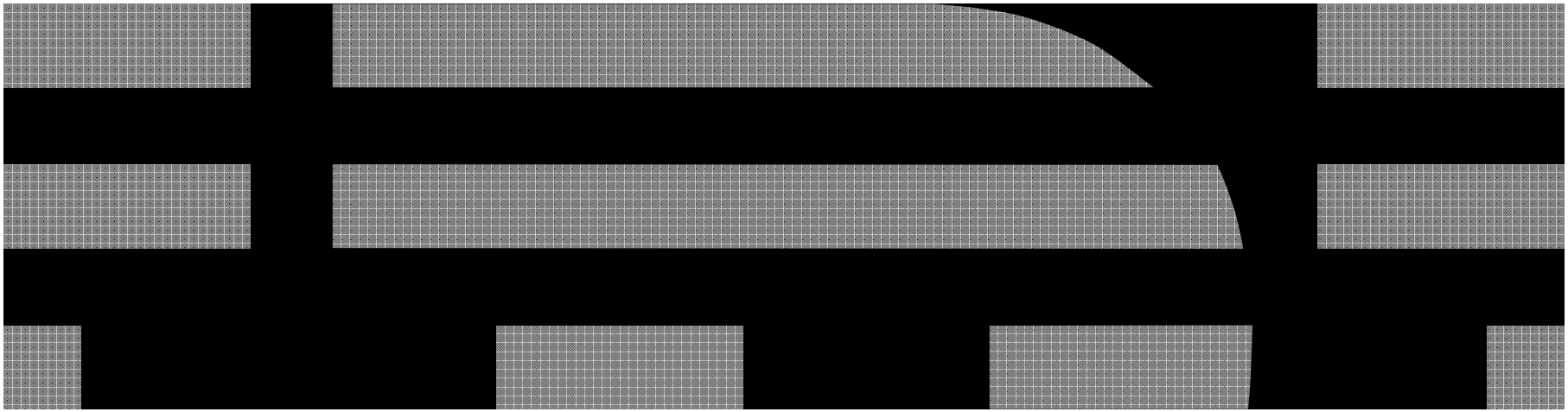
Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen@us.ibm.com

Keys to the Virtual Kingdom

Or, Virtualizing your System z hardware's cryptographic features for exploitation by your guest operating systems.



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.

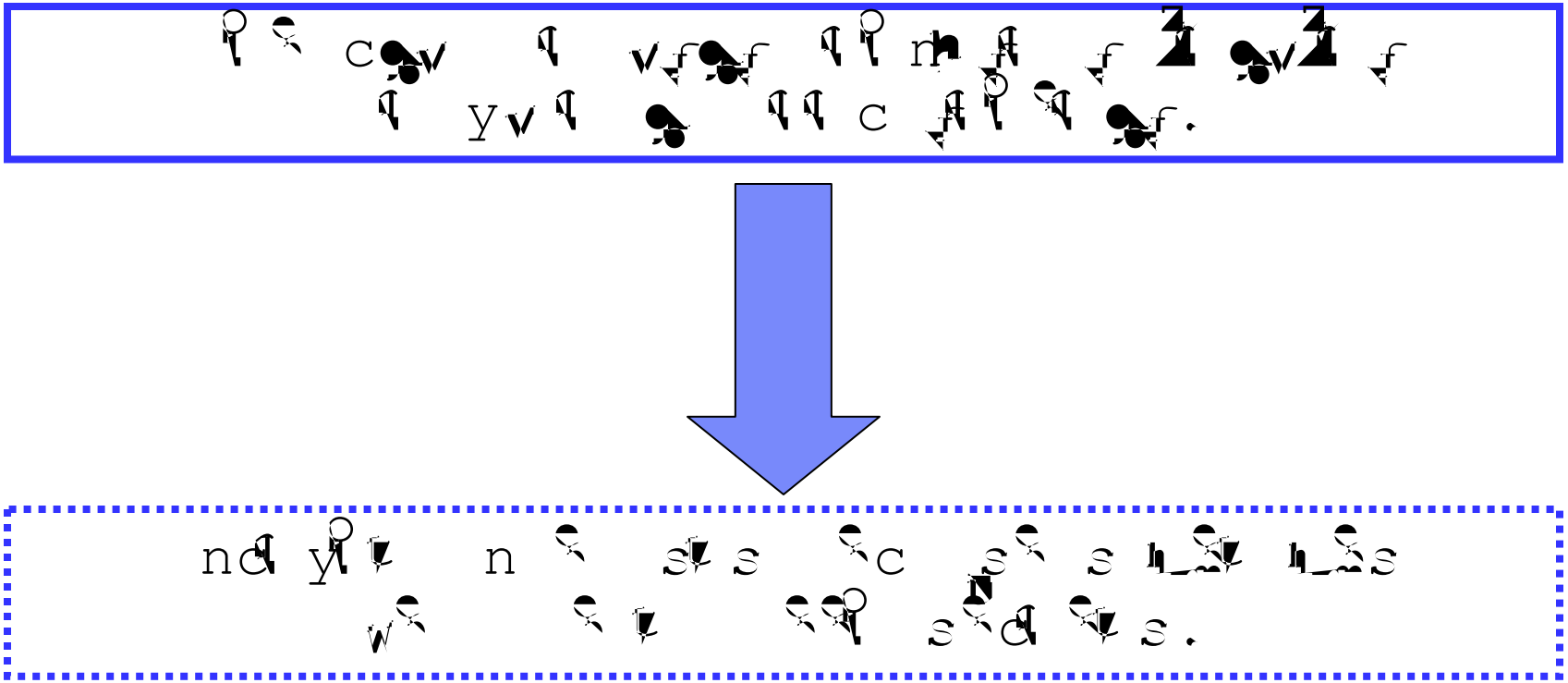
Objectives of this Presentation

- To clarify what cryptographic features are available to System z
- To explain how z/VM can virtualize these features for guest support
- To answer common questions about configuration

The New zEC12 – “Ultimate Security”

… and here's your cryptography "Bingo" card.

