Saying Hello to z/VM V7.5 Security

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

Agenda

- **Certifications**
- **Recent News (Feature Packs and details)**
- **z/VM 7.5**
  - RACF/VM Simplification
  - Host Secure Boot
- **Coming Next**
  - TLS 1.3 Support
  - Linux-Native Interface for RACF/VM

z/VM releases not listed are "designed to conform to the standards of each security evaluation."

z/VM Security Certifications

z/VM Level	Common Criteria	
z/VM 7.5	*Not evaluated ("designed to conform to standards")*	
z/VM 7.4	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ – Completed!***	***NIAP VPP with Server Virt. Extended Package – Completed***
z/VM 7.3	*Not evaluated ("designed to conform to standards")*	
z/VM 7.2	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ – Completed!***	***NIAP VPP with Server Virt. Extended Package – Completed!***

z/VM Level	FIPS 140-n
z/VM 7.5	*To be evaluated to FIPS 140-3*
z/VM 7.4	***CAVP algorithm certificates pending**; not CMVP validated ("designed to conform…")*
z/VM 7.3	*Not evaluated ("designed to conform to FIPS 140-2 standards")*
z/VM 7.2	***FIPS 140-2 L1 for z/VM System SSL and ICSFLIB – Completed!***

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Recently…

- Enhancements to RPIDIRCT for more intelligent RACF configuration
  - RACF Feature 03 Fix 00
  - APAR VM66892

RACF: The Right Way
Thursday, 4:45pm, 1201

- Control-only domain support for virtualization of Crypto Express features
  - CP Feature 04 Fix 00
  - APAR VM66891

Keys to the Kingdom
Friday, 11:00am, 1201

- GetShopZ for Installation Media

ZIP Through Install
Thursday, 3:30pm, 1107

- RENEW option for CERTMGR

CERTMGR

z/VM 7.4
TCPIP Feature Pack 03 Fix 00
PTF for APAR PH68728

- Rexx wrapper for gskkyman (the z/OS key database application)
  - Designed for ease-of-use and automation
  - Displays certificate chains, expiry dates, etc

- Uplifted **z/VM's System SSL 3.1 and added:**

gskkyman –r <options>
Receive a certificate

gskkyman –rn <options>
Renew a certificate

- **CERTMGR**
- QUERY
- **RECEIVE *new***
- **RENEW *new***
- IMPORT
- EXPORT

Introducing Security on z/VM V7.5

Removal of the z/VM LDAP Server

- A Statement of Direction was issued with z/VM V7.4 General Availability:

  z/VM V7.4 is planned to be the last z/VM release to support the z/VM LDAP server. This server, a rehost of the z/OS Directory Server, will be removed from z/VM TCP/IP as part of a future release. This includes the LDAPSRV virtual machine and associated components. All future releases will continue to support ldap-bind as an authentication factor through the IBM Z Multi-factor Authentication product.

  CMS-based LDAP client utilities, and the RACF r_admin interface, are not impacted by this statement.

- *We're going to loop back on this later, don't worry*

RACF/VM Simplification

- Removal of RACF-specific CP parts
  - Introduce CP Exits for loading a security manager
  - Goal is to remove the need to recompile CPLOAD (see also: Secure Host Boot)
  - Ease of use for RACF clients

- Change in RACF-specific management
  - Move SYSSEC configuration to System Configuration file
  - CP commands (not RACF commands) to update configuration
  - CMS utility to extract old SYSSEC configuration

RACF/VM Simplification – What's Changing?

- HCPRW* CP parts, to allow for one of two choices:
  No ESM or CPXLOADed ESM (RACF or a Broadcom ESM)

- CPSYNTAX, System Configuration

- SALIPL (new keyword "NOESM")
  - CP QUERY IPLPARLMS will reflect whether NOESM was chosen

- CP commands for managing RACF

RACF/VM Simplification – HCPRWAC

- What's going away?
  - HCPRWAC -- the sample Common Criteria config for SYSSEC
  - Current plan is to ship with a default of DEFER, as done currently
    - Migration to new RACF supersedes security by default
    - Guidance already exists for meeting the **Common Criteria version of the configuration**, which looks like so:

```
SYSSEC ,
        DISKP=ALLOW,DISKU=FAIL,DISKF=FAIL,DISKW=FAIL,DISKM=ON,
        RDRP=ALLOW,RDRU=FAIL,RDRF=FAIL,RDRW=FAIL,RDRM=ON,
        NODEP=ALLOW,NODEU=FAIL,NODEF=FAIL,NODEW=FAIL,NODEM=ON,
        CMDP=ALLOW,CMDU=FAIL,CMDF=FAIL,CMDW=FAIL,CMDM=ON,
        LANP=ALLOW,LANU=FAIL,LANF=FAIL,LANW=FAIL,LANM=ON,
        DEFLTP=ALLOW,DEFLTU=FAIL,DEFLTF=FAIL,DEFLTW=FAIL
```

RACF/VM Simplification – CP SET ESM

- CP SET ESM **(Class C)**

  - CP SET ESM ACTIVE|INACTIVE
    - Does not supersede requirement to enable the RACF component / obtain a license
    - RACF state cannot be changed in an SSI cluster with more than 1 active member
    - SET ESM INACTIVE only allowed after all RACF servers have been stopped

  - CP SET ESM ACTIVE RACF
    - Associates and enables all ESM CP exits to call RACF modules

  - CP SET ESM INACTIVE
    - Disables ESM checks – does not change CP Exit configuration
    - CP SET ESM INACTIVE CLEAR will disassociate all ESM CP Exits.
    - RAC SETRACF is replaced by CP SET ESM INACTIVE

RACF/VM Simplification – QUERY ESM

- CP QUERY ESM STATUS|DETAILS **(Class C or Class E)**
  - Display current ESM state (active, inactive)
  - DETAILS provides CP Exit information

```
ESM status is ACTIVE
Exit EPName Status
6000 HCPRAHIN Enabled
6001 HCPRAPHR Enabled
6002 HCPRADEP Enabled
6003 HCPRAHEQ Enabled
6011 HCPRAIRA Enabled
6012 HCPRAICN Enabled
6013 HCPRAIIL Enabled
6014 HCPRAISV Enabled
6015 HCPRAIQS Enabled
6016 HCPRAIRM Enabled
6020 HCPRAWEP Enabled
6021 HCPRAWPR Enabled
6030 HCPRAHIS Enabled
ESM Name: RACF
ESM Product Version String: 750
ESM is active
ESM Vendor Name: IBM
ESM Product Information: RACF Security Server for z/VM FL750, 5741-A09
```

