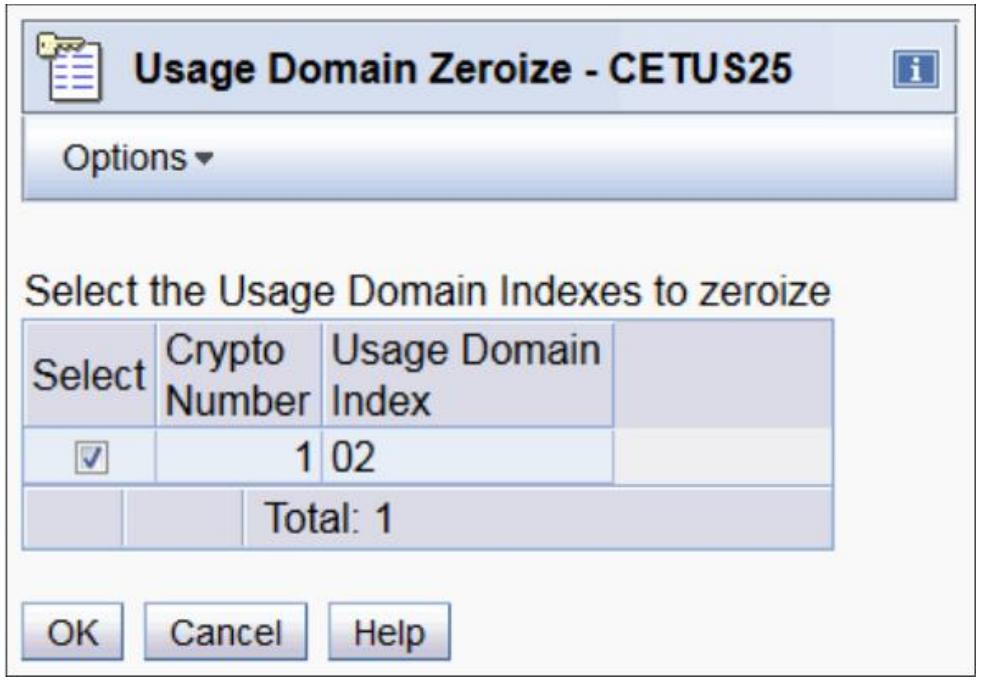
- Accelerator (clear key only)
- CCA Coprocessor (more security, HSM features)
- EP11 (open-source crypto framework, also has HSM features)

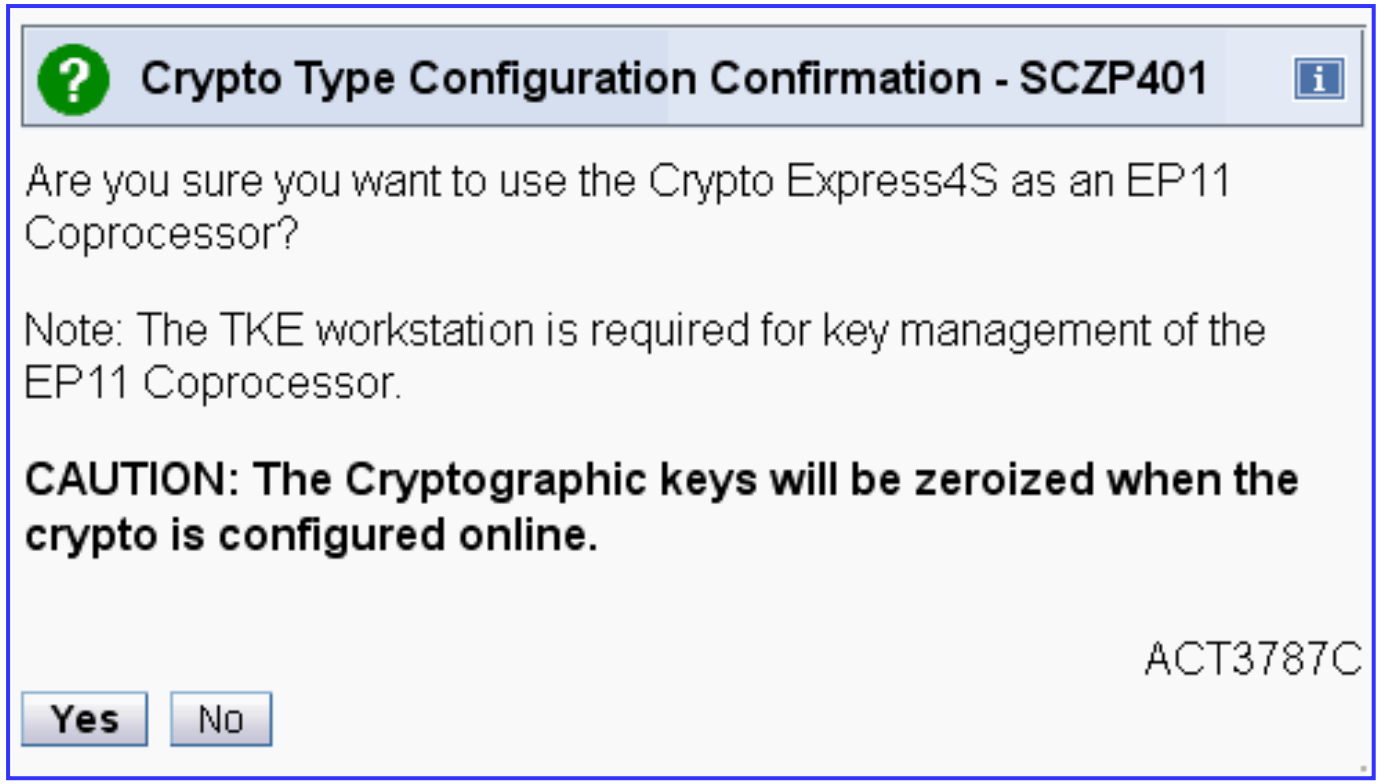


Setting Operational Mode for a Crypto Express Adapter (2/2)

Step 3: Validate option selection

- May zeroize existing keys in the process (destroy any residual secrets)

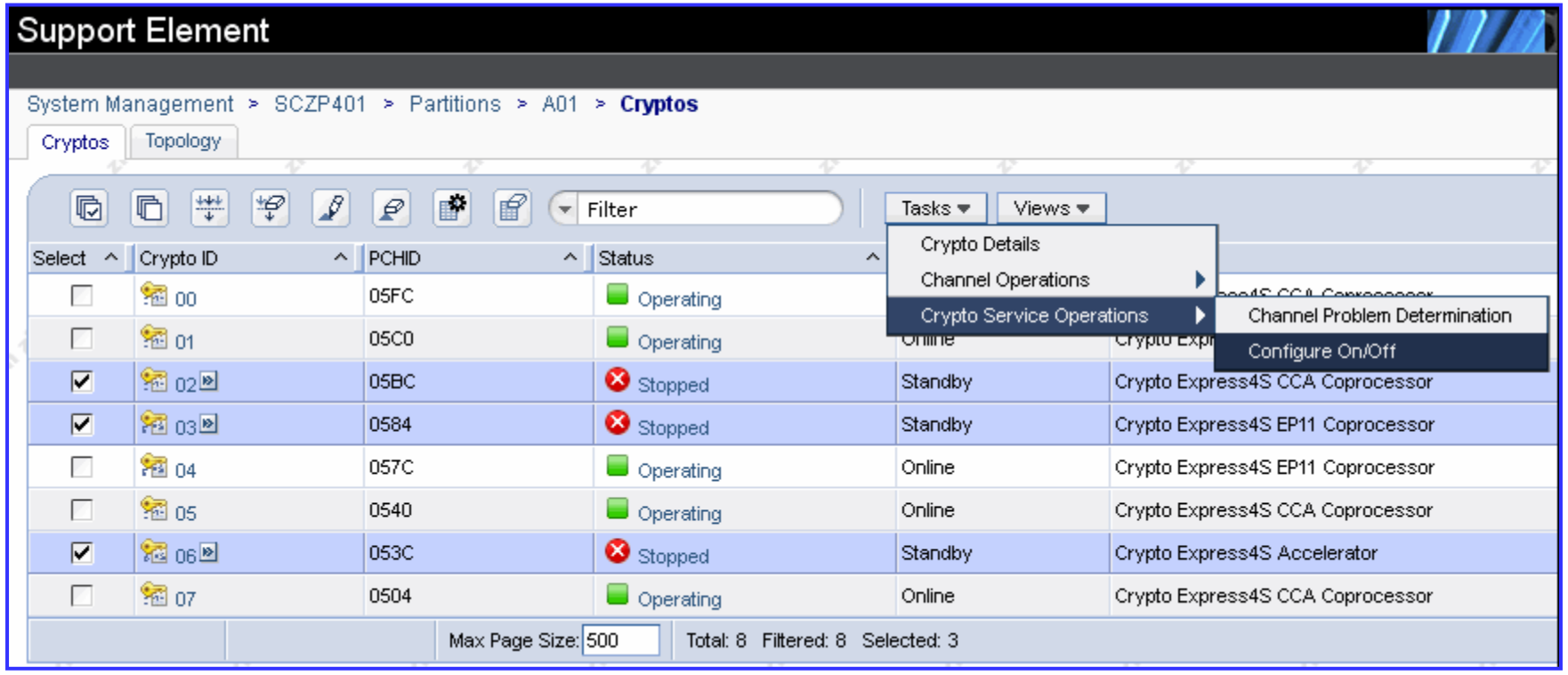




Activating a Crypto Express Adapter

Hardware activation is done from the **Support Element**

Select pertinent feature, "Configure On/Off"

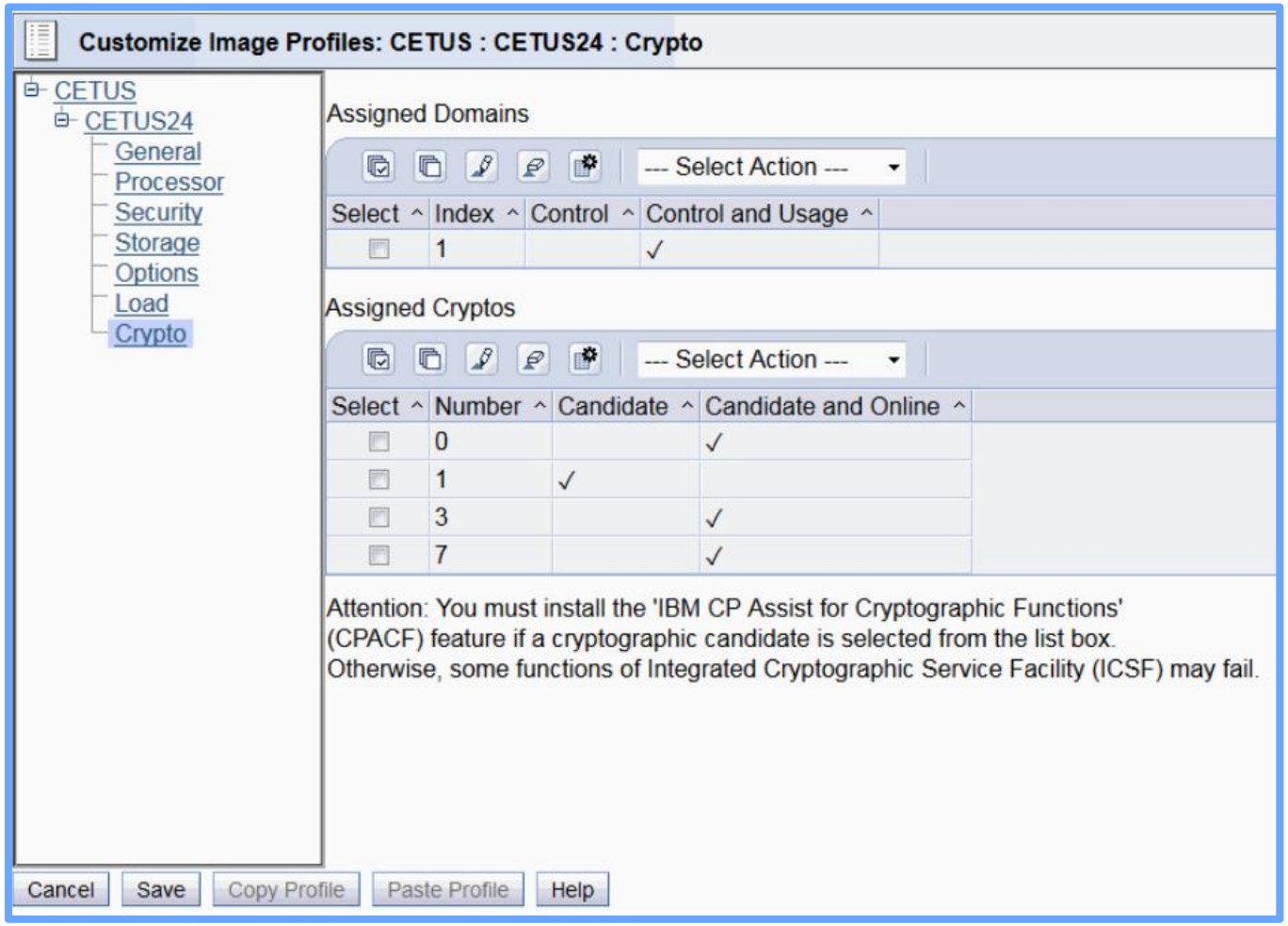


Attaching a Crypto Express logical domain to an LPAR

LPAR assignation is done from the **HMC** (building an activation profile)