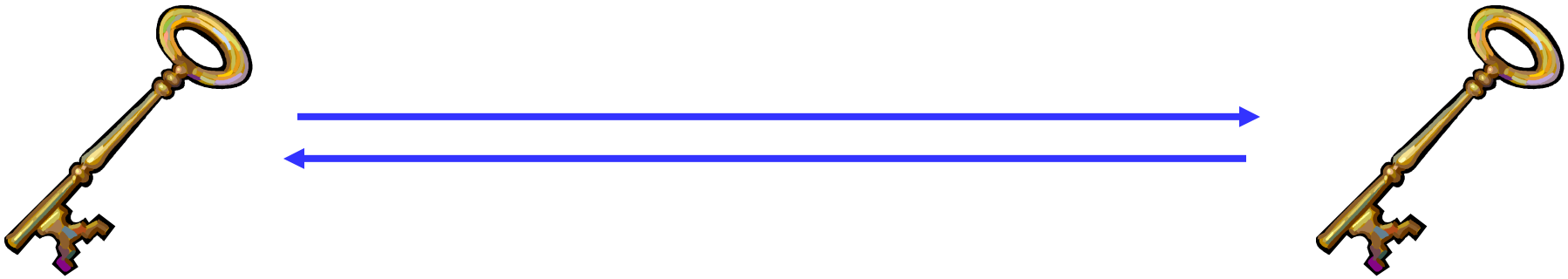
AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority
CBC	Cipher Block Chaining
CCA	IBM Common Cryptographic Architecture
CCF	Cryptographic Coprocessor Facility
CDSA	Common Data Security Architecture
CEX2/3A	Crypto Express 2/3 Accelerator Mode
CEX2/3C	Crypto Express 2/3 Coprocessor Mode
CFB	Cipher Feedback
CKDS	Cryptographic Key Data Set
CRL	Certificate Revocation List
CRT	Chinese Remainder Theorem
CVC	Card Verification Code
CVV	Value
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Standard
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GSS	Generalized Security Services
ICSF	Integrated Cryptographic Service Facility
IETF	Internet Engineering Task Force
IPKI	Internet Public Key Infrastructure
KGUP	Key Generation Utility Program
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MDC	Message Detection Code
MD5	Message Digest 5
OAEP	Optimal Asymmetric Encryption Padding
OCSF	OS/390 Open Cryptographic Services Facility
OCSP	Online Certificate Status Protocol
PCICA	PCI Cryptographic Accelerator
PCICC	PCI Cryptographic Coprocessor
PCIXCC	PCIX Cryptographic Coprocessor
PKA	Public Key Architecture
PKCS	Cryptographic Standards
PKDS	Public Key Data Set
PKI	Infrastructure
RA	Registration Authority
RACF	Resource Access Control Facility
RSA	Rivest-Shamir-Adleman
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SLE	Session Level Encryption
SSL	Secure Sockets Layer
TKE	Trusted Key Entry
TLS	Transport Layer Security
VPN	Virtual Private Network



Cryptography is a mathematical function whereupon plaintext ("information in the clear") is transmuted into a secret ("encrypted") and can only be decrypted by someone who shares a common secret.

Symmetric keys
(Examples: DES, Triple-DES, AES)

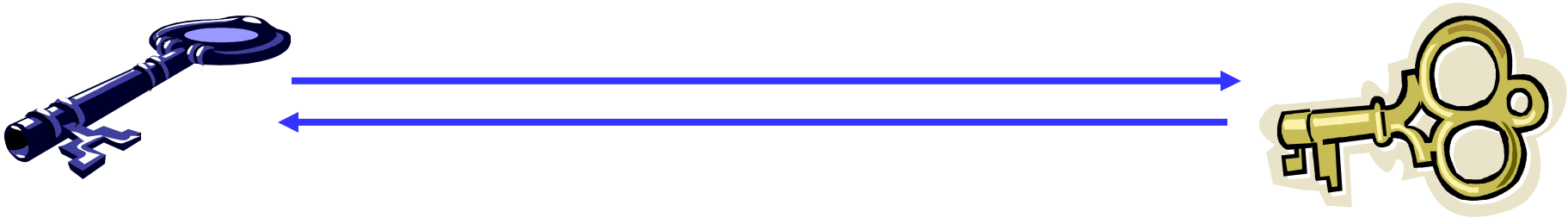
- A secret held in common by two parties
- Used to encrypt or decrypt a message in flight.
- Without the shared secret, a third party could not reasonably decrypt the message



- Faster than asymmetric, but only provides confidentiality – not authentication or nonrepudiation.
- The problem: how does the secret key go from person A to person B?

Asymmetric keys
(Examples: Diffie-Hellman, RSA, DSA, Elliptic Curve)

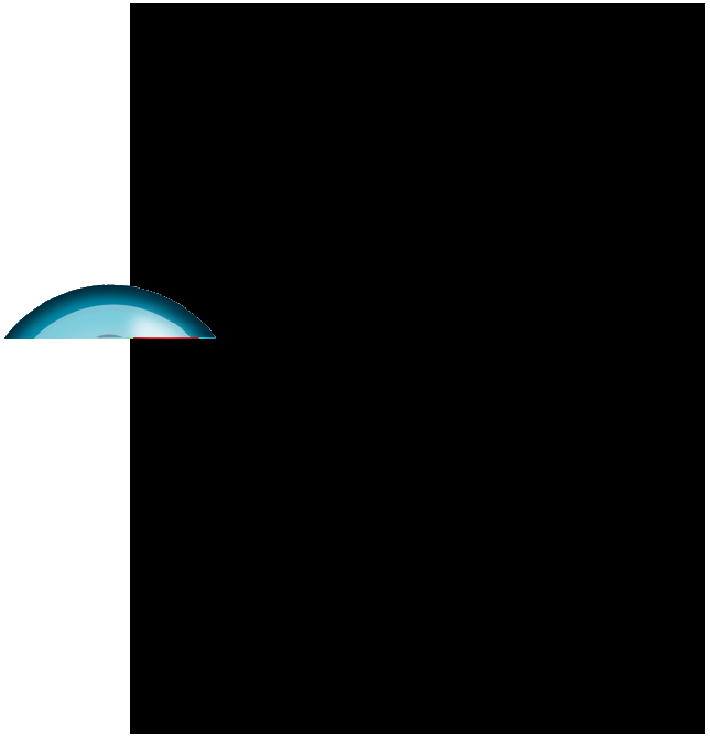
- Corresponding secrets used to encrypt information
- Data encrypted by the private key can be encrypted by anyone with the public key
  - Only Alice has Alice's private key; if we can decrypt this message, we know it is from Alice.
  - If we encrypt the response with Alice's public key, we know only Alice will be able to read it.



- Mathematically more intensive than symmetric (and therefore much slower)

How do these functions help System z?

- Hardware crypto combines the security functionality with the trust and reliability of System z hardware
- Protect your data, both at rest and in flight
- Offloaded from the CPU (saves on MIPS)
- Functionality – modern algorithms aren't always implemented in the software libraries
- Meet regulations and comply with standards



System z Cryptographic Features

- **System z provides two flavors for accelerating cryptographic operations**

- *CP Assist for Cryptographic Function* (**CPACF**) is a no-charge enablement feature on System z hardware
  - CPU support for symmetric algorithms is included in every CP and IFL
  - Pseudo-random number generator

- *Crypto Express feature* (**CEX2, CEX3, CEX4**)
  - Asymmetric algorithm offload and hardware RNG
  - *Accelerator mode* and *Coprocessor mode* for fine-tuning of security and performance

- **CPACF and Crypto Express help you to**
  - Move cryptographic workload away from central processors
  - Accelerate encryption and decryption
  - Heighten your security level by protecting and securing keys

System z Cryptographic Features

Three different types of **key protection** in the **IBM Crypto hardware:**

- **Clear keys:**
  - The security of keys is provided by operating procedures. (May appear in the clear in the environment somewhere)

- **Secure keys: (FIPS 140-2 Level 4 certified)**
  - Secure keys are protected by another key, called master key, which is stored in the hardware
  - When a secure key must leave the hardware, the key is encrypted under the master key
    - The clear value of the secure key is never exposed to the operating system

- **Protected keys**
  - Protected keys are encrypted under a wrapping key uniquely created for each LPAR
  - Cryptographic operations using protected keys can benefit from CPACF performance

Getting Keys into the CryptoExpress Features

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

- **z/OS Integrated Cryptographic Services Facility (ICSF)** – a base component which allows interaction with CryptoExpress features. (Requires MVS.)