RACF/VM Simplification – SET RACF

- CP SET RACF **(Class C) – for RACF-specific configuration**

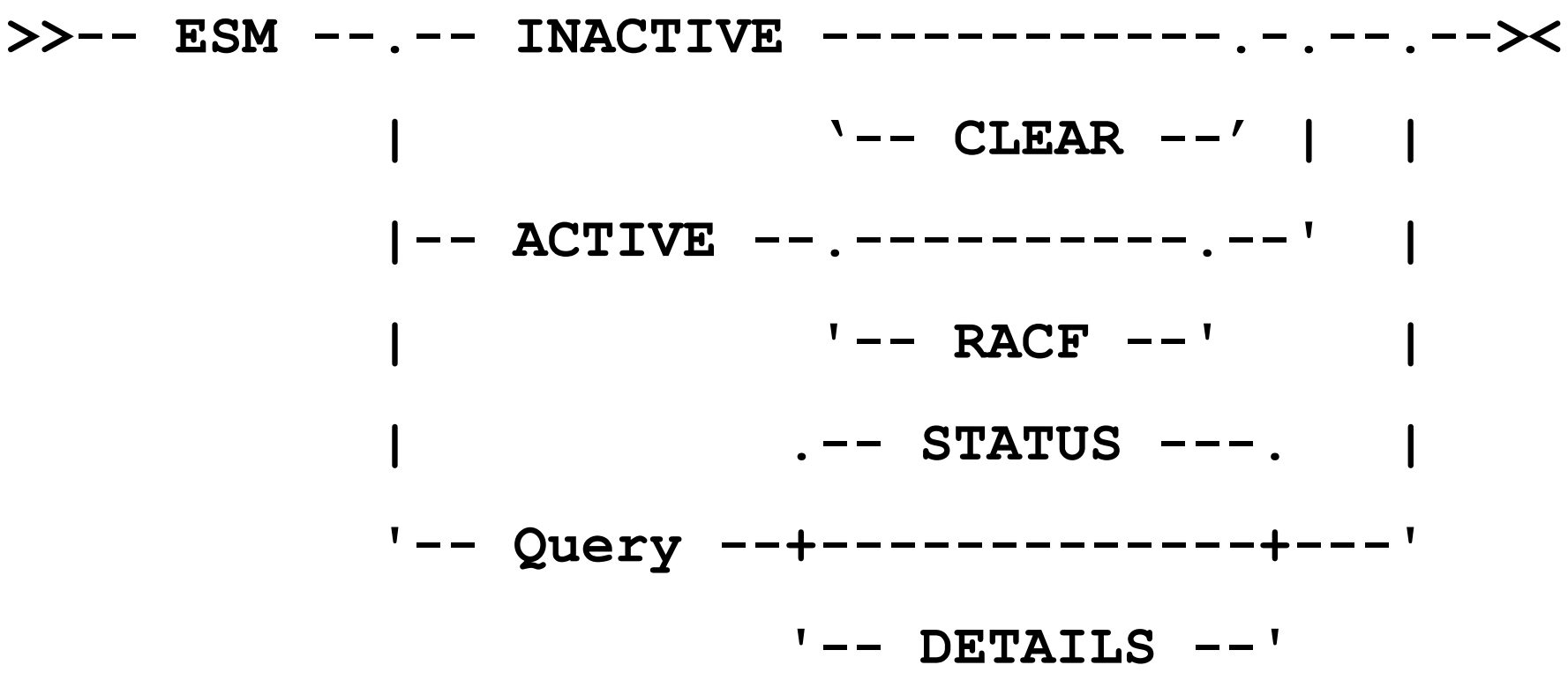
  - CP SET RACF SYSSEC {DISK|RDR|NODE|CMD…} {ALLOW|DEFER|FAIL}
  - CP SET RACF SERVER <server_userid>
  - CP SET RACF POSIX ENABLE|DISABLE
  - CP SET RACF GLOBAL_MINIDISK
  - CP SET RACF LOCK
    - No further SET RACF commands accepted
    - No UNLOCK version
    - Past this point, a reboot of the system is required for config changes

RACF/VM Simplification – QUERY RACF

- CP QUERY RACF (STATUS | DETAILS)

```
RACF has been configured as ESM
RACF Settings are not locked
RACF OpenEdition (POSIX) support is disabled
RACF Server RACFVM is used by CP
RACF Server RACMAINT is used by CP
RACF SYSSEC DISKP ALLOW DISKU DEFER DISKF FAIL DISKW DEFER DISKM ON
RACF SYSSEC RDRP ALLOW RDRU DEFER RDRF FAIL RDRW DEFER RDRM ON
RACF SYSSEC NODEP ALLOW NODEU DEFER NODEF FAIL NODEW DEFER NODEM ON
RACF SYSSEC CMDP ALLOW CMDU DEFER CMDF FAIL CMDW DEFER CMDM ON
RACF SYSSEC LANP ALLOW LANU DEFER LANF FAIL LANW DEFER LANM ON
RACF SYSSEC DEFLTP ALLOW DEFLTU DEFER DEFLTF FAIL DEFLTW DEFER RACF Global Minidisk Slot
001: AAA 0001 LOCAL ACIGRP01
RACF Global Minidisk Slot 002: AAA 0002
RACF Global Minidisk Slot 003: AAA 0003 GLOBAL
```

RACF/VM Simplification – System Config



RACF/VM Simplification – CP Exit definitions

New CP Exits for ESM use are assigned in the range 6000-61FF

- *6000 - ESM Init*
- *6001 - ESM SSI Scan HROTABLE*
- *6002 - ESM diagnose x'A0'*
- *6003 - ESM Show Details*
- *6011 - ESM request authorization*
- *6012 - ESM IUCV connect from ESM server for *RPI*
- *6013 - ESM IUCV message pending*
- *6014 - ESM IUCV sever from ESM server*
- *6015 - ESM IUCV quiesce from ESM server*
- *6016 - ESM IUCV resume from ESM server*
- *6020 - ESM Password verification*
- *6021 - ESM Password prompt*
- *6030 - ESM INACTIVE screening*