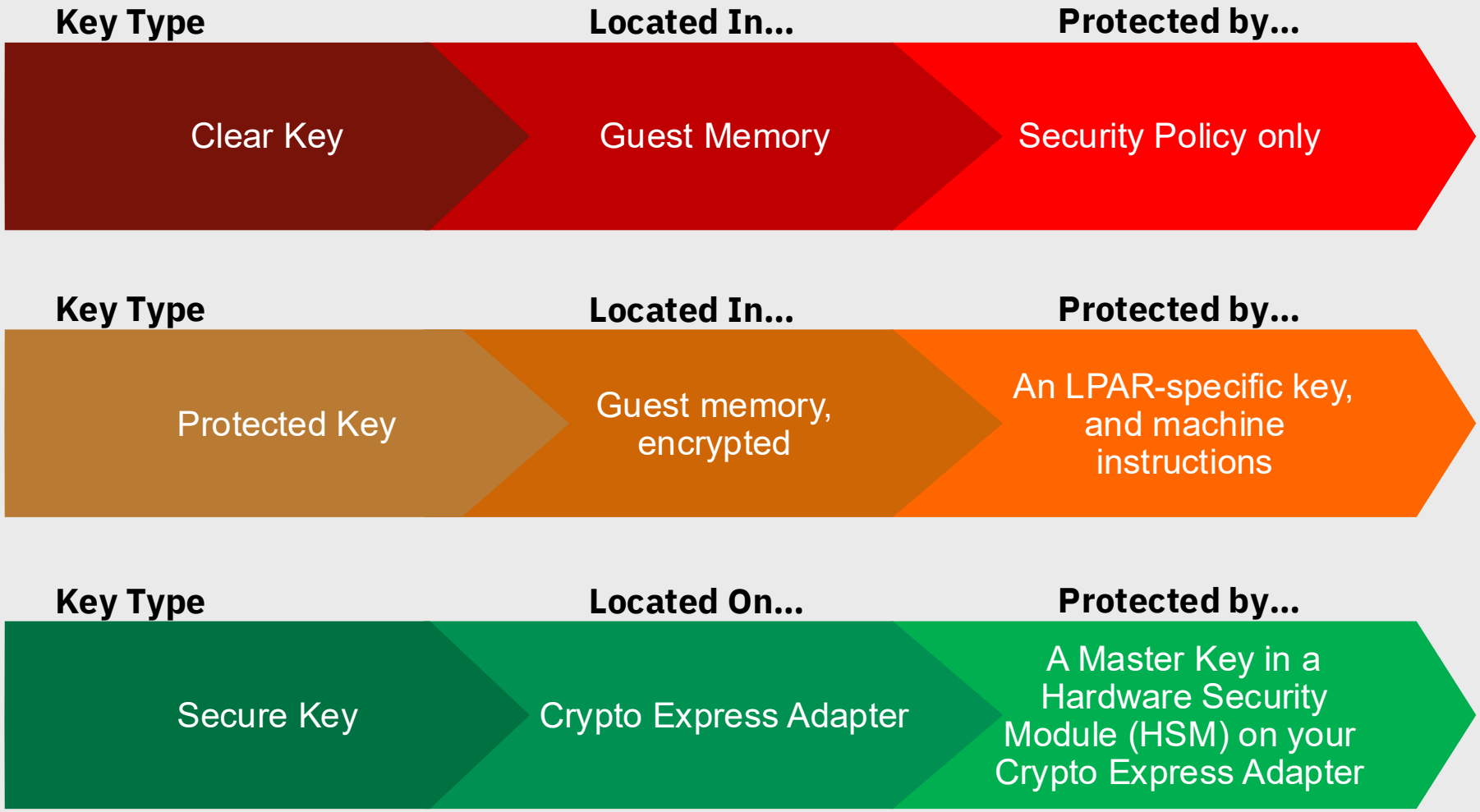
- **Candidate list**: domains on this adapter which are eligible to be accessed by this partition
- **Online List**: crypto resources automatically brought online at LPAR startup.
- **Usage Domain**: bundles domains across assigned adapters inside a common cryptographic boundary
- **Control Domain**: identifies domain index pertinent to TKE control of the LPAR. *If the Usage Domain is checked, the Control Domain must also be checked.*

z/VM will only detect those adapters and domains assigned to the LPAR



IBM Z and LinuxONE Operational Keys: Clear, Protected, or Secure

- Clear Keys are not encrypted. **Crypto operations may be performed in CPACF or on a Crypto Express adapter**
- Protected keys are encrypted under a CPACF wrapping key. **Crypto operations are performed only using CPACF**
- Secure keys have key values that are encrypted by a Master Key on a tamper-responding **Crypto Express adapter**.



Getting Keys into Your Crypto Express features

Trusted Key Entry (TKE) Workstation – an optional priced feature which communicates directly with the Crypto Express features over a secure TCP/IP connection.

- Functions as a separate physical device to the side of your IBM Z or LinuxONE
- Card reader for crypto secret storage
- Generates new secrets, stores data in Crypto Express domains
- Required if running Crypto Express features in EP11 mode!

z/OS Integrated Cryptographic Services Facility (ICSF) – a base component which allows interaction with Crypto Express features. (Requires z/OS; only for installing keys in CCA mode).

Panel and Catcher Utilities for Linux – **Panel** is a Linux package installed as part of the IBM .rpms which allows for key management function. **Catcher** is the Linux daemon for communicating with TKE.

- `/opt/IBM/CEX8C/bin/panel.exe`

IBM Unified Key Orchestrator (UKO) – previously EKMF and/or ACSP. A z/OS-based product for key lifecycle management

- https://www.ibm.com/products/unified-key-orchestrator-for-zos

IBM Key Protect for IBM Cloud– a cloud offering for key storage and retrieval.

- https://www.ibm.com/products/key-protect

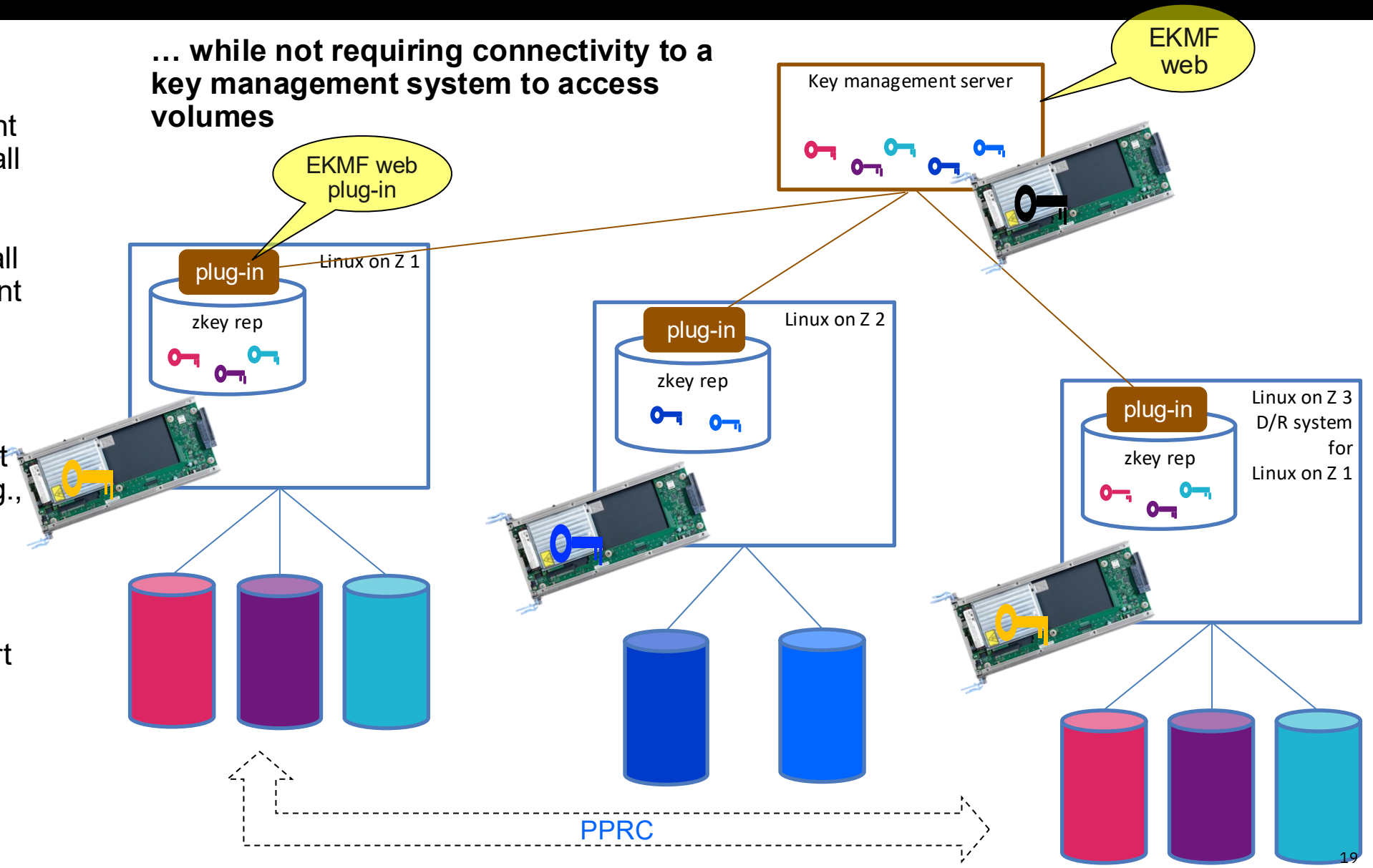
zkey now connects to UKO

upstream: new KMIP plug-in for KMIP server (GKLM, GDE)

Goal:
Allow for central enterprise key management system managing keys in all zkey repositories

- Generate and manage all keys on key management server
- Access control by key server:
- restrict key access to set of authorized clients (e.g., primary and backup systems)
- Simplify MK role procedures: just reimport from key management server