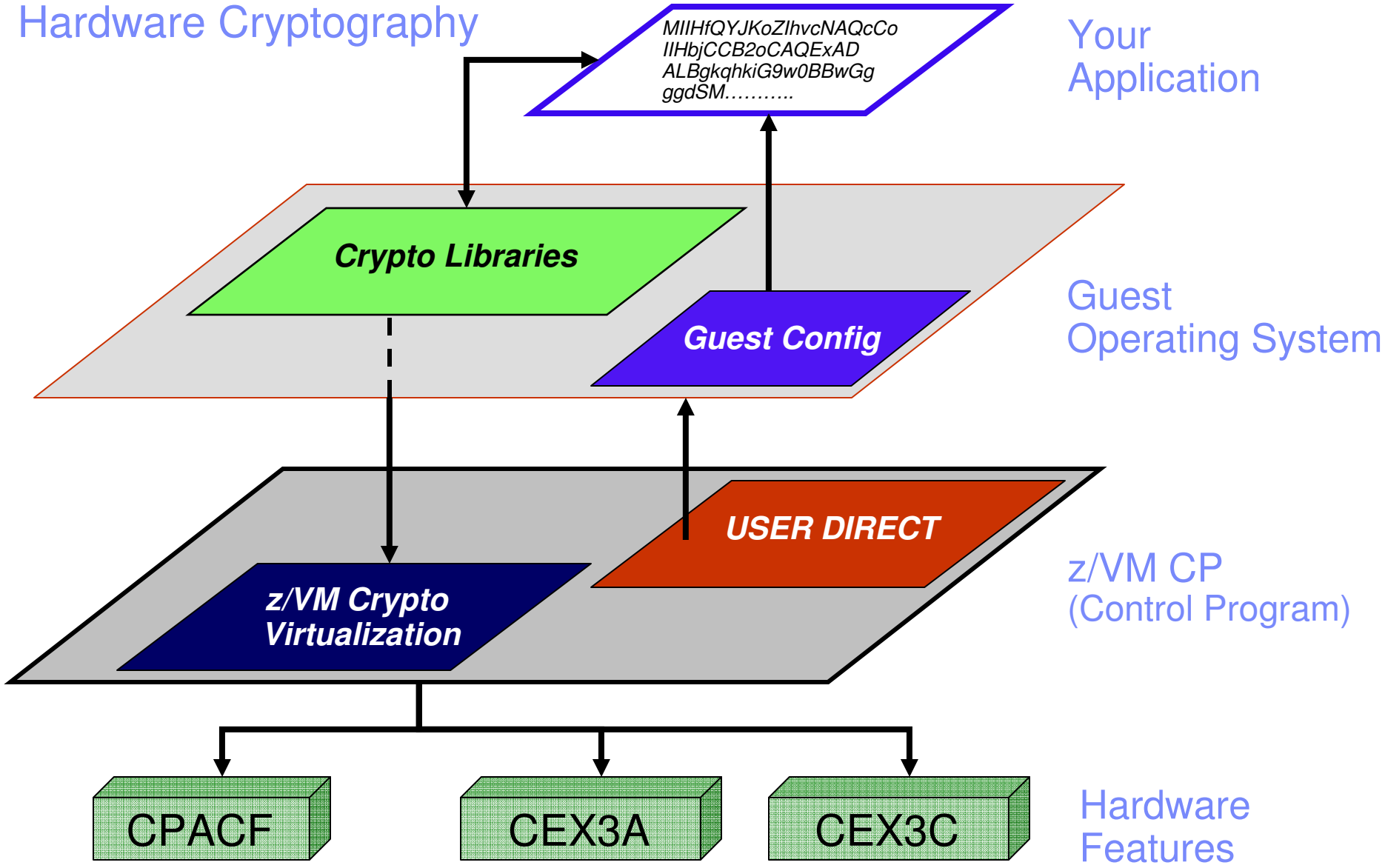
- **Panel.exe Utility for Linux** – a Linux package installed as part of the IBM .rpms which allows for key management function.
  - / [illegible] BM X? / [illegible] n [illegible]

- **IBM Enterprise Key Management Foundation (EKMF)** – an IBM Lab Services offering for flexible and secure key management services.

But that's just the hardware, and you're probably not running a single guest on an entire zEC12 …

Let's take a look at how this ties into the rest of the System z virtual ecosystem.