RACF/VM Simplification – QRACFCNF Utility

- QRACFCNF – utility for pulling current SYSSEC config (and other details) out of older RACF systems, for ease of use in transitioning to new configuration approach
  - Class C or E authorization will be required to issue

```
qracfcnf (config
RACF SYSSEC DISKU DEFER DISKW DEFER
RACF SYSSEC RDRU DEFER RDRW DEFER
RACF SYSSEC NODEU DEFER NODEW DEFER
RACF SYSSEC CMDU DEFER CMDW DEFER
RACF SYSSEC LANU DEFER LANW DEFER
RACF SYSSEC DEFLTU DEFER DEFLTW DEFER
RACF Global_Minidisk MAINT 0190 LOCAL ACIGRP1
RACF Global_Minidisk MAINT 019C
RACF Global_Minidisk MAINT 019D GLOBAL
RACF Global_Minidisk MAINT 019E
RACF ACTIVE
Ready; T=0.01/0.01 10:06:29
```

RACF/VM Simplification – Summary

- Goal to make security easier to adopt
  - Eliminate extra hurdles to configuration
  - No need to reboot z/VM system to come online with/without the ESM
  - Utility for migration purposes

- The ESMs are migrating to CP Exits
  - VM:Secure users will be fine with z/VM V7.5 out of the box
  - More to follow from Broadcom when they're ready

- Added bonus of making a CPLOAD MODULE easier to digitally sign…

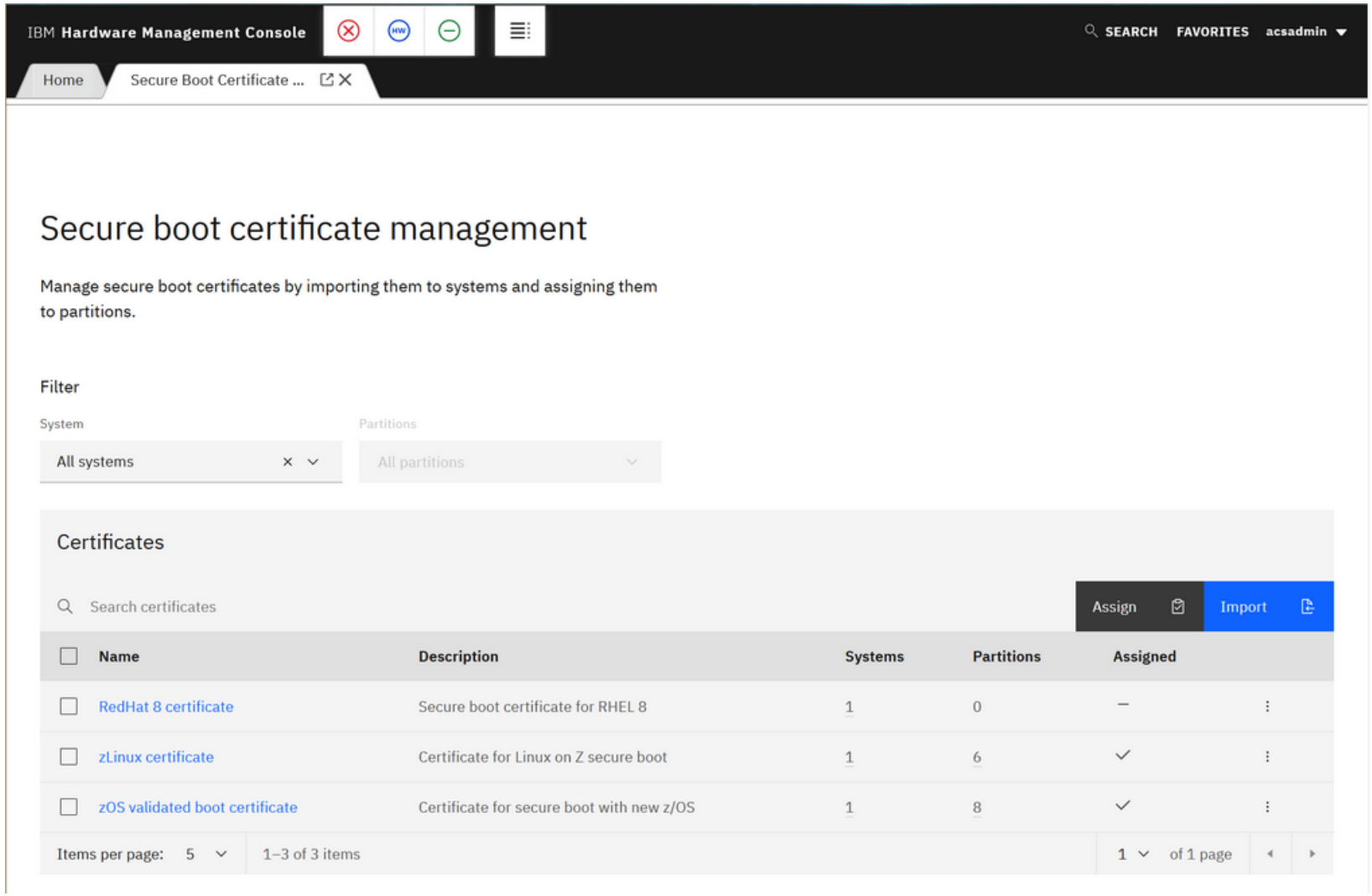
Host Secure Boot of z/VM (starting with z/VM 7.5)

Validate the module code responsible for bringing z/VM online

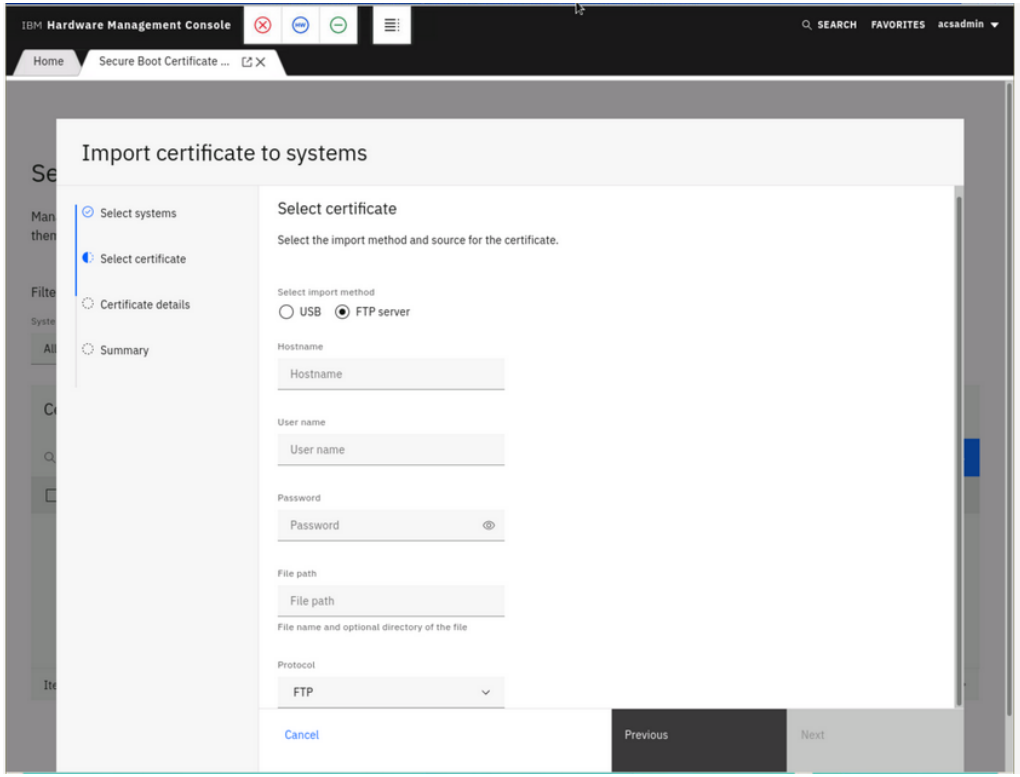
- Guest boot support has existed for a while
- z/VM 7.5 will have the capacity to validate signed SALIPL modules (at time of GA) and signed CPLOAD modules (follow-on)
  - IBM will sign these modules in-house
  - IBM will post a public key for validation purposes (www.vm.ibm.com/security)