… while not requiring connectivity to a key management system to access volumes

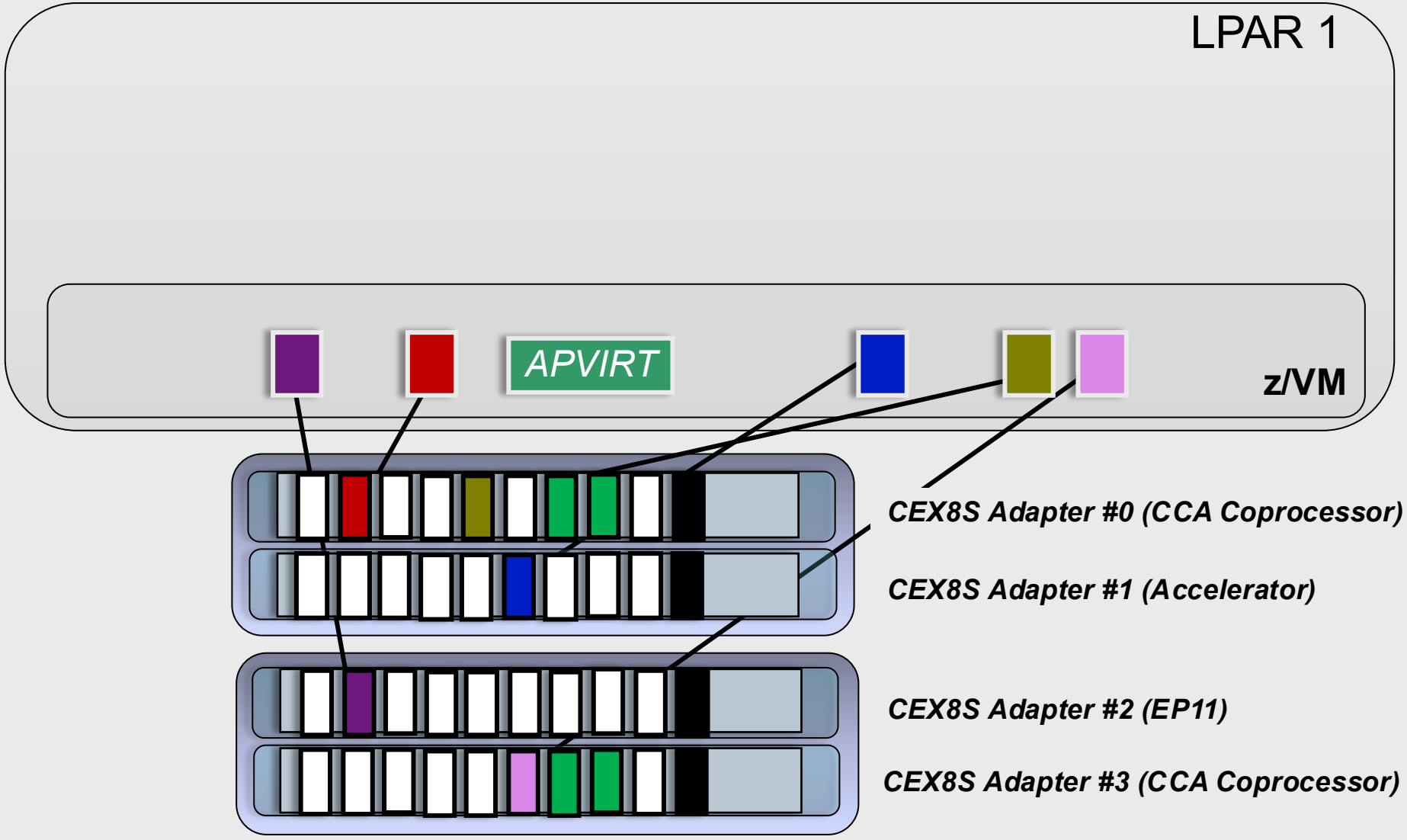


z/VM Support for Hardware Crypto

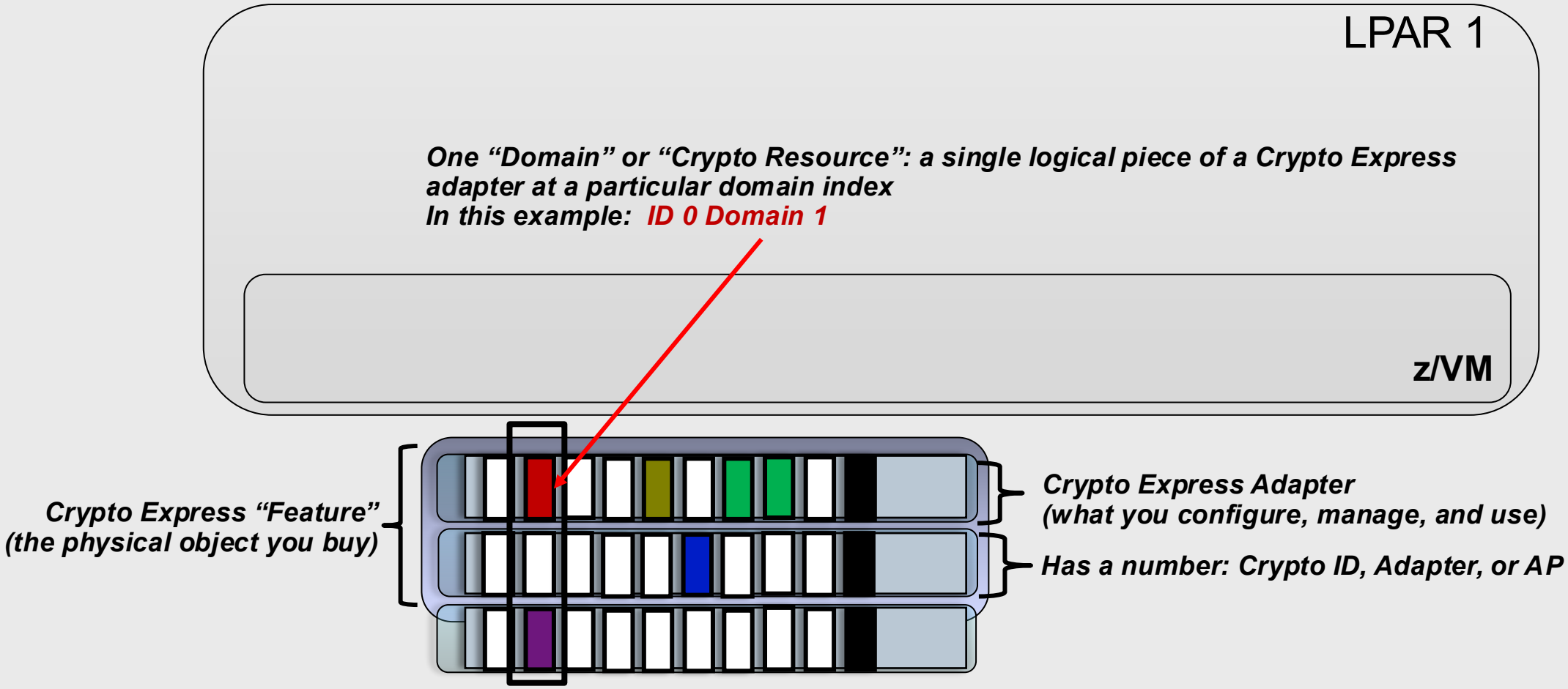
z/VM Virtualization of Hardware Cryptography (z/VM's view)

Once domains are assigned to a z/VM LPAR for use, they appear to the hypervisor and can be used by virtual machines.

z/VM sees crypto resources as virtual devices represented by a **Crypto ID** and a **domain index**.

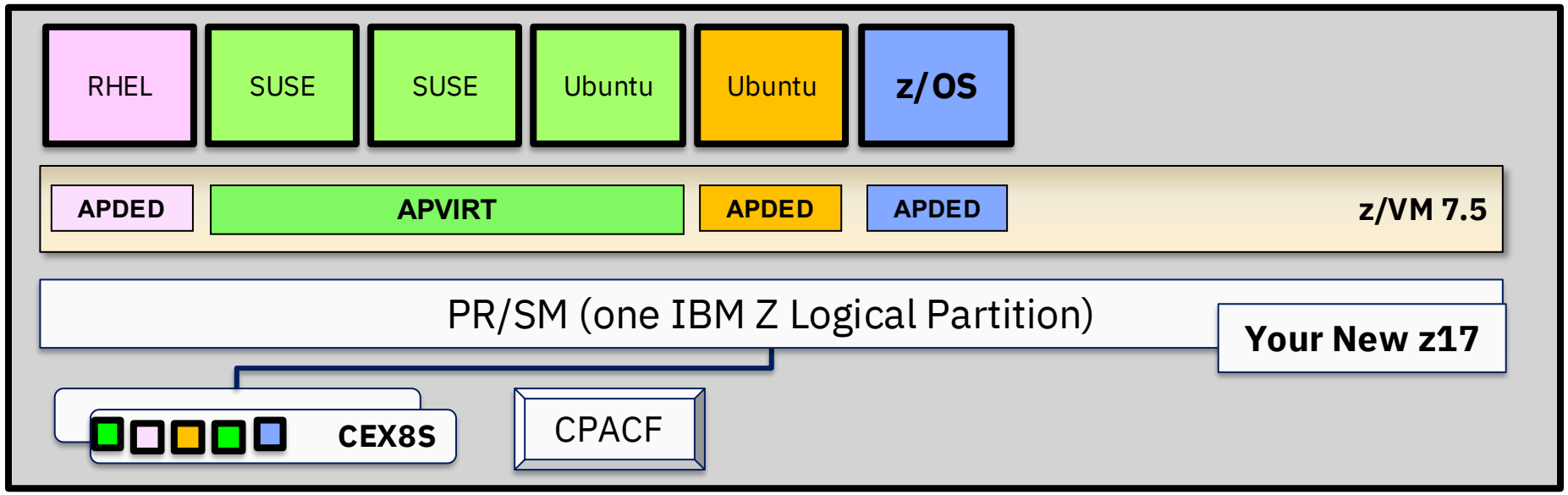


Your Crypto Lexicon (what the terms mean)



Intro to z/VM and Cryptographic Virtualization

Crypto Express adapters attached to your z/VM partition are **virtualized for the benefit of your guests**:



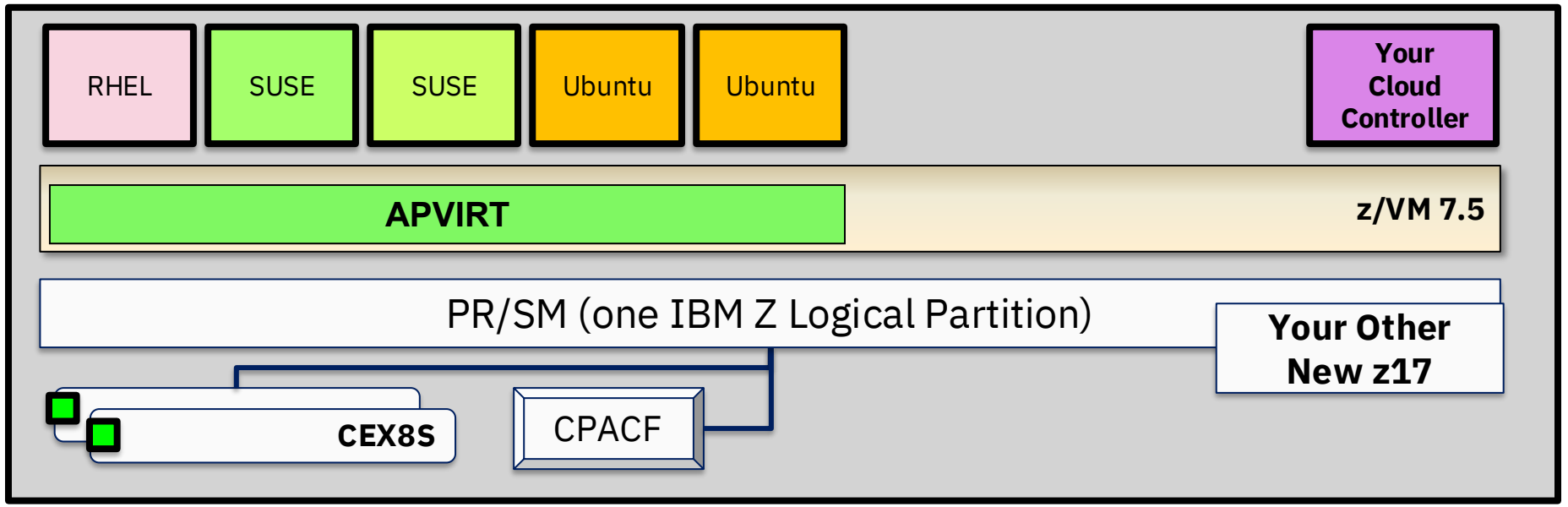
`Dedicated` (“APDED”)