z/VM Virtualization of Hardware Cryptography



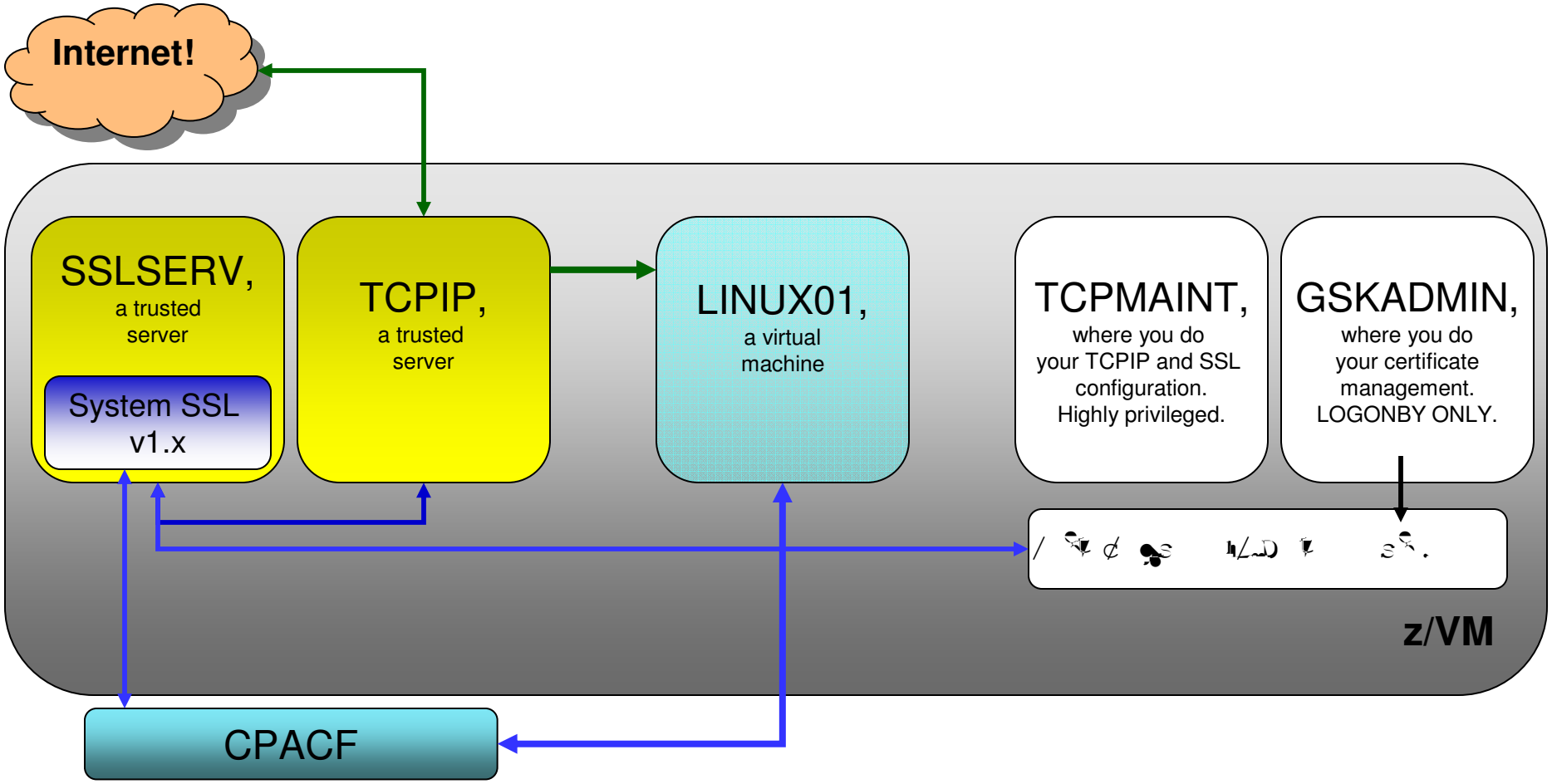
#WAVV #zVM #IBMSecurity

System z Cryptographic Features

CPACF Support

- Available on all modern z hardware (z9 onward), but it must be explicitly enabled
- If this feature of the hardware is enabled, z/VM virtual machines (including the SSL Server) can make use of it

Guests under z/VM can use CPACF if enabled …



#WAVV #zVM #IBMSecurity

Frequently Asked Questions

- **CPACF, you say? Cool beans.**
  But does z/VM SSL use the Crypto Express Cards?

- **Answer**: No. While SSLSERV and LDAPSRV use **CPACF** if enabled, z/VM only virtualizes Crypto Express support for hosted operating systems. z/VM's CMS-based servers will not utilize them.

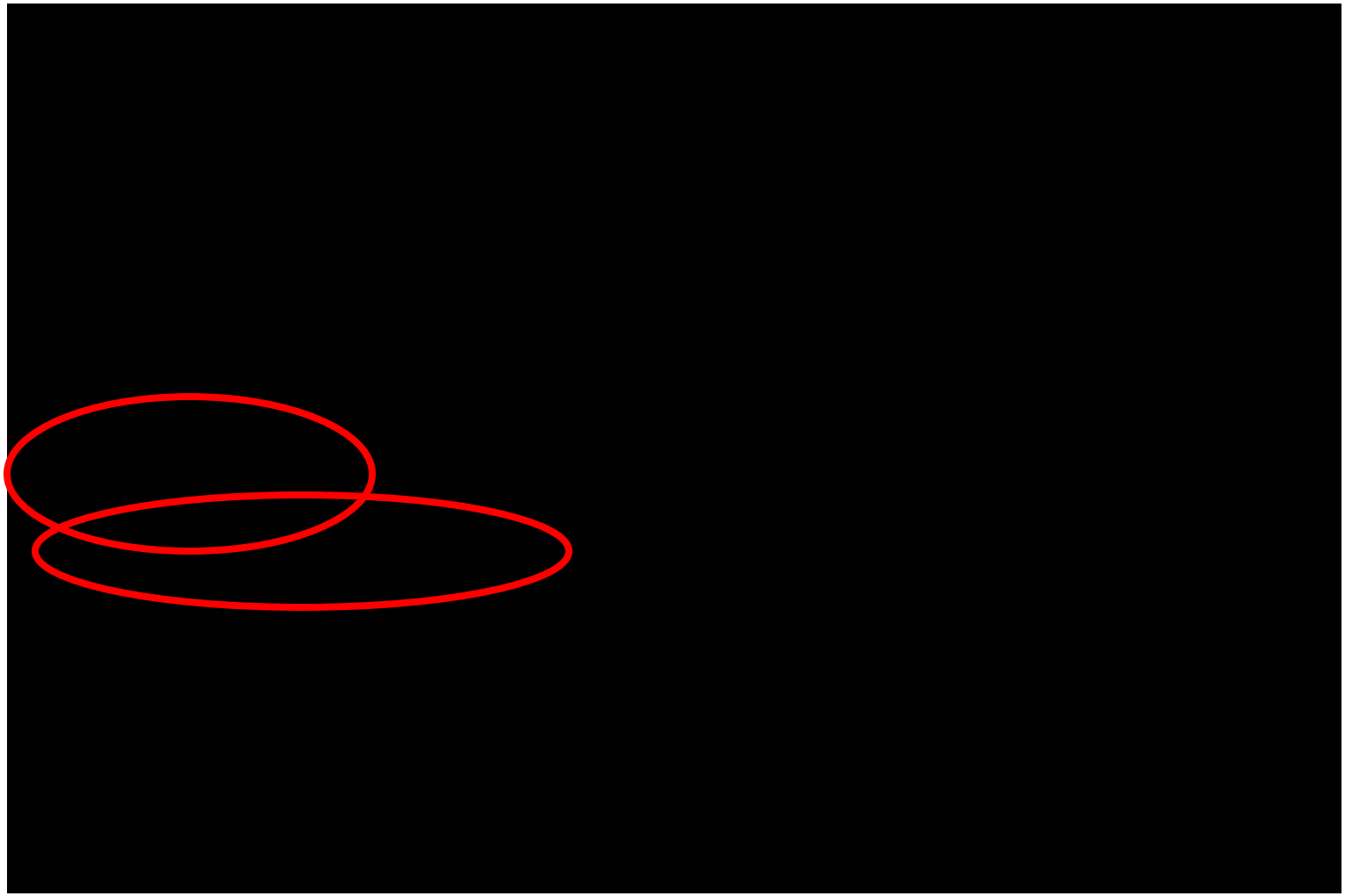
- Check out the following session for more details:

Managing Digital Certificates for z/VM
Brian W. Hugenbruch, CISSP: IBM Endicott
Tuesday, 9:45am, in U3

System z Cryptographic Features

Crypto Express Support

- Mode is set (Accelerator or Coprocessor) on the Support Element.
  - **Accelerator mode**: meant for offload and acceleration of CPU intensive public/private key operations. Pertinent to workloads such as SSL, where secure handshaking factors heavily.
  - **Coprocessor mode**: Accelerates public/private key operations, and supports secure key operations for encryption and decryption.
    - Coprocessor mode is the more cryptographically interesting of the two
    - Host master keys would be stored in Coprocessor domains