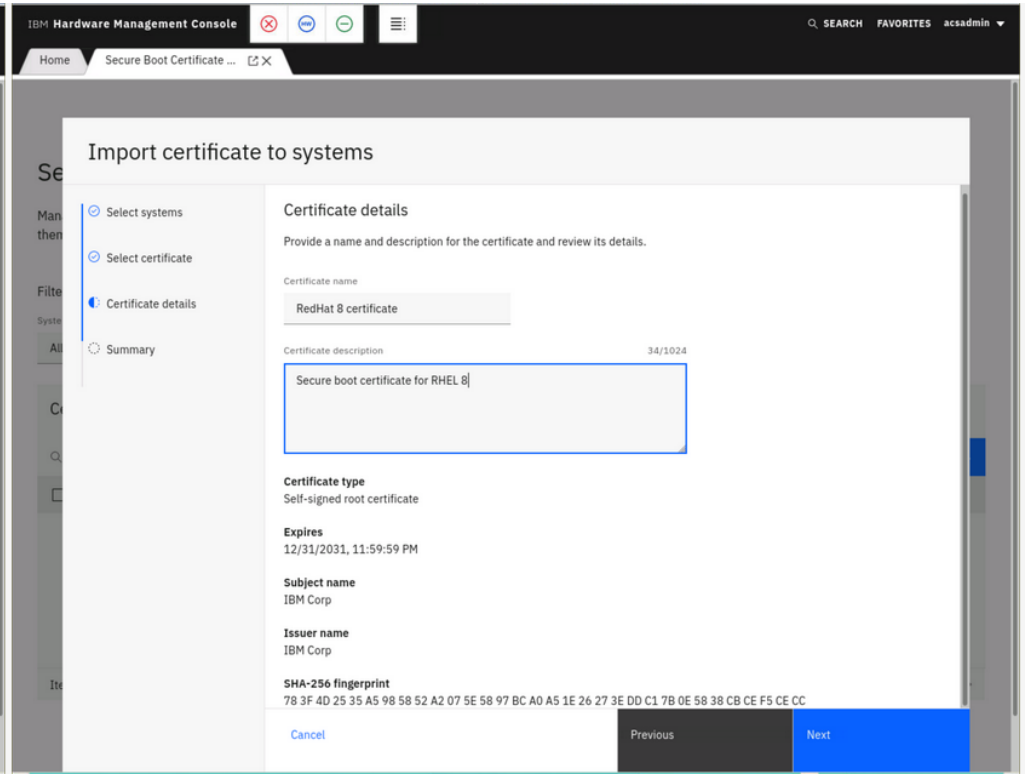
- Requires IBM z16 (with a certain level of firmware) or IBM z17
- Requires ECKD (for now)
- Requires z/VM V7.5
- Requires an appropriate certificate associated with the LPAR
- Will support second-level z/VM guests (use SET LOADDEV as you would for other guests)