Connects a particular Crypto Express domain (or multiple crypto resources) directly to a virtual machine – no hypervisor interference
All card functions are available to the guest

`Shared` (“APVIRT”)

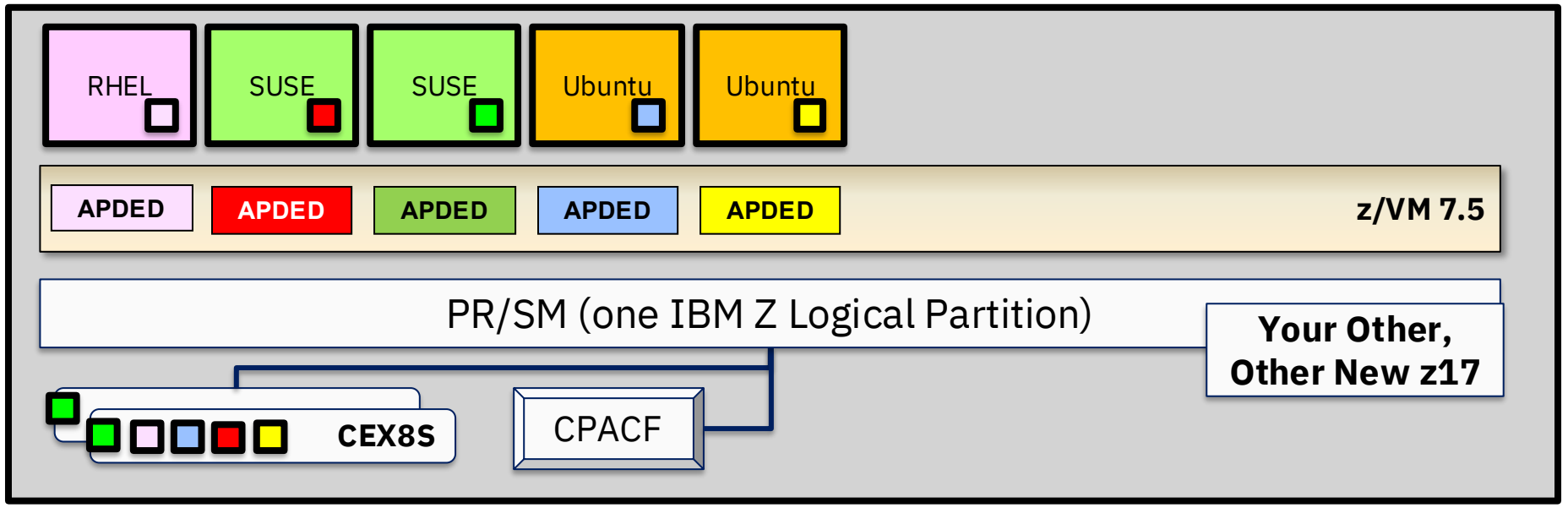
Virtual machine can access a collection of domains controlled by the hypervisor layer
Restricted to **clear-key operations only** – sharing crypto material might break security policy.

Sample of Virtualization: LinuxONE Developer Cloud



Crypto operations: SSH (RSA, SHA-2, AES), and *whatever data handled inside the guests*
Environmental Requirements: Guests must be relocatable (it's a cloud)
Recommended Hardware: CPACF and a Crypto Express Accelerator in shared configuration ("APVIRT")
– Assign 1 domain from 2-3 different adapters (for hardware failover and better performance)

Sample of Virtualization: a “roll your own” Hyperledger fabric



Crypto operations: A lot. It's a Blockchain

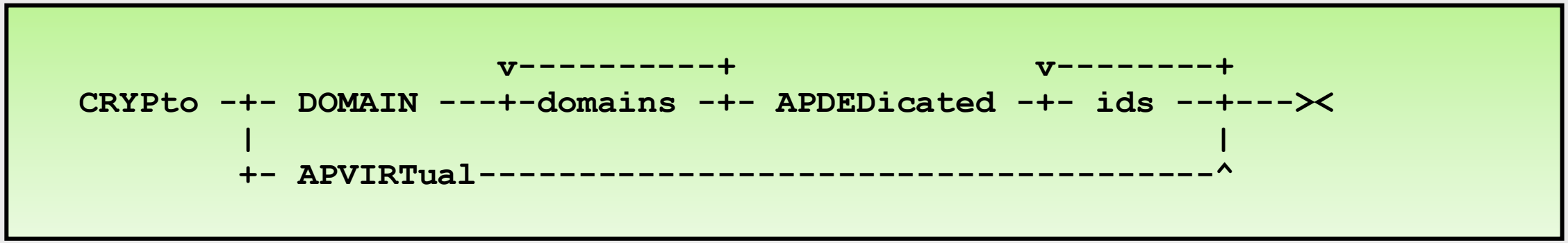
Environmental Requirements: Protection of key material. (It's a Blockchain.)

Recommended Hardware: CPACF and Crypto Express adapters in EP11 (PKCS #11) mode

- One domain per guest participating in the Hyperledger fabric

z/VM Virtualization of Hardware Cryptography

The **CRYPTO User Directory statement** grants a z/VM userid access to crypto resources associated with the Crypto Express adapters:



Notes:

- Guests should not try to dedicate the same domains *(first to IPL wins, all others complain)*
- Guests with a dedicated crypto resource may not be relocated
- Guests may not have both dedicated and shared crypto resources
- Shared crypto resources are limited to clear-key (Accelerator) mode only

Assigning Domains to APVIRT

The CRYPTO APVIRT statement in your System Configuration file allows you to request particular crypto resources (by Crypto ID and domain index) to be assigned to hypervisor's list of **shared crypto resources**:

```
CRYPTO APVIRT AP 1 DOMAIN 0 1
CRYPTO APVIRT AP 0 DOMAIN 22
```

Usage Notes:

- z/VM will designate the first available domain in this list as the designated type (hardware + mode)
- Any other available domains in SYSTEM CONFIG also of that type are designated for shared usage
- Domains that do not meet criteria are ignored.
- If no domains meet criteria, no APVIRT usage will be allowed
- EP11 domains (and adapters) may not be used for shared use or assigned to APVIRT

If this statement is not present in the System Configuration file, z/VM will select two available domains, with a preference for Accelerator mode domains on the latest hardware.

CRYPTO APVIRT NONE

z/VM 7.4
Feature Pack 04 Fix 00
PTF for APAR VM66891

But what if you don’t want shared crypto devices provided by your hypervisor?

```
CRYPTO APVIRT NONE
```

Usage Notes:

- Place anywhere in the System Configuration file
- Will override any other CRYPTO APVIRT statements
- If not specified, assignment to APVIRT proceeds as described

Assigning Domains to APVIRT

Given the following System Configuration:

```
CRYPTO APVIRT 1 2 DOMAIN 7 8
CRYPTO APVIRT 4 DOMAIN 9
```

… z/VM will check domains in the following order:

```
AP 1 DOMAIN 7          /* CEX8A */
AP 1 DOMAIN 8          /* CEX8A */
AP 2 DOMAIN 7          /* CEX7A */
AP 2 DOMAIN 8          /* CEX7A */
AP 4 DOMAIN 9          /* CEX6C */
```

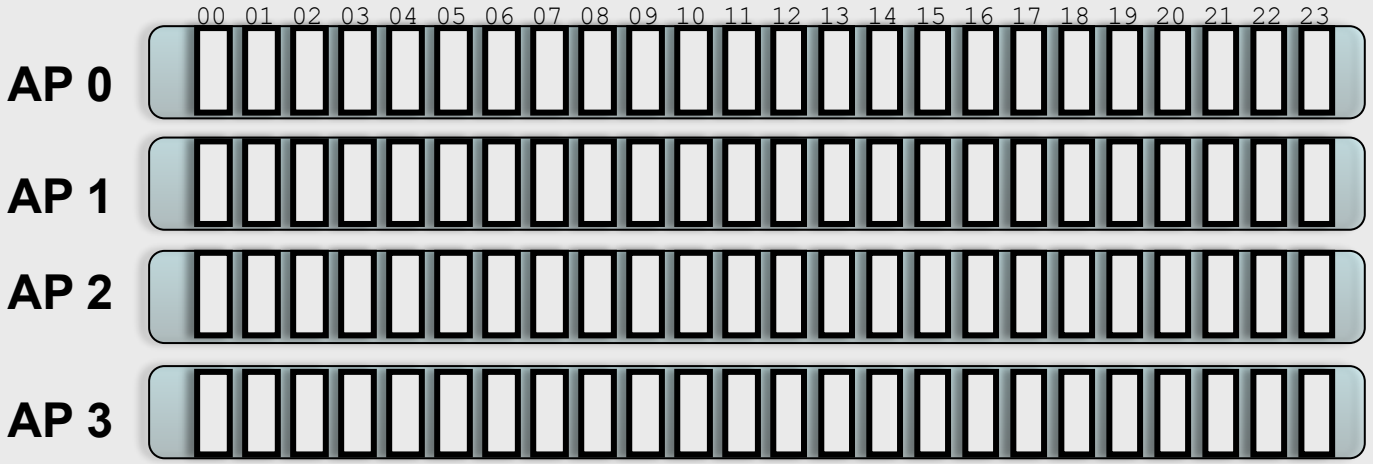
If **AP 1 DOMAIN 7** is available at system initialization, it will be APVIRT.

- APVIRT must then use type CEX8A
- Only AP 1 DOMAIN 8, with a matching type and mode, is set as APVIRT
- If a guest lists AP 1 DOMAIN 7 as **APDED**, the guest will be denied access

Example: Static Assignment of Domains for z/VM Guests

```
System Configuration:  CRYPTO APVIRT  AP 1-2 DOMAIN 15-16
Guest A:  CRYPTO DOMAIN 13-18 APDED 0-3
/* Conflicts on AP 1-2; no domains granted on AP 1 or 2. */
Guest B:  CRYPTO DOMAIN 11-14 APDED 0
/* Conflict at Domain 14. No Domains granted on this AP. */
Guest C:  CRYPTO DOMAIN 2 APDED 0-3
/* No conflicts. */
```

Reverse the logon order of Guest A and Guest B ...



Mixed-APVIRT Live Guest Relocation

Mixed-APVIRT LGR allows flexible crypto configurations so guests using APVIRT can relocate with fewer hardware restrictions.