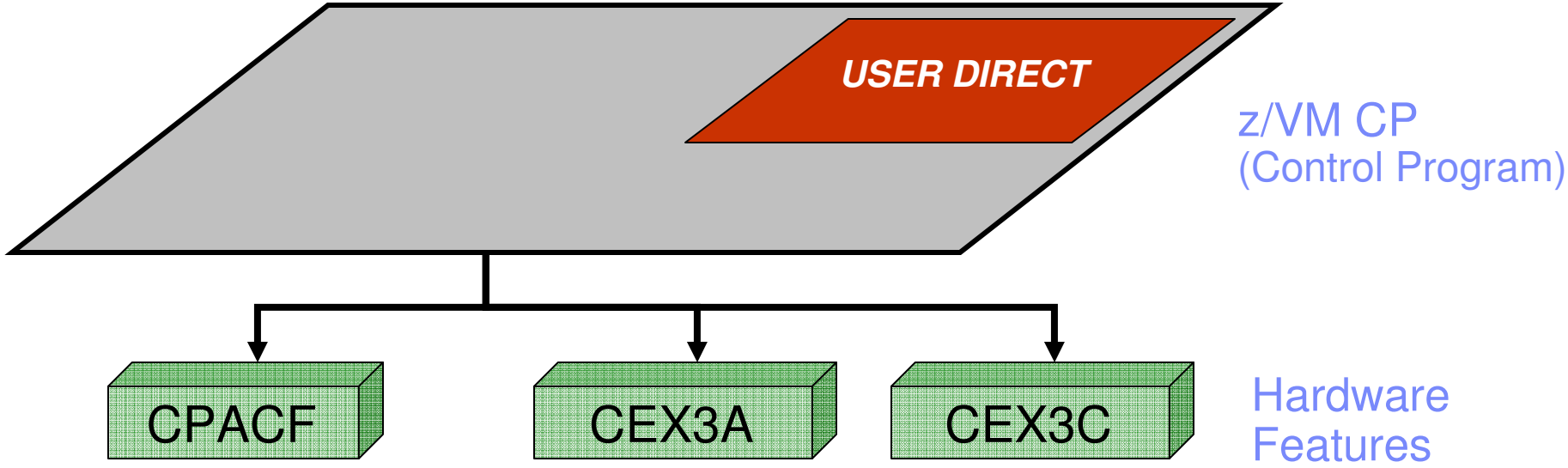


System z Cryptographic Features

Crypto Express Support

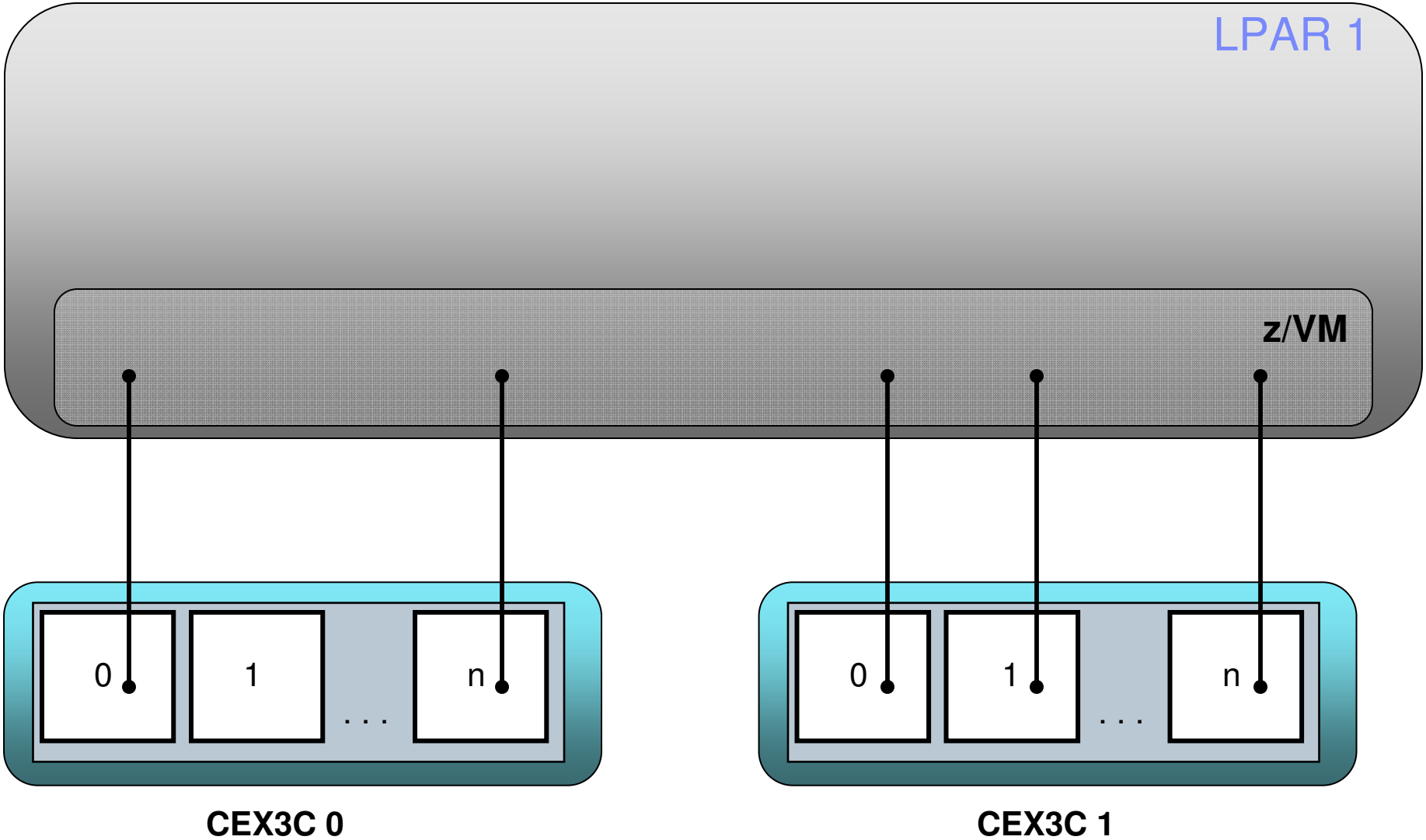
- LPAR assignation is done from the HMC
- z/VM will only detect those cards and domains assigned to the LPAR
- **Candidate list**: domains on this AP which are eligible to be accessed by this partition
- **Online List**: processors automatically brought online at LPAR startup.
- **Usage Domain**: bundles domains together inside a common cryptographic boundary
- **Control Domain**: identifies domain index pertinent to TKE control of the LPAR. Must also contain Usage Domain.

z/VM Virtualization of Hardware Cryptography (stack view)



#WAVV #zVM #IBMSecurity

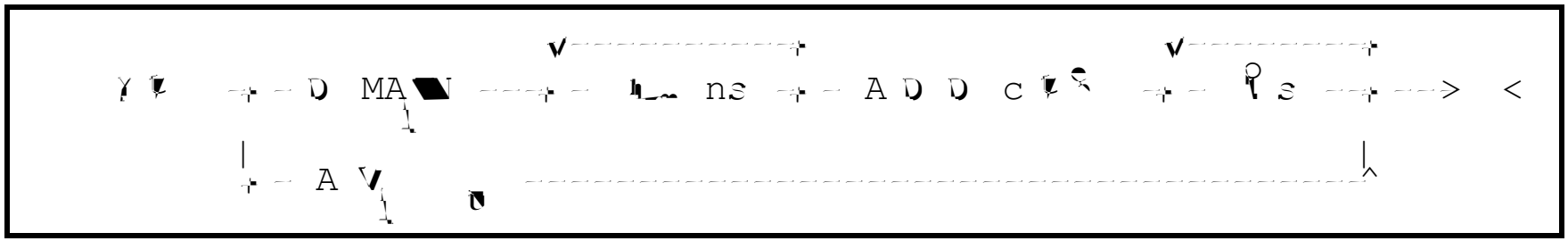
z/VM Virtualization of Hardware Cryptography (z/VM's view)



#WAVV #zVM #IBMSecurity

z/VM Virtualization of Hardware Cryptography

The CRYPTO User Directory statement grants a z/VM userid access to cryptographic features associated with the hardware:



ADD

Dedicates a particular AP domain (or set of domains) to this virtual machine. Domains granted in the directory are “reserved for dedication”; they are not actually in-use until the virtual machine logs on.