SE/HMC Certificate Management – Certificate View

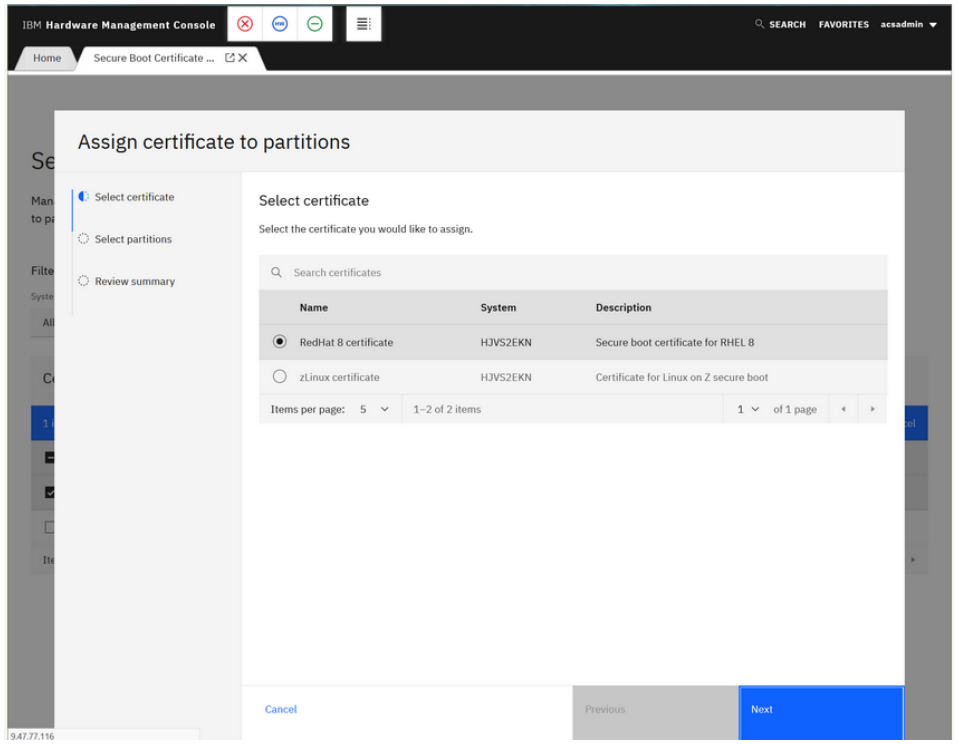


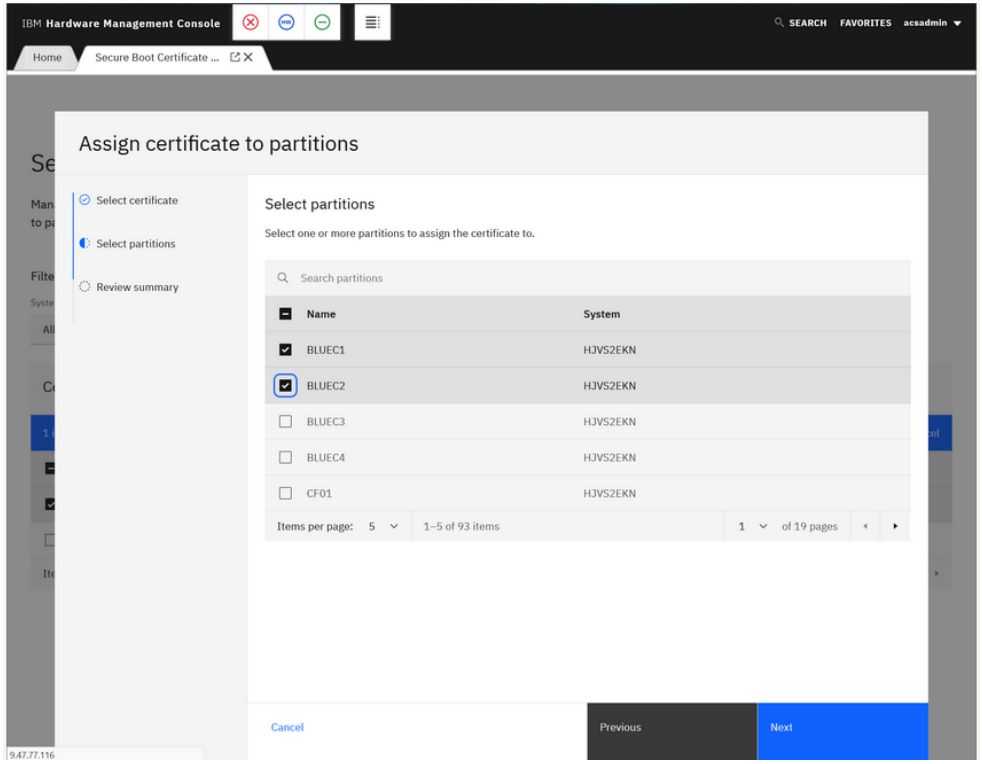
SE/HMC Certificate Management - Import





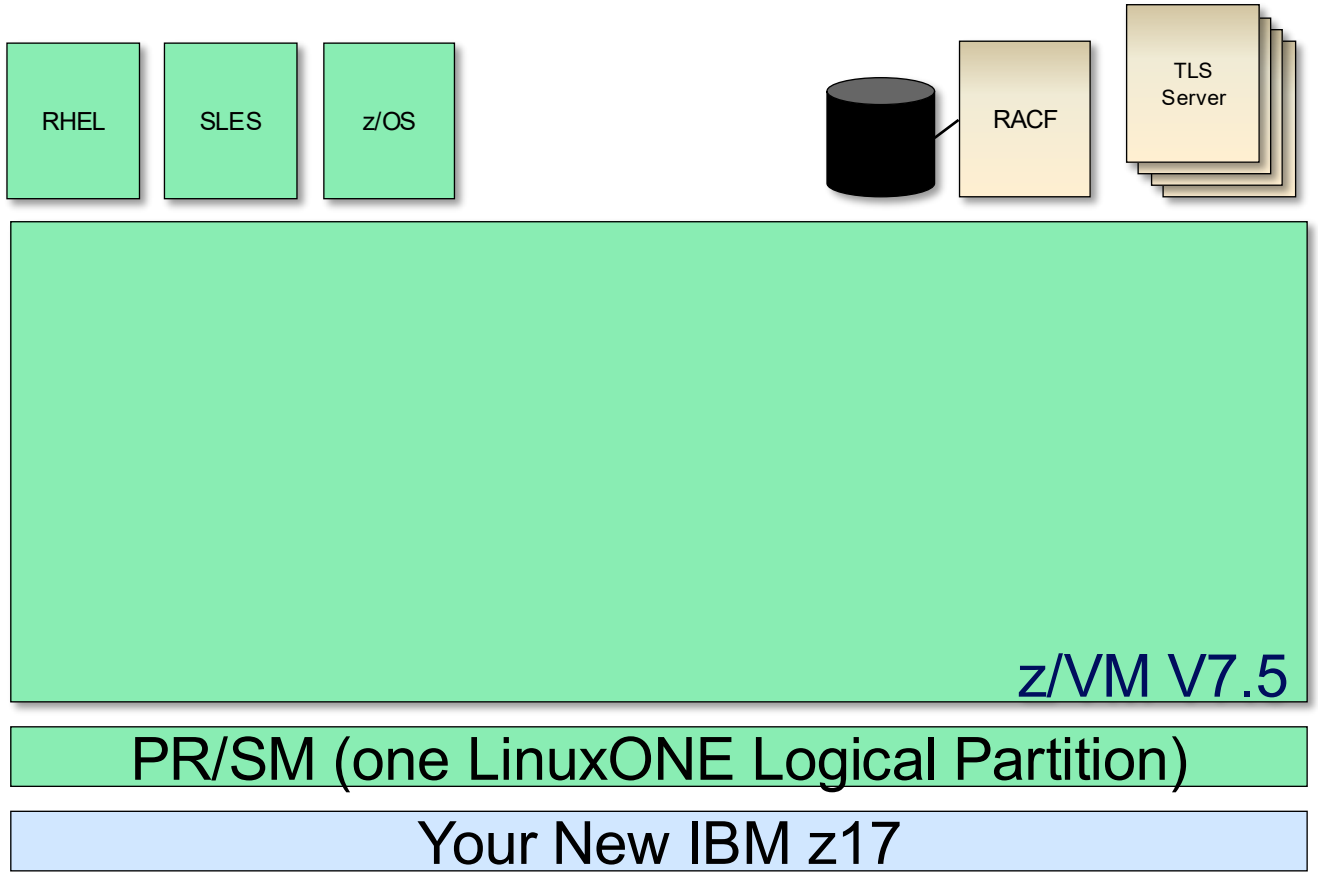
SE/HMC Certificate Management - Assign





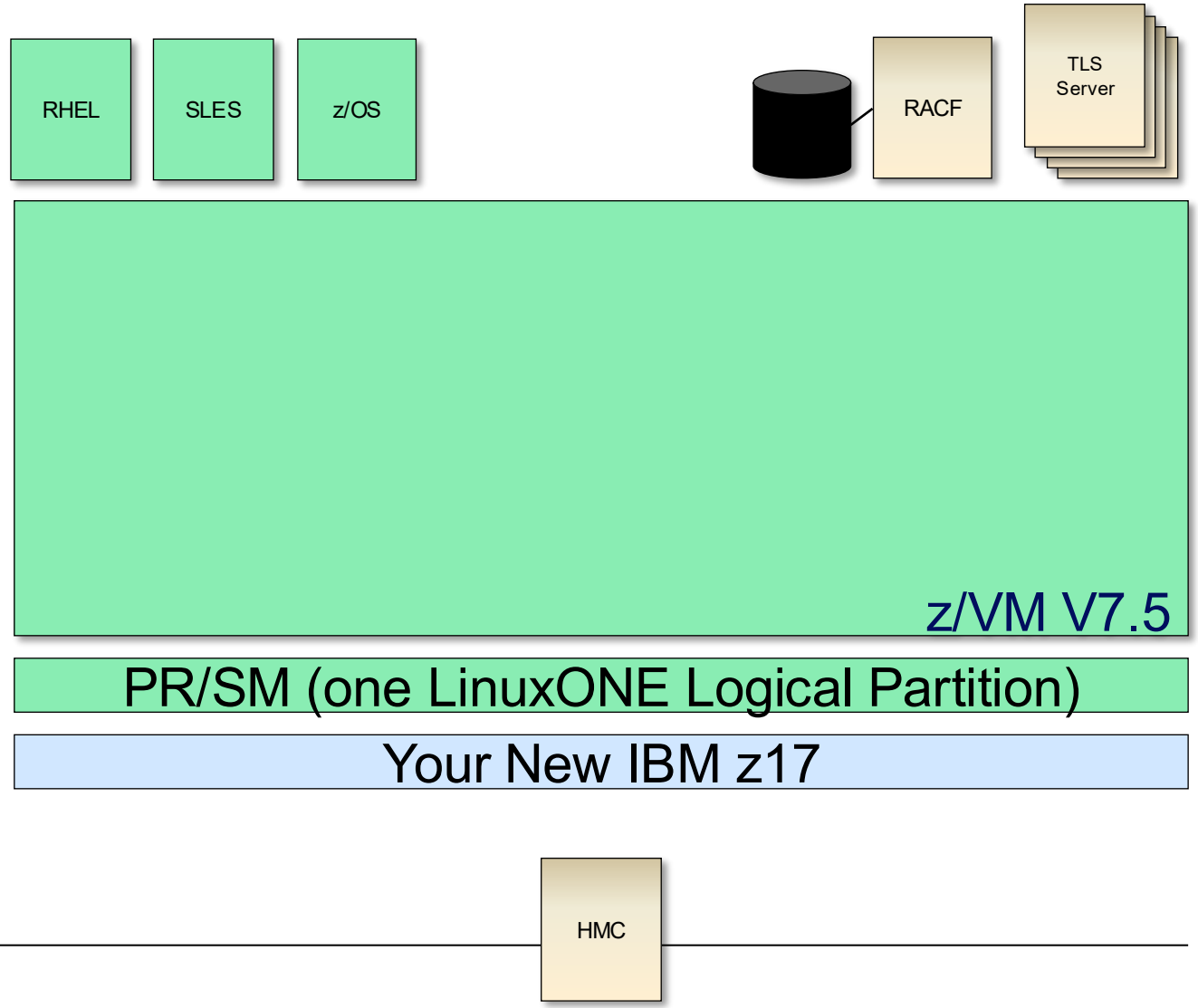
How z/VM Signature Verification Will Work

- Initiated by associating a logical partition with certain public keys on the HMC/SE
- Requires a List-Directed IPL to ECKD DASD
- For SALIPL, the signature and metadata are compiled into the module file
  - SALIPL's signature will be in PKCS #7 format
- CPLOAD will have records appended to the module that contain its signature and metadata.
- Signature content is **attached** to prevent potential conflicts inherent in having multiple files for multiple MODULEs available on an IPL volume



Reasons a z/VM Host Secure Boot might fail

- No hardware support (audit message 8514I)
- No certificates assigned to this LPAR (8511)
- CPLOAD does not have a signature (8512)
- No valid or unexpired certificates assigned to this LPAR match the signature on the module (8513)
- The system was loaded by a version of SAPL or CP that does not support secure IPL (8515)
- The system was loaded by a CCW IPL which does not support secure IPL (8516)
- Calculated hash of the module does not match decrypted signature (8523)