Removes restrictions on guest relocation in a z/VM Single System Image:

- *Then*: needed common type and mode (e.g., CEX8A) on source and target system
  - including firmware levels
- *Now*: guests in a relocation domain see lowest type of a common mode
  - E.g., a combination of CEX7A and CEX5A is seen as a CEX5A by all guests in that domain
  - Guests without a need to relocate, or in specialized domains, can see higher levels
  - Still requires common adapter “mode” (Accelerator or Coprocessor; EP11 cannot be relocated)

Control-Only Access for Guest Crypto Domains

z/VM 7.4
Feature Pack 04 Fix 00
PTF for APAR VM66891

Pain point: a Linux guest under z/VM needs dedicated access to a crypto resource to update keys

- Caused by a lack of granularity in virtualization of domains (always CONTROL+USAGE)
- Previous client usage leaned heavily on APVIRT, but *Linux dm-crypt* is causing a rise in APDED use

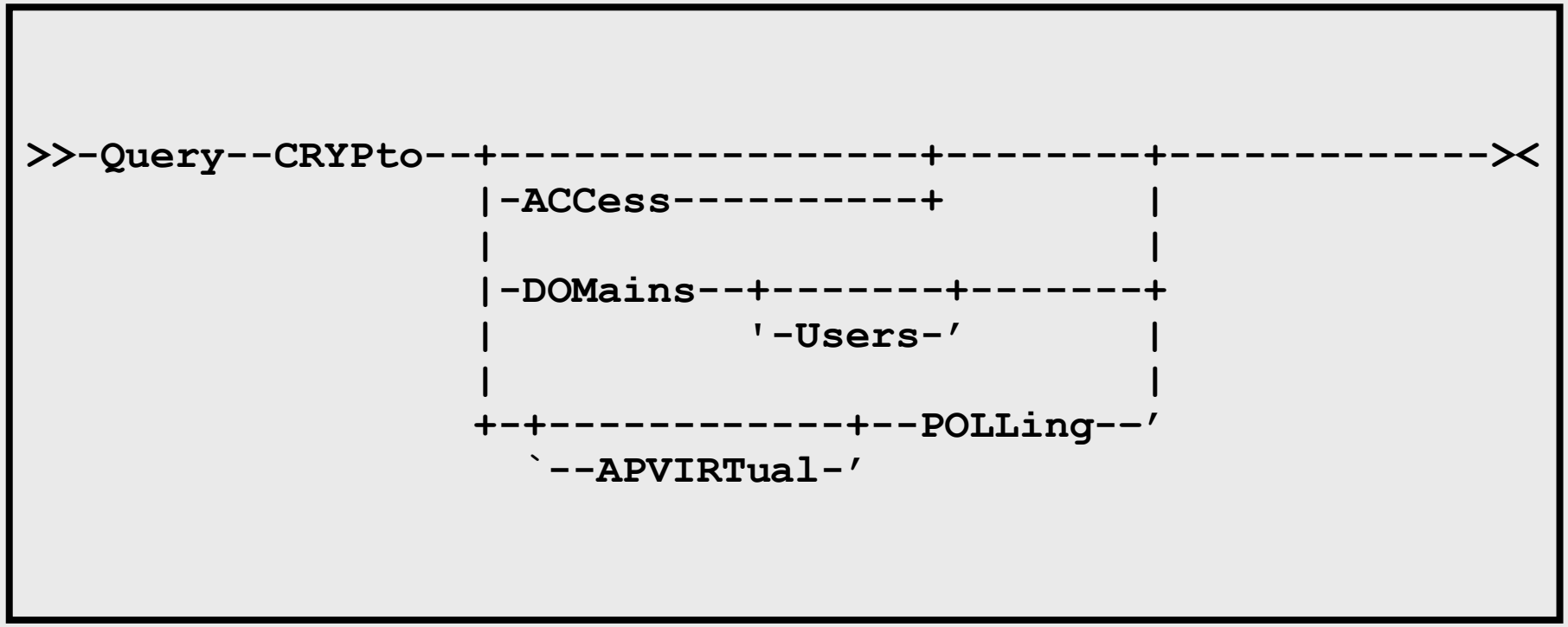
To be: dynamic commands and virtual machine definition updates to specify CONTROL only access to crypto resources assigned to your z/VM partition

- Allows (as primary use-case) TKE catcher to run as a Linux guest under z/VM
  - Create a local “key manager guest”
  - No need to reassign domains to manage keys (disrupting operations) or to load Linux into that partition to manage keys (very much disrupting operations)

z/VM Virtualization of Hardware Cryptography

QUERY CRYPTO

(Class A, B, C, or E) will display which crypto resources are available to your z/VM system. Note that this list will be limited to adapters and domains associated with a z/VM instance.



z/VM Virtualization of Hardware Cryptography

```
QUERY CRYPTO DOMAINS USERS
```

Crypto ID	device	Domain Index	device status	config state	planned crypto resource usage
AP 001	CEX8A	Domain 010	operational	online	free, dedication planned
AP 001	CEX8A	Domain 011	operational	online	free, dedication planned
AP 001	CEX8A	Domain 084	operational	online	free
AP 002	CEX8C	Domain 010	resetting	online	free, dedication planned
AP 002	CEX8C	Domain 011	resetting	online	free, dedication planned
AP 002	CEX8C	Domain 084	resetting	online	shared
AP 003	CEX8C	Domain 010	operational	online	attached to BWHUGEN
AP 003	CEX8C	Domain 011	operational	online	attached to BWHUGEN
AP 003	CEX8C	Domain 084	operational	online	shared

Notes:

- **Device Status** can be operational, resetting, checkstop, deconfigured, busy, revoked, unsupported
- **Configuration State** can be online or offline. **These are logical states (how the card looks to z/VM)**
- **Device assignment** can be **free, dedication planned; attached to *userid;* free; shared**

z/VM Virtualization of Hardware Cryptography

```
QUERY CRYPTO DOMAINS USERS
```

Crypto ID	device	Domain Index	device status	config state	planned crypto resource usage
AP 000	CEX7C	Domain 009	control-only	online	attached, control-only
AP 000	CEX7C	Domain 010	control-only	online	attached, control-only
AP 000	CEX7C	Domain 029	operational	online	free, dedication planned
AP 000	CEX7C	Domain 030	operational	online	free
AP 000	CEX7C	Domain 031	operational	online	attached to TRACYK

Notes:

- **QUERY CRYPTO DOMAINS cannot tell if a domain is attached for control-only purposes**

z/VM Virtualization of Hardware Cryptography

z/VM 7.4
Feature Pack 04 Fix 00
PTF for APAR VM66891

```
QUERY CRYPTO ACCESS
```

Crypto ID	device	Domain Index	Full Access	Control-Only Access
AP 000	CEX7C	Domain 009	U+C: (unavail)	C: TRACYK
AP 000	CEX7C	Domain 010	U+C: (unavail)	C: TRACYK
AP 000	CEX7C	Domain 029	U+C: --------	C: --------
AP 000	CEX7C	Domain 030	U+C: --------	C: --------
AP 000	CEX7C	Domain 031	U+C: TRACYK	C: OPERATOR TKVIRT

Assigning AP Domains to z/VM Guests

The Big Question: Which type of adapter do I need, and what domains do I want to assign to my guest?

It depends:

- Do you need secure key operations? (APDED)
- Does your security policy require physical isolation? (APDED)
- Do your guests need to exploit EP11 mode? (APDED **only**)
- Do you need to relocate your guest? (APVIRT*)
- Can you share your domains without impact to security or performance? (APVIRT)
- Are you running out of domains attached to the LPAR?
- Are your guests similar, cloned, or tied to HA solutions?
- Does your guest operating system have particular restrictions?

Different guests will have different needs, based upon their drivers and configuration requirements.

And, until recently, this meant a lot of planning, because changing your config at the LPAR level, or changing shared crypto resource assignments, meant a re-IPL of your z/VM system…

*Note: some restrictions apply. Consult the *CP Planning and Administration Guide* or *Getting Started With Linux* manuals.

Dynamic Crypto Support for z/VM

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

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.

z/VM Dynamic Crypto – Commands

VARY ONLINE CRYPTO (B)
- Bring a Crypto Express adapter online

VARY OFFLINE CRYPTO (B)
- Take a Crypto Express adapter offline (device associations remain in place)

ATTACH CRYPTO (B)
- Add crypto resource(s) to your z/VM guest (or APVIRT)

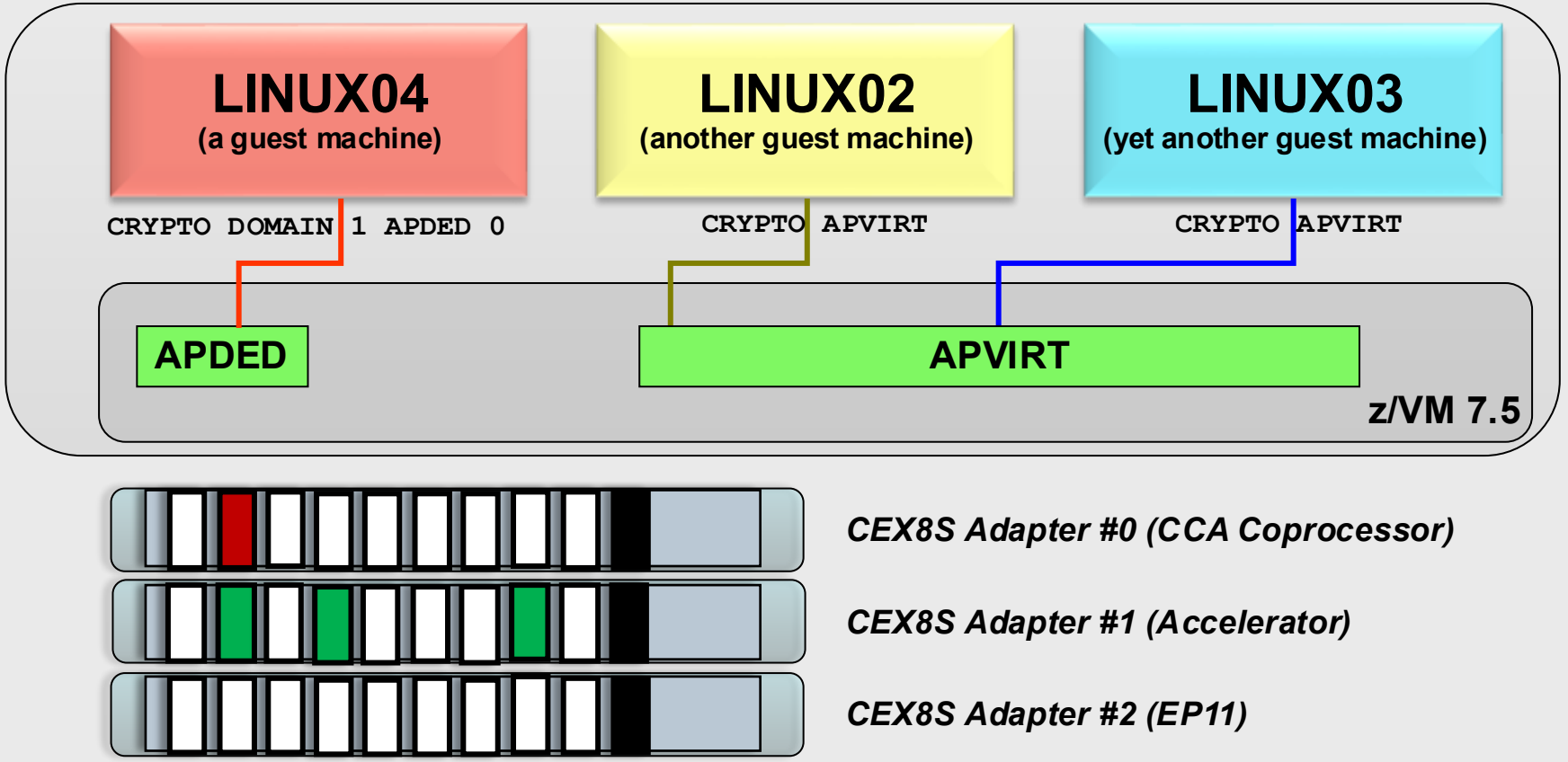
DETACH CRYPTO (B or G)
- Remove dedicated crypto resources from a guest
- Remove crypto resources from the shared crypto pool
- Remove guest access to the shared crypto pool

– **DEFINE CRYPTO** APVirtual (G)
- assign or reassign shared crypto resource access to a z/VM guest

– **QUERY CRYPTO DOMAINS** (per prior slides)