AVAIL

Virtual machine can access a collection of domains controlled by the system.

Frequently Asked Questions

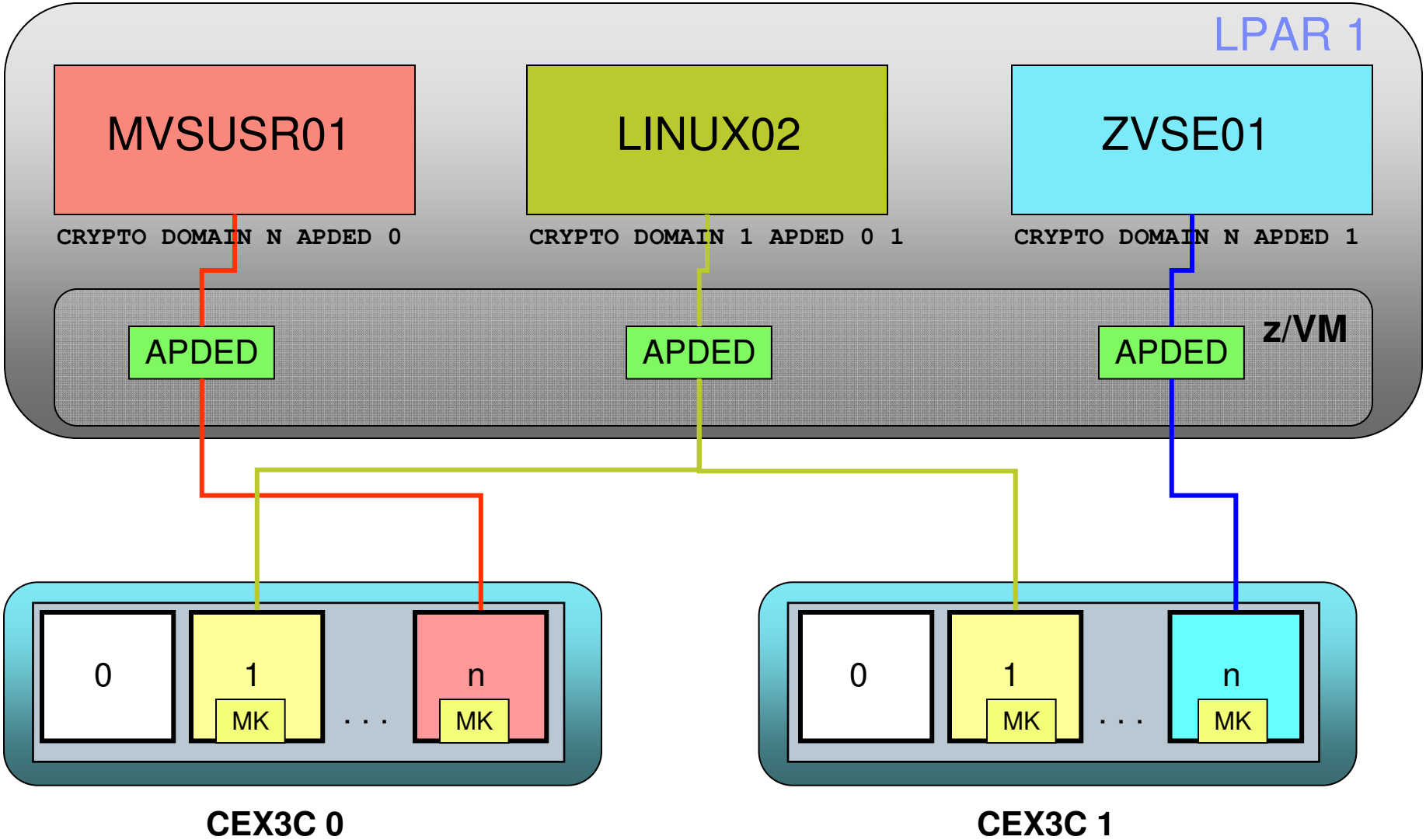
- **Terminology question – is it a *domain?* or a *queue*? or an *AP?***

- **Answer**: In this context, “domain” and “queue” are mostly synonymous.

  z/VM’s QUERY CRYPTO command (as of z/VM 6.2) documents the sub-structures associated with the Crypto Express features as “domains.” APQS (short for ‘Adjunct Processor Queues’) is still accepted as an operand, and the terminology of ‘queues’ may still appear in documentation related to other IBM products.

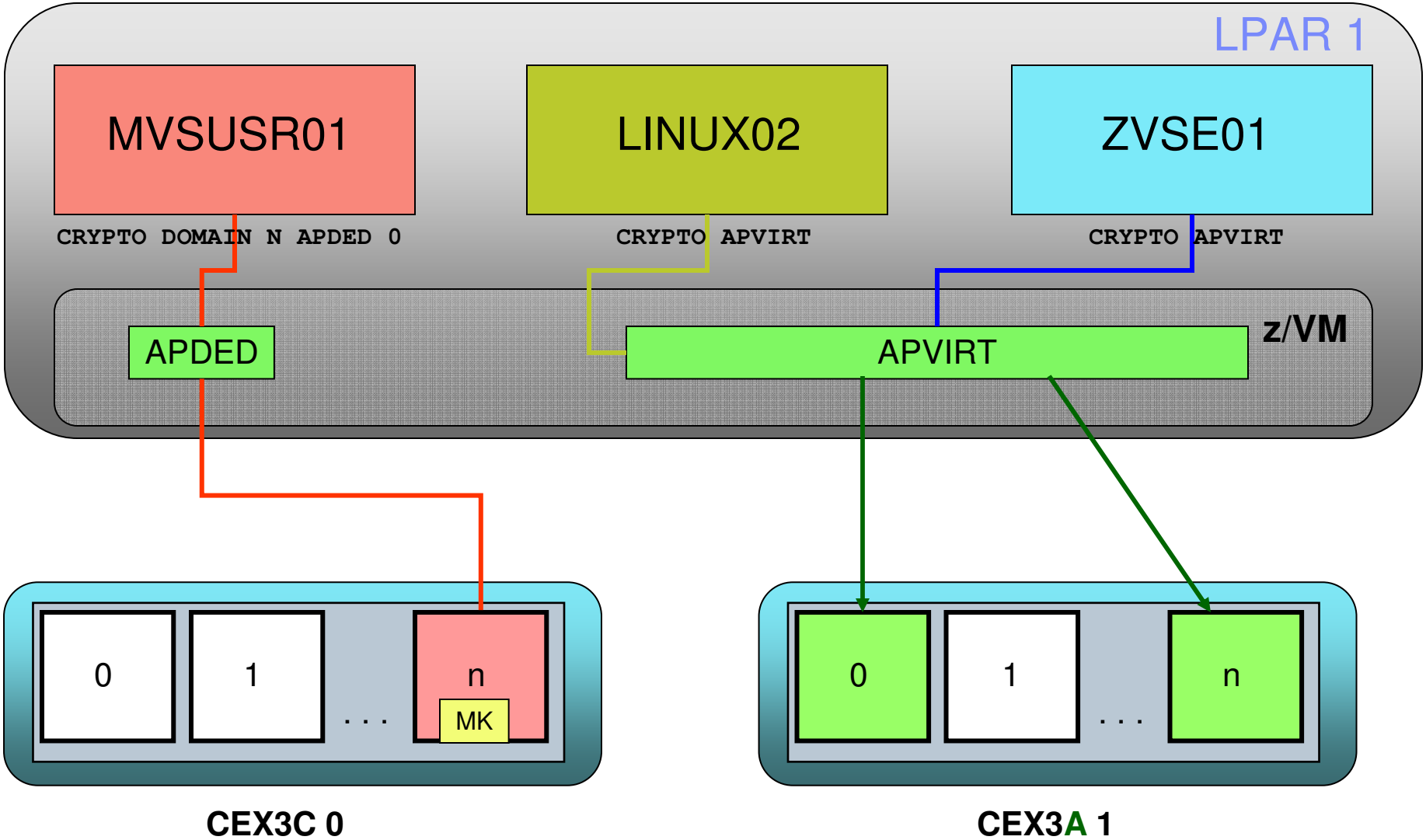
  The ‘AP’ in abbreviations like ‘APDED’ and ‘APVIRT’ refers to ‘Adjunct Processor’ … which is another term of the CryptoExpress features (CEX2 and onward).