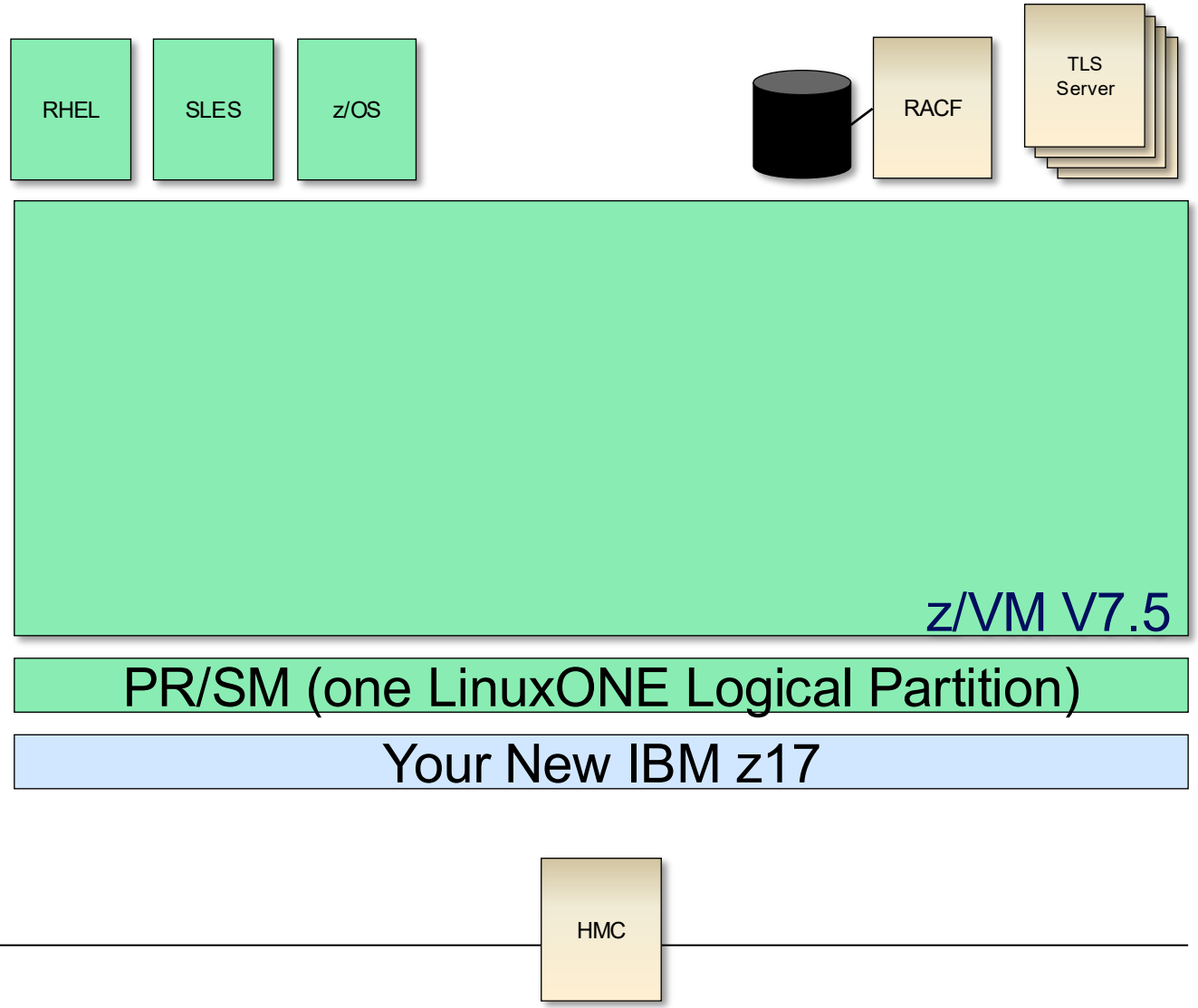


Other cases

- If z16+ or z17 does not request a secure-mode list-directed IPL, processing continues in ‘audit mode’ – zBootLoader messages may appear on Operating System Messages console, but a lack of security will not halt processing

- If you’re using an old z/VM, new hardware:
  - Works as it currently does – no new messages, because it’s still the old code

- Secure boot and use of an old SAPL and/or CPLOAD
  - If secure-mode IPL required, either zBootloader will fail to load SAPL (error messages on Operating System Message screen), or
  - SAPL will fail to validate CPLOAD

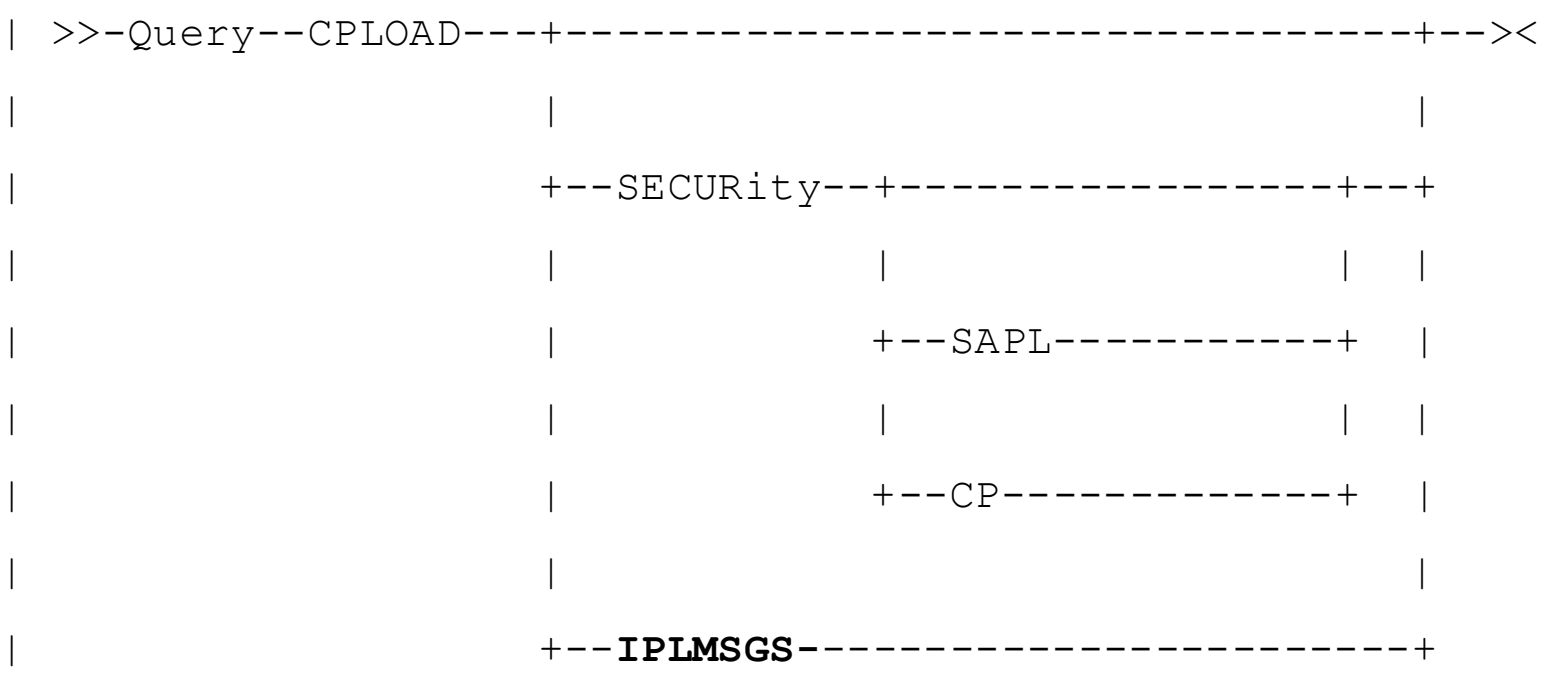


SALIPL

```
+-------------------------------------------------------------------+
| STAND ALONE PROGRAM LOADER: z/VM VERSION 7 RELEASE 5.0            |
|                             SECURE IPL = YES                      |
| DEVICE NUMBER:   01E0       MINIDISK OFFSET:    6       EXTENT:  1|
|                                                                   |
| MODULE NAME:     CPLOAD     LOAD ORIGIN:       2000              |
|                                                                   |
| ---------------------------------IPL PARAMETERS------------------ |
|                                                                   |
|                                                                   |
| -----------------------------------COMMENTS----------------------- |
|                                                                   |
|                                                                   |
|                                                                   |
| ----------------------------------------------------------------- |
|                                                                   |
|                                                                   |
|                                                                   |
| 9= FILELIST  10= LOAD  11= TOGGLE EXTENT/OFFSET                   |
+-------------------------------------------------------------------+
```