How To: Make a new adapter available to z/VM

`VARY ON CRYPTO 2`

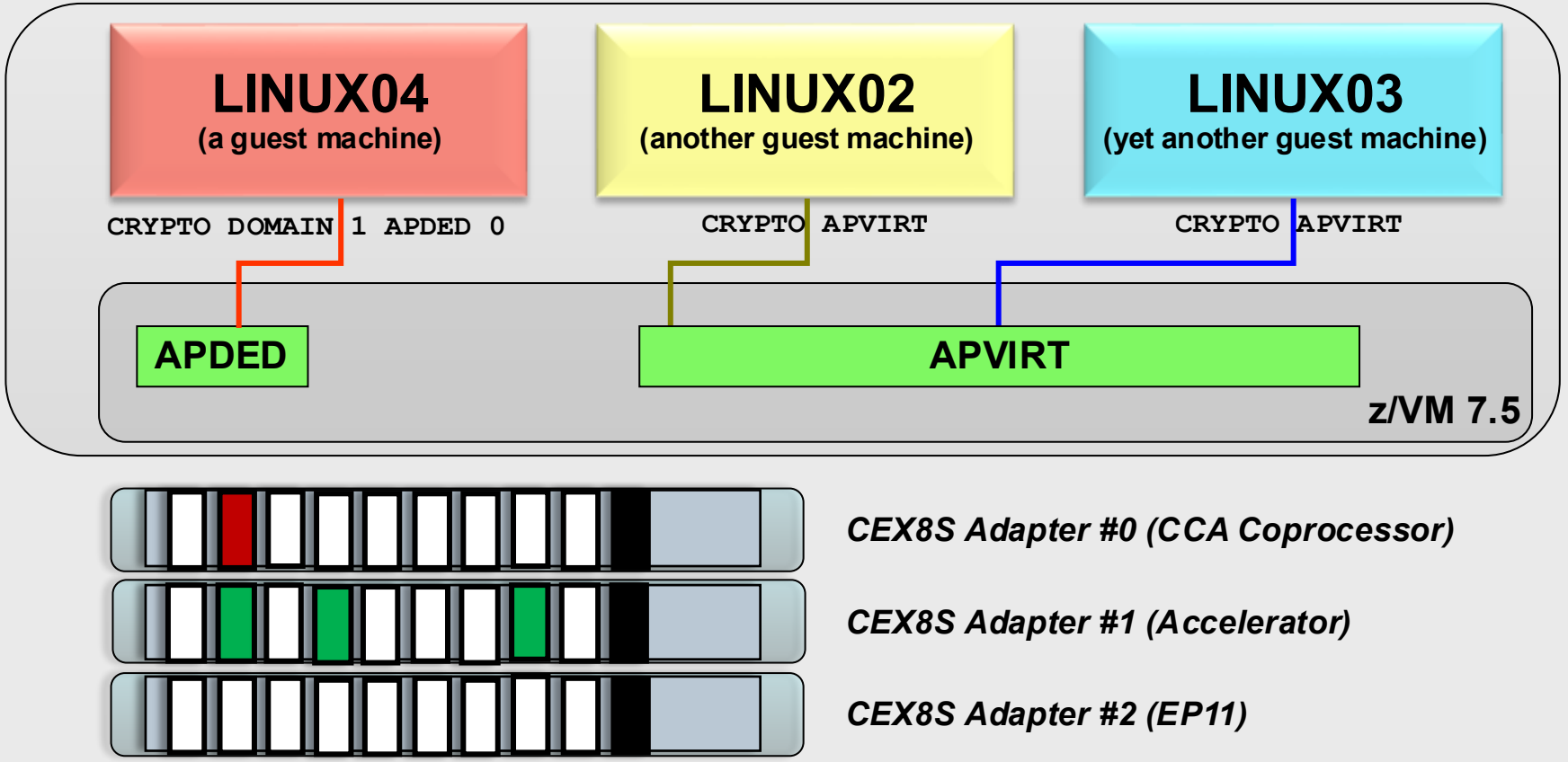


How To: Assign a crypto resource to a user

`ATTACH CRYPTO AP 2 to LINUX04`

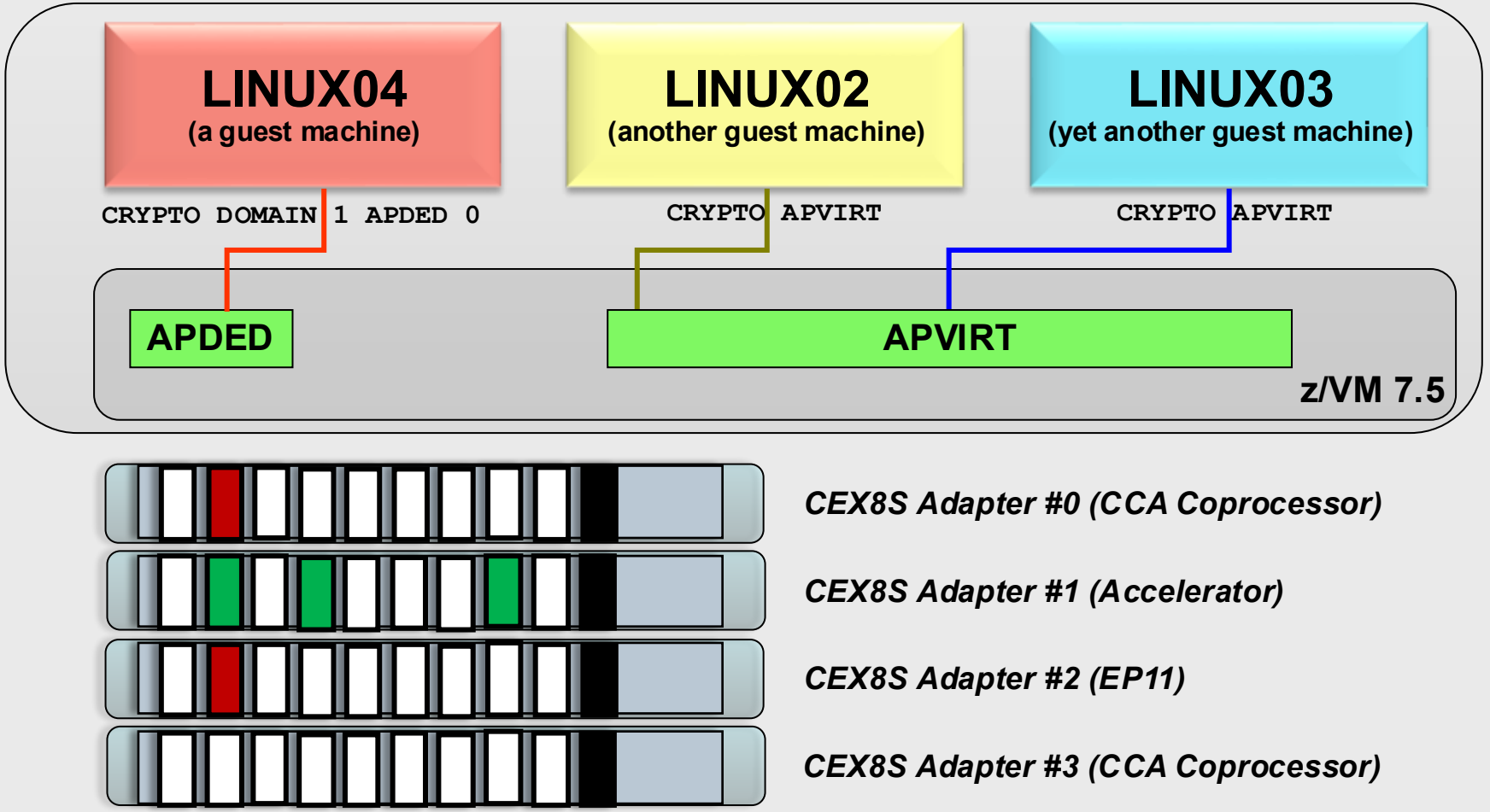
Warning: does not change your z/VM User Directory… so static configuration does not update automatically.

Don't forget to update your defaults!



How To: Assign new crypto resources for sharing

```
VARY ON CRYPTO 3
ATTACH CRYPTO AP 0 3 DOMAIN 6 7 to SYSTEM
```

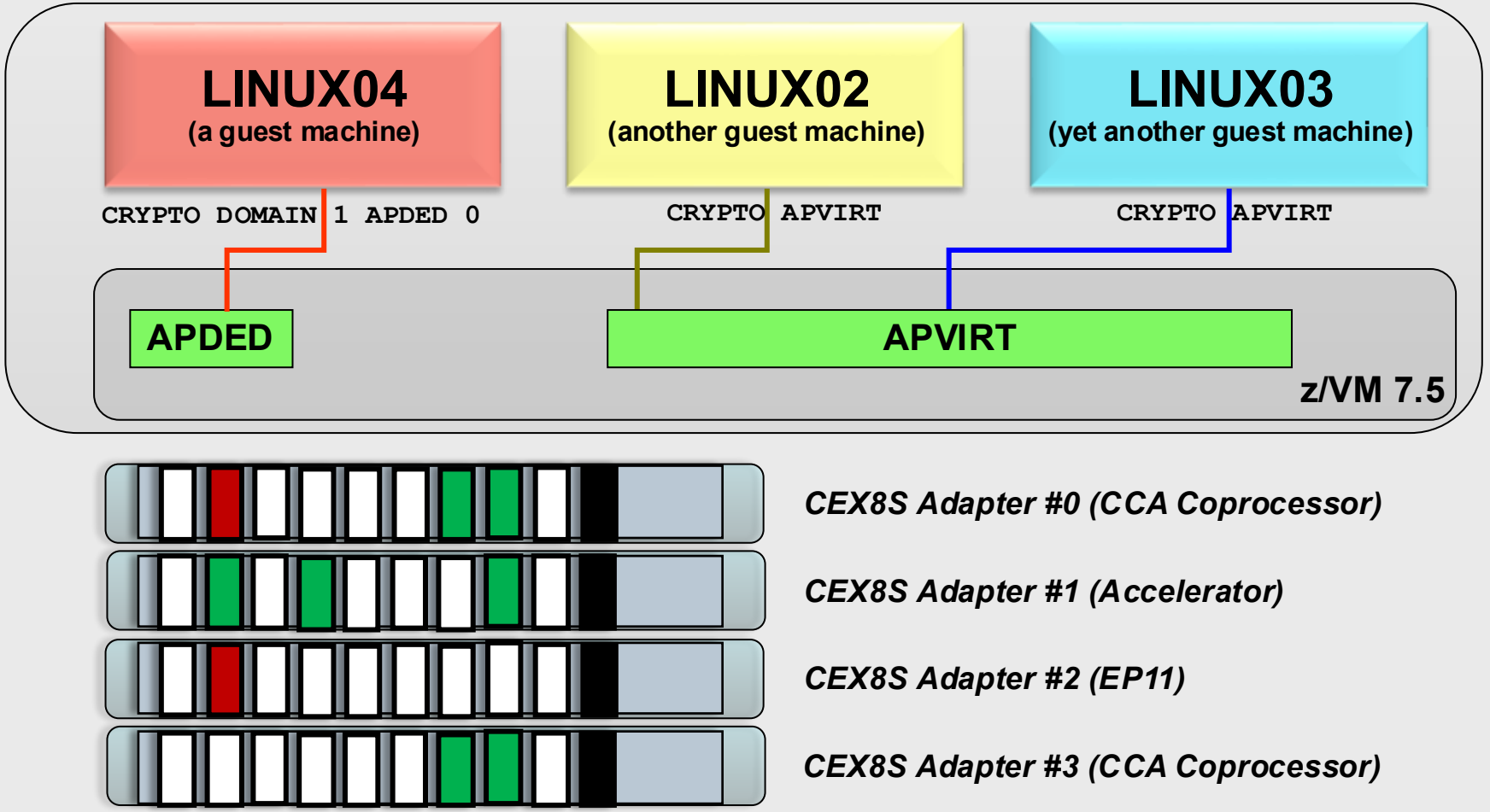


How To: remove crypto resources from shared pool

`DETACH CRYPTO AP 1 DOMAIN 1 3 7 from SYSTEM FORCE`

Change does not remove APVIRT access from the guests.