Assigning AP Domains to z/VM Guests



#WAVV #zVM #IBMSecurity

Assigning AP Domains to z/VM Guests



#WAVV #zVM #IBMSecurity

Frequently Asked Questions

- **What happens if two z/VM guests have the same**

Frequently Asked Questions

- **Bonus Question! Explain the following statement:**

```
CRYPTO DOMAIN 0 1 APDED 14 15
```

- **Answer**: The guest receives dedicated access to the following domains:

```
[0,14]      [0, 15]      [1, 14]      [1, 15]
```

  – Domain assignation is a **union** of the AP queues and specific domains listed; be careful about assigning too many domains when configuring your z/VM virtual machines.

Frequently Asked Questions

- **Question 1: Who picks what domains are used for APVIRT?**
- **Question 2: I just overhauled my USER DIRECT, and suddenly my guests can't use their crypto domains. What happened??**

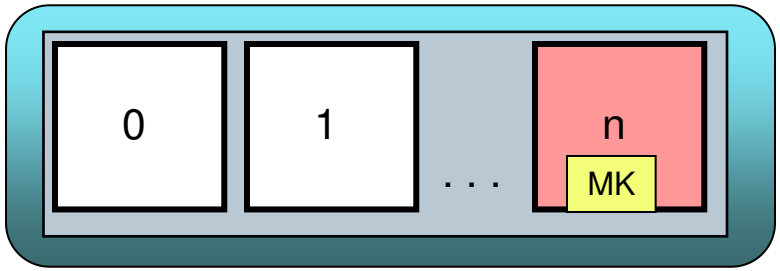
- **Answer**: APVIRT domains are assigned at system IPL, and are managed by CP. If you've stomped on domains in-use by either APVIRT or by another virtual machine, you're going to see a loss of cryptographic service. APVIRT domains are not updated while CP is running; you may need to reIPL.

  Fortunately, there are queries to tell you what domains are available to (a) your system and (b) your guests …

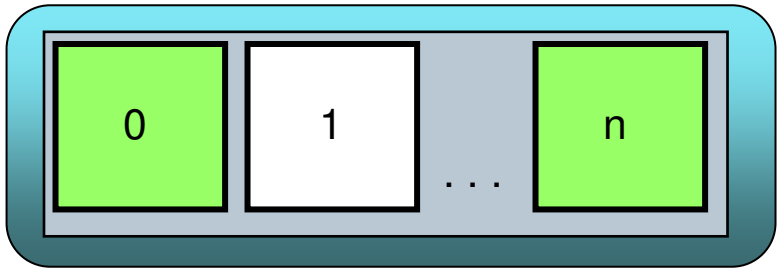
z/VM Virtualization of Hardware Cryptography

- [illegible] (Class A, B, C, or E) will display which domains/APs are available. Note that this list will be limited to devices available to a z/VM instance.

```
>> [illegible] y [illegible] +-----------------------------------------+ [illegible] >  <
                              '-D M  ns [illegible] +-----------+ -'
                                        '- [illegible] s -'
```



CEX3C 0



CEX3A 1

z/VM Virtualization of Hardware Cryptography

QUERY CRYPTO DOMAINS USERS

AP	device	Domain nn	device status	system usage	planned usage
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

[illegible]

[illegible]

#WAVV #zVM #IBMSecurity

z/VM Virtualization of Hardware Cryptography

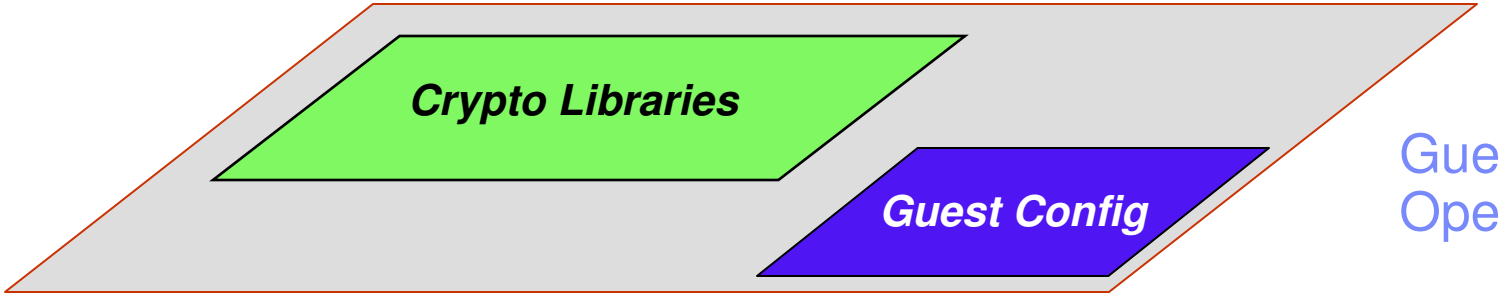
- [illegible] (Class G) will display virtual crypto facilities for your guest.
  Keyword “virtual” required for Guests with A, B, C, or E privileges.

```
>> [illegible] y--+--------------------+--- [illegible] ----><
```

```
QUERY VIRTUAL CRYPTO
```

```
A 0[illegible] X[illegible]A [illegible] n 06 [illegible] c [illegible]
[illegible] y[illegible]
```

z/VM Virtualization of Hardware Cryptography



Guest Operating System

- Cryptographic libraries will vary from operating system to operating system
- Some may require specific configuration to make use of certain features
- Consult pertinent local documentation