Note: this is an extreme example, you may not want to remove these all at once.



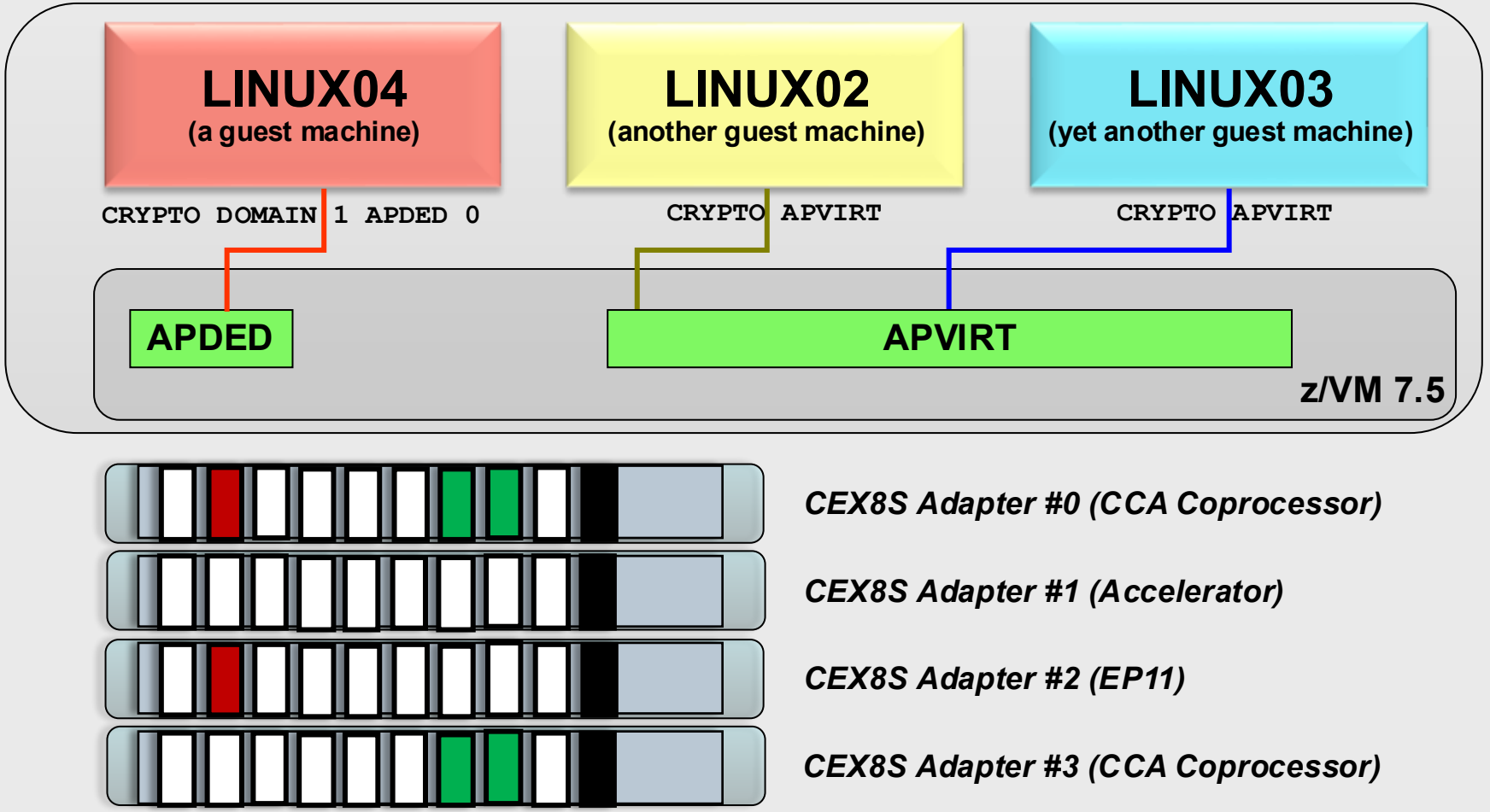
How To: Take an adapter offline

`VARY OFF CRYPTO 1`

Adapter will be listed as offline, and will not be available for use.

VARY ON the adapter to bring it back to active configuration…

…no IPL required.



z/VM Dynamic Crypto – Usage Notes

Attachments persist even when a device is taken offline

Resource assignment (dedicated/shared) does not change when an adapter is varied on/off

FORCE option:

- Not required when DETACHing from a user
- Required when VARYing OFF an adapter with crypto resources in use
- Required when detaching last resource from shared pool
- Exercise caution when using

The Importance of Cryptographic Hygiene

Dynamic Crypto gives you a lot of power to modify the environment

- This is a good thing and a bad thing
- **“With great power comes great responsibility.”**

z/VM does not zeroize domains before reassigning to a guest (or to APVIRT)

- We don’t want to make that assumption (traditionally, this is HMC territory)
- **This might lead to “residual crypto” (Ewww)**

Basic guidelines:

- Zeroize (at HMC) when changing adapter modes or changing security zones
- Changes between unused and APVIRT: safe (no key material involved)
- Changes involving clear-key APDED: consider zeroizing
- Changes involving secure-key APDED: definitely zeroize

See z/VM CP Planning & Administration, Chapter 5. Crypto Planning and Management
https://www.ibm.com/support/pages/zvm/library/740pdfs/74627104.pdf

Host Exploitation of Crypto Interruptions

With the PTF for APAR VM66534, z/VM V7.2 supports host crypto-interruption exploitation for APVIRT cryptographic resources in the shared pool. The host is not required to poll cryptographic resources for replies that are ready to be delivered to the guest.

- Some performance benefit may be derived from enabling this capability
- Enabled by setting APVIRT POLLING to OFF
  - Not enabled by default via z/VM V7.2 PTF (default state is “polling is on”)

Commands impacted:

- **SET CRYPTO APVIRT POLLING** – change setting for entire APVIRT pool
- **QUERY CRYPTO POLLING** – query POLLING state [ON/OFF]

```
QUERY CRYPTO POLLING
```

```
Shared-crypto polling is OFF
Ready;
```

z/VM Support for IBM z17

With the PTF for APAR VM66532, z/VM® 7.3 and 7.4 provide support to enable guests to exploit function on IBM z17® and LinuxONE Emperor 5 ®. The following crypto-relevant support is included:

- The Crypto Express8S (CEX8S) adapter, supported as a dedicated or shared resource. Dedicated guests are able to take advantage of all functions available with the CEX8S adapters, including assorted new enhancements and use of Quantum-Safe APIs.

  All crypto adapters that are configured in EP11 mode are reported with the 'P' suffix instead of the 'S' suffix (e.g., CEX8P).

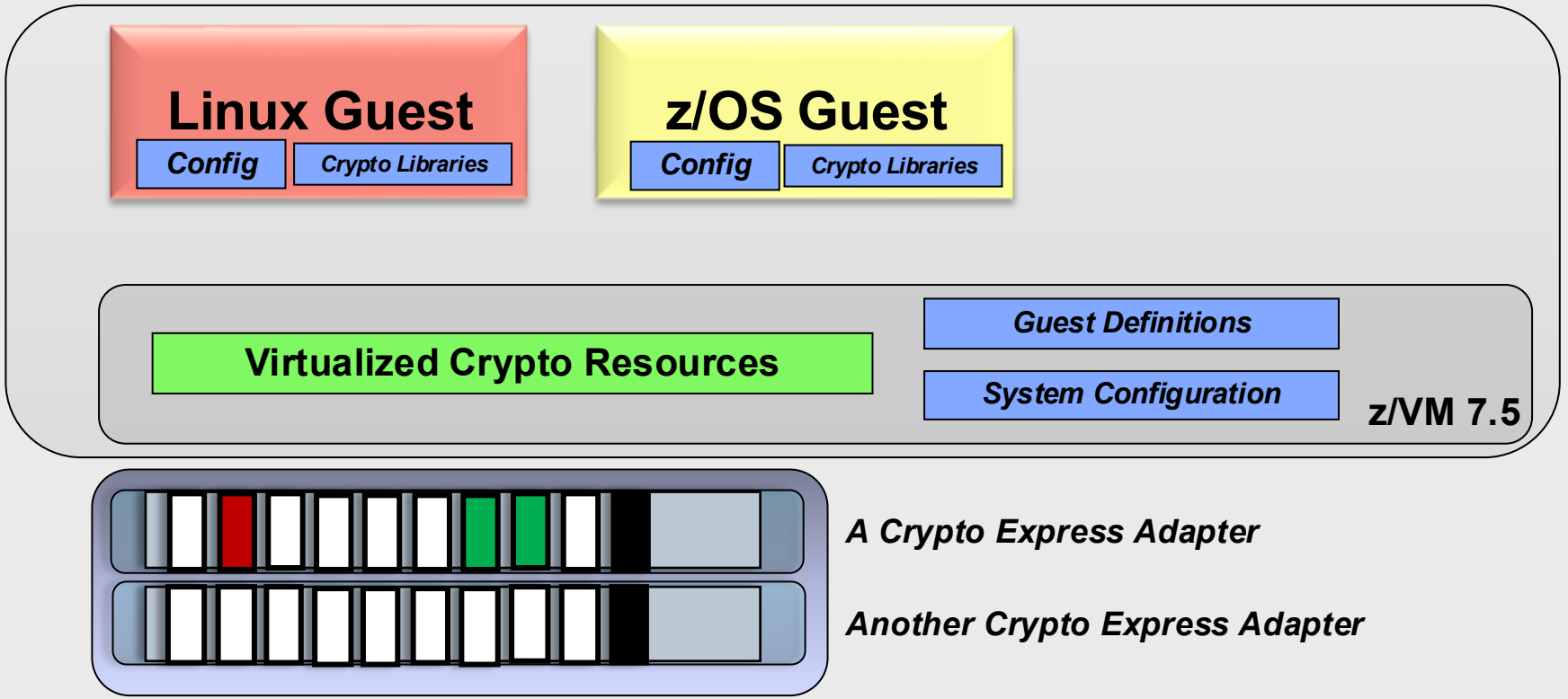
Guest Use of Hardware Crypto

How To: Configure your Crypto on IBM Z and LinuxONE

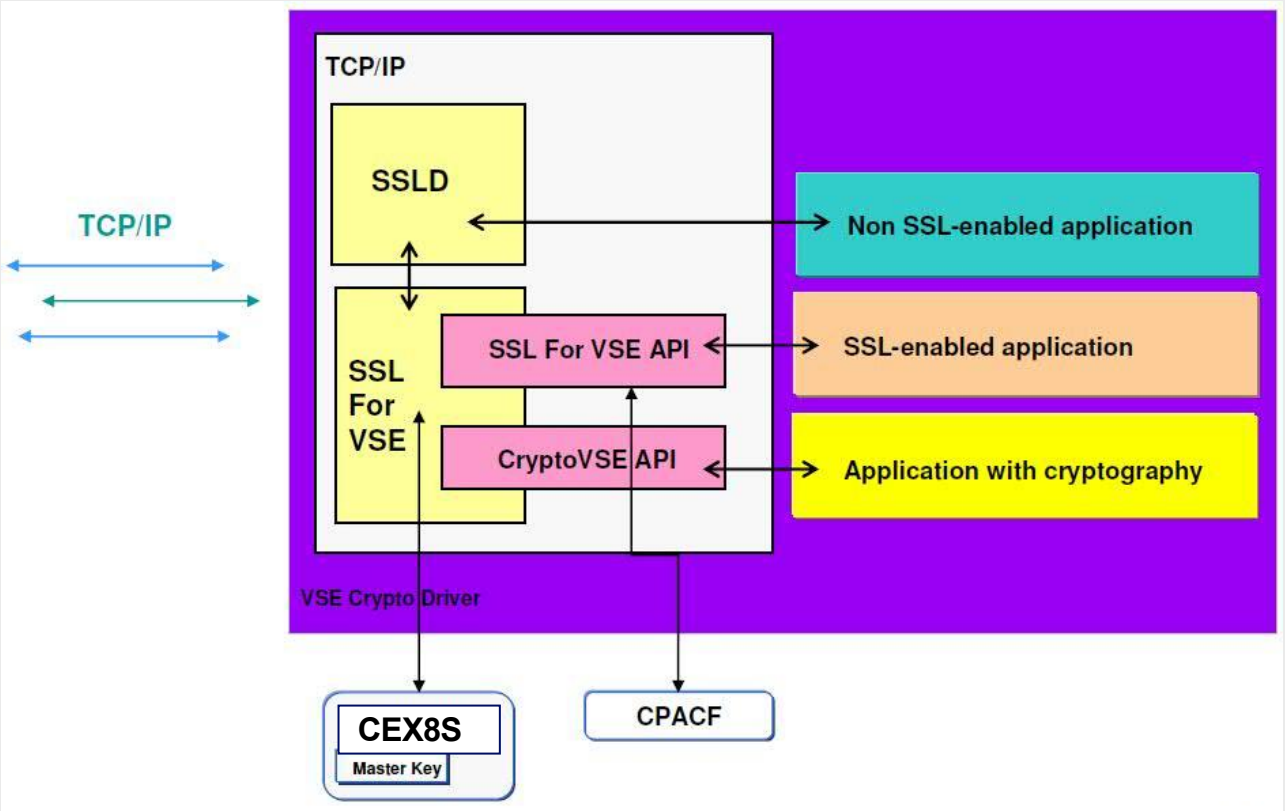
Crypto libraries will vary from OS to OS

Some may require specific configuration to make use of certain features

Consult pertinent local documentation



z/VSE Cryptographic Infrastructure



z/VSE automatically detects any Crypto Express features dedicated to (or shared with) the virtual machine in which it's running

CMS Guests Running on z/VM

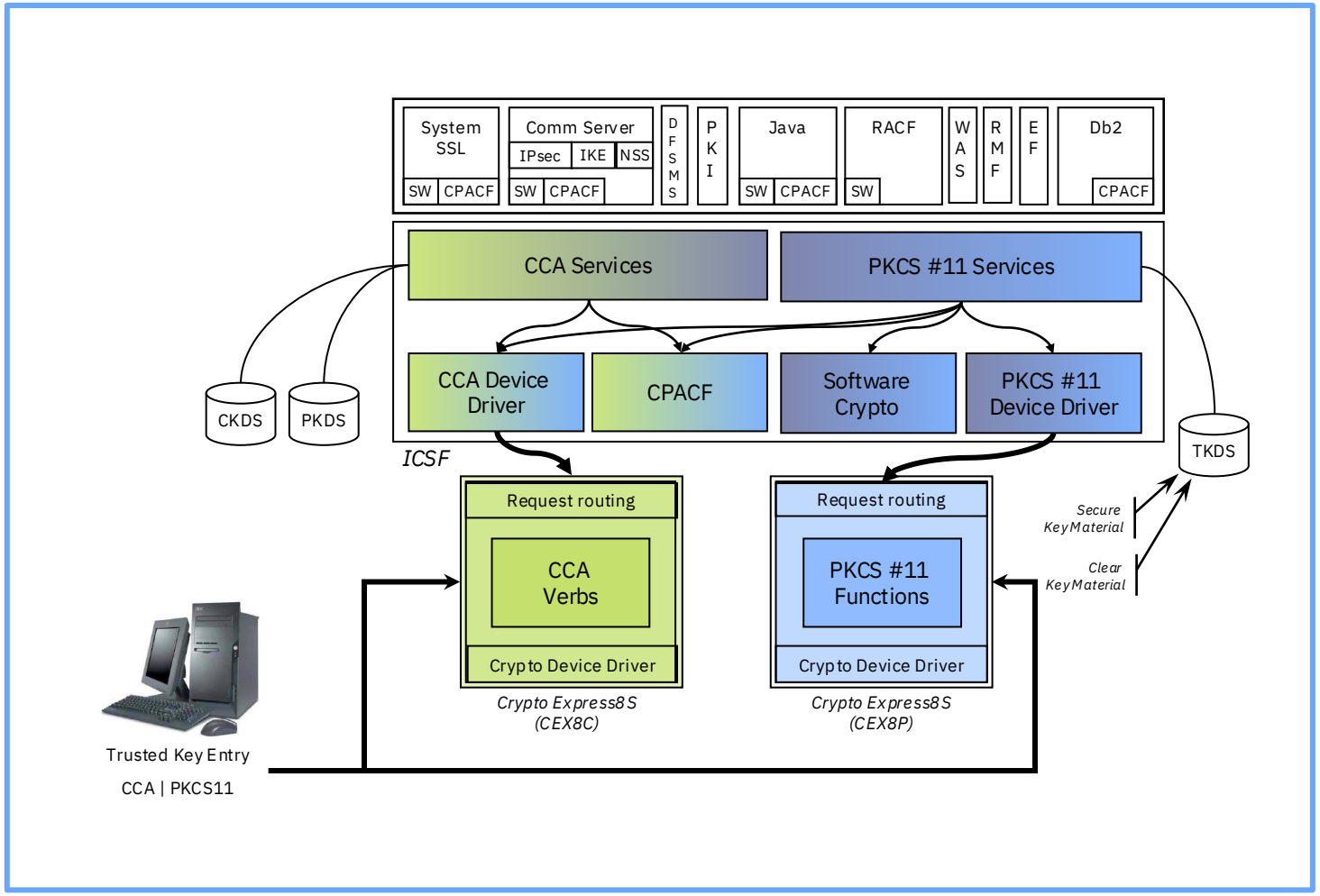
CMS guests can utilize CPACF if enabled

- Need to issue appropriate machine instructions
- Some functions (Pipelines, TLS/SSL Server) use these automatically

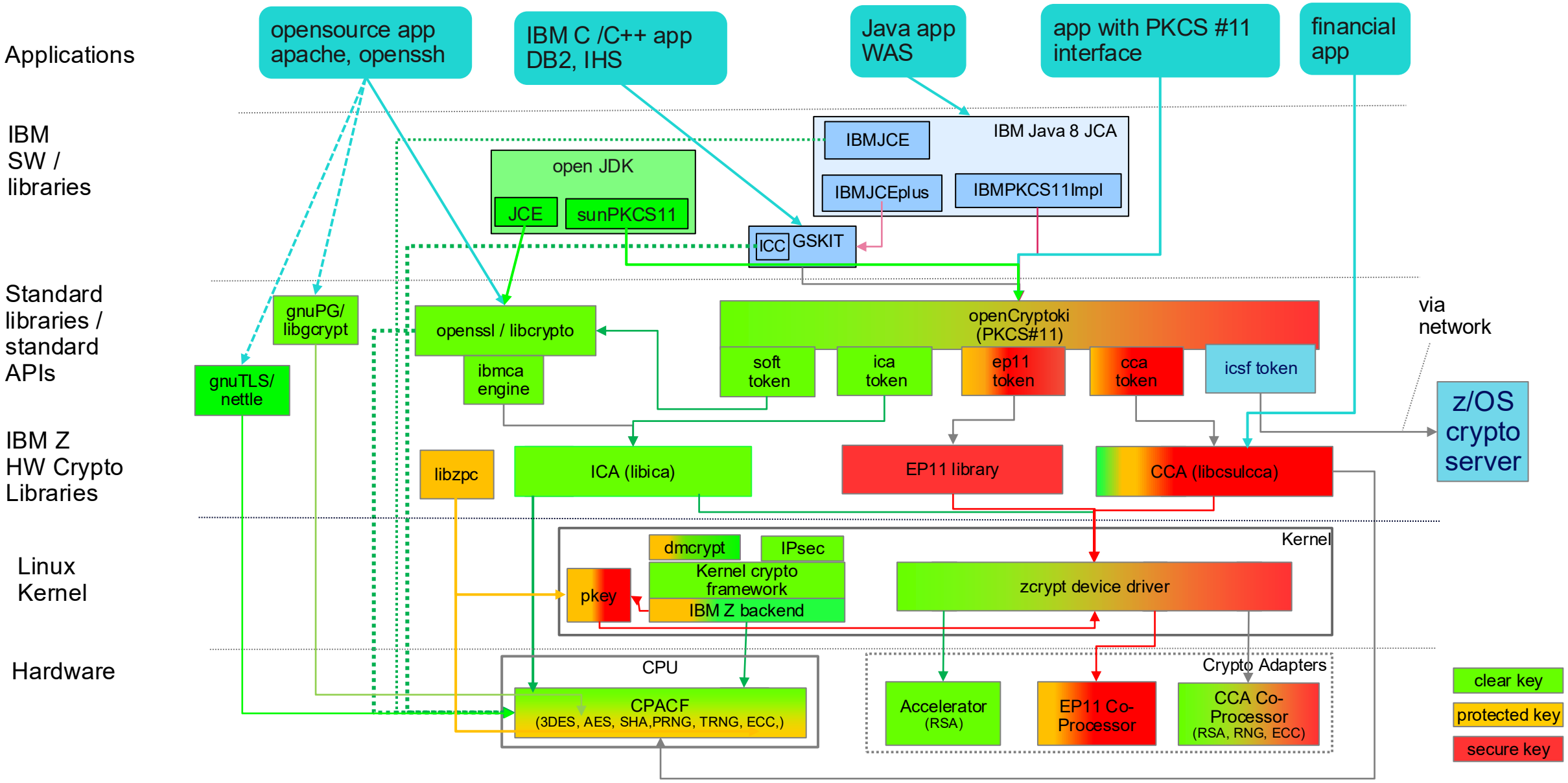
The CMS environment does **not** have Crypto Express libraries

- Different instructions / communication paths than CPACF
- Nothing available yet for general system programmer use
- **Exception**: TLS/SSL Server for data-in-flight encryption to/from/within the hypervisor (APVIRT only)

z/OS Cryptographic Infrastructure



Linux on Z and LinuxONE crypto stack usage by applications



Linux Kernel and Cryptography

The Linux kernel provides a set of cryptographic functions

- Generic, platform-independent implementations of cryptographic algorithms
- Support for platform-optimized algorithms that are automatically used if available

The Linux on IBM Z kernel includes support for

- Exploiting CPACF to optimize and accelerate symmetric cryptographic functions
- Managing Crypto Express cards with the ***zcrypt*** device driver

Which applications can benefit from accelerated in-kernel cryptographic functions?

- IPsec and ssh (from the beginning of the presentation, remember?)
- Linux device-mappers – for example, **dm-crypt** or **eCryptFS**

This is the part where Brian talks about quantum cryptography

But only if you don’t observe him.

Summary

Summary

IBM Z and LinuxONE **hardware** accelerates the hard math of cryptographic operations

- Saves **time**, saves CPU processing **power**, saves MIPS **cost**
- Secure Key operations are FIPS 140-2 Level 4 certified

z/VM **virtualizes** IBM Z hardware cryptography

- Architectural fidelity in all things IBM Z
- A "shared" flavor as well as dedicated use of crypto resources

Guests understand they can utilize IBM Z cryptography

- May require configuration of the guest to exploit
- Different guests provide different options

Don't let cryptography (or its acronyms) scare you away

- Security is meant to enhance business, not impede it
- Cryptography protects your data, whether at rest or in flight

Brian W. Hugenbruch
IBM Z and LinuxONE Security Certification Strategist &&
IBM z/VM Security and Cryptography Product Owner

IBM webpage:
https://www.vm.ibm.com/devpages/hugenbru/

Technical Blog: https://bwhugen.github.io/

Steven Horvath
IBM z/VM CP I/O and Crypto Development

Social Media:

https://www.linkedin.com/in/bwhugen/

@the_lettersea

@apictureofaman@infosec.exchange