z/VSE Cryptographic Infrastructure

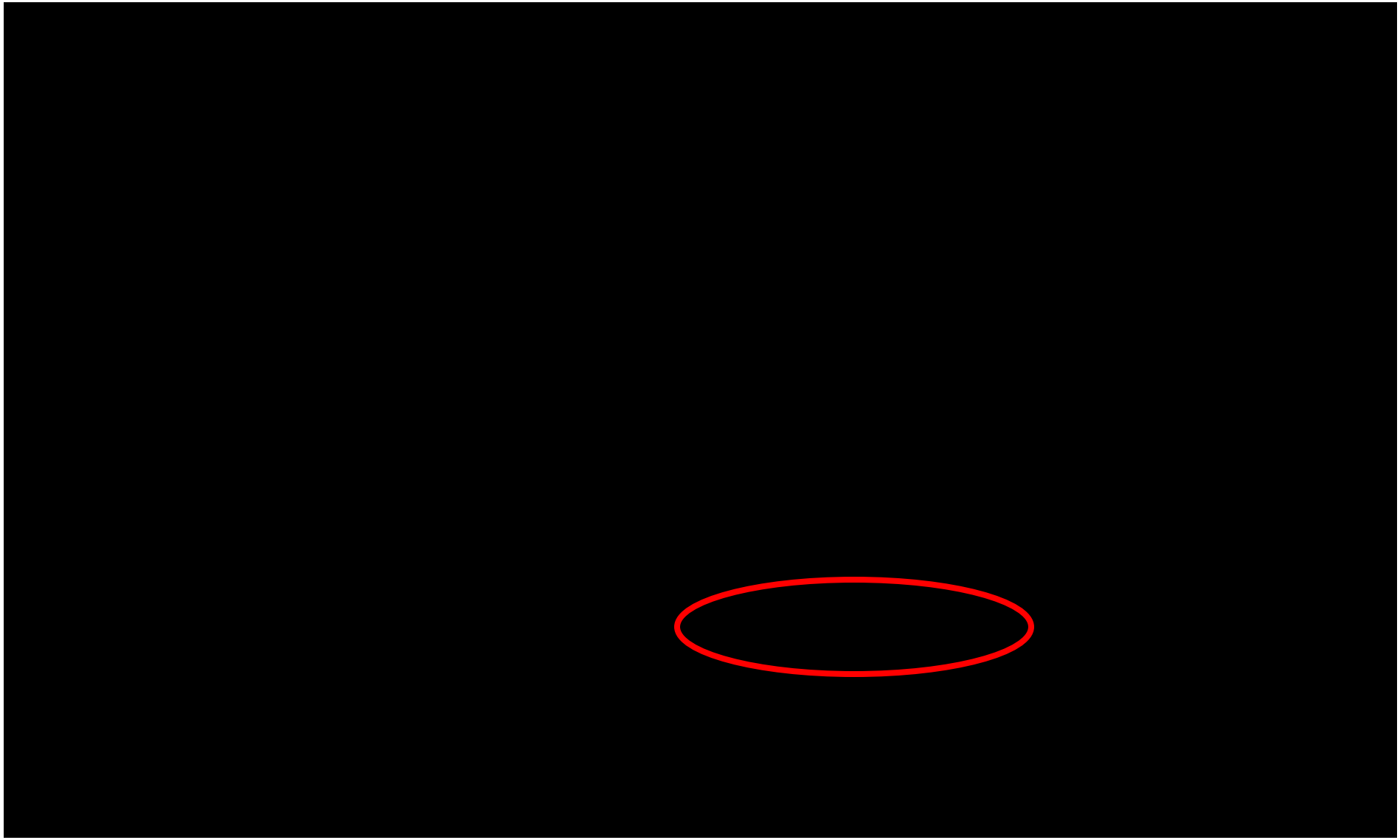
[redacted]

- Check out the following session for more details:

<u>Session</u>: z/VSE Security Overview and Update
Ingo Franzki, IBM Boeblingen
Wednesday, 8:30am, in Ballroom E

z/OS Cryptographic Infrastructure

Linux on z Cryptographic Infrastructure



```
L [illegible] n: [illegible] M[illegible] 28 10:18:05 2012 [illegible] [illegible]nn.nn.nn.nnn
c[illegible] : # cat /proc/crypto
n[illegible] : [illegible]
[illegible] : [illegible]
[illegible] : [illegible]
[illegible]y : 200
[illegible]cn[illegible] : 1
[illegible] : [illegible]
[illegible] : [illegible]
[illegible] : 0

n[illegible] : [illegible]
[illegible] : [illegible]-[illegible]n[illegible] c
[illegible] : [illegible]
[illegible]y : 0
[illegible]cn[illegible] : 1
[illegible] : [illegible]
[illegible] : [illegible]
c [illegible] : 6
[illegible] : 20

n[illegible] : [illegible]5
[illegible] : [illegible]5-[illegible]n[illegible] c
[illegible] : [illegible]
[illegible]y : 0
[illegible]cn[illegible] : 1
[illegible] : [illegible]
[illegible] : [illegible]
c [illegible] : 6
[illegible] : 16
```

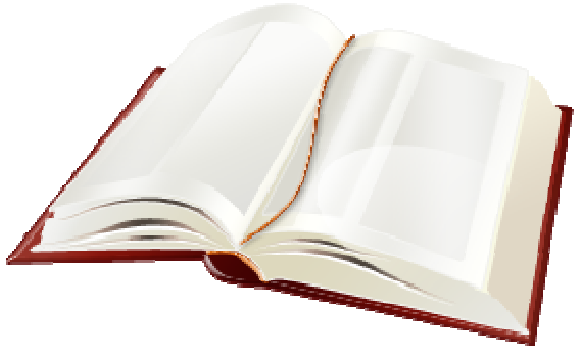
```
c[illegible]  :  # icainfo

[illegible] w n[illegible]  Ass[illegible] [illegible] y[illegible] [illegible] c
  nc[illegible] n (  A  ) [illegible] [illegible] ns [illegible] s [illegible] [illegible] y
    c  n [illegible] s sys[illegible]

  A-1 :     y s
  A-256 :   y s
  A-512:    y s
D  :        y s
 D  -128:   y s
 D  -192:   y s
A  -128:    y s
A  -192:    y s
A  -256 :   y s
  [illegible]C:     y s
```

For More Information …

- **developerWorks** http://www.ibm.com/developerworks/linux/linux390/
- **IBM TechDocs:** http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/Search
- **Information on the IBM System z CryptoExpress Features:** http://www-03.ibm.com/security/cryptocards/pciecc/overview.shtml
- *Secure Key Solution with the Common Cryptographic Architecture Application Programmer's Guide [PDF]*
- **Article** in Enterprise Systems Media: *"Using Crypto Hardware with Java in Linux on System z"*



For More Information …

- **System z Security:** http://www.ibm.com/systems/z/advantages/security/
- **z/VM Security resources:** http://www.vm.ibm.com/security
- ***Security for Linux on System z*** (SG24-7728), IBM RedBooks
- ***z/VM Security*** (SG24-7471), IBM RedBooks
- ***z/VM Secure Configuration Guide*:** http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf

Contact Information:

Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen at us dot ibm dot com
+1 607.429.3660
Twitter: @Bwhugen

Dank u
Dutch

Merci
French

Спасибо
Russian

Gracias
Spanish

شكراً
Arabic

감사합니다
Korean

Tack så mycket
Swedish

धन्यवाद
Hindi

תודה רבה
Hebrew

Obrigado
Brazilian Portuguese

谢谢
Chinese

Dankon
Esperanto

Thank You

ありがとうございます
Japanese

Trugarez
Breton

Tak
Danish

Danke
German

Grazie
Italian

நன்றி
Tamil

děkuji
Czech

ขอบคุณ
Thai

go raibh maith agat
Gaelic

#WAVV #zVM #IBMSecurity