QUERY CPLOAD SECURity

- Display details of supply-chain security for CPLOAD or SALIPL



QUERY CPLOAD SECURity

- CP QUERY CPLOAD SECUR SAPL
  (date format based on the virtual machine's DATEFORMAT setting)

```
Secure IPL was requested and successful
SAPL IPL SECURITY DETAILS
HCPQCP8510I The verification of the signature of SAPL was successful.
Verification date and time:  02/04/26 17:03:20
Matching verification certificate name:
IBMtestcert
Matching verification certificate fingerprint:
E54585DB D99C0733 D1712833 F92B9317 7CC1B76F DA884826 9ADC1EC5 CCAEE28E
Matching verification certificate expiration:  05/22/29 14:35:57
Ready;
```

QUERY CPLOAD SECURity

- CP *Q CPLOAD SECURITY*

```
Secure IPL was not requested; audit only
```

- *SAPL IPL SECURITY DETAILS*

```
HCPQCP8513I The signature of SAPL did not match the signature in any of the valid and
unexpired certificates assigned to this partition.
```

- *CP IPL SECURITY DETAILS*
  (date format based on the virtual machine's DATEFORMAT setting)

```
Verification date and time: mm/dd/yyyy hh:mm:ss

Matching verification certificate name: <VCname>

Matching verification certificate fingerprint: <VChash>

Matching verification certificate expiration: mm/dd/yyyy hh:mm:ss
```

QUERY CPLEVEL SECURity

- (if a signature is present)
  (date format based on the virtual machine's DATEFORMAT setting)

```
Signed on: mm/dd/yyyy hh:mm:ss
Signed with certificate with fingerprint: <cert fingerprint>
Signature algorithm: <algo>
Hash algorithm: <algo>
Module hash: <module hash>
```

- (if no signature is present)

```
No signature found.
```

So what happens next?

- **SAPL will be signed at z/VM V7.5 GA and can be validated**

- **At a future date, IBM will start signing CPLOAD MODULE(s)**
  - These will be provided as part of linear service directly
  - Less local rebuild
  - Less use, by extension, to QUERY CPSERVICE

- **What about…**
  - SCSI devices **<< follow-on**
  - CPXLOADed text decks **<< also a follow-on**
    - Especially vital for ESM support and vendor product support
  - The algorithms
    - Currently **ECDSA.P521/SHA256**
    - Quantum-safe algorithms (ML-DSA) under discussion
  - "My mods"
    - Discussions on-going with sponsor users about assistance on localized signing
    - z/VM not presently including a signing service as part of this support

ZTRUST
Friday, 9:45am, 1201

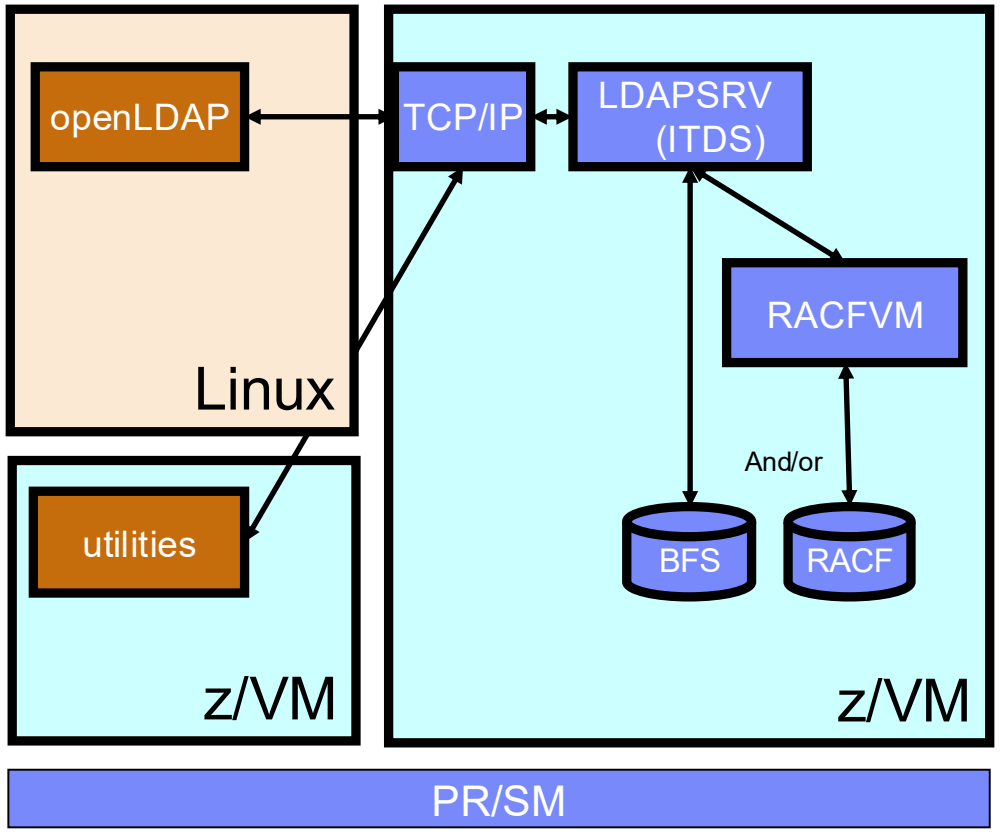
What Else Is Next?

TLS 1.3 Support

- Addition of TLS 1.3 to TLS Server
  - More secure protocol
  - Greatly reduced subset of ciphers available
  - Addition of RSASSA-PSS
  - *ChaCha20_Poly1305 under discussion at this time*
- TLS Server “Quality of Life” enhancements
  - Algorithm reordering and selection by cipher code
  - EC Curve selection
  - Extended Master Secret support (for TLS 1.2)
  - Diffie-Hellman Group Configuration
  - Server Name Indication (SNI) Configuration
- *Sponsor User program underway - https://www.ibm.com/support/pages/zvm/newfunction/#tls-1.3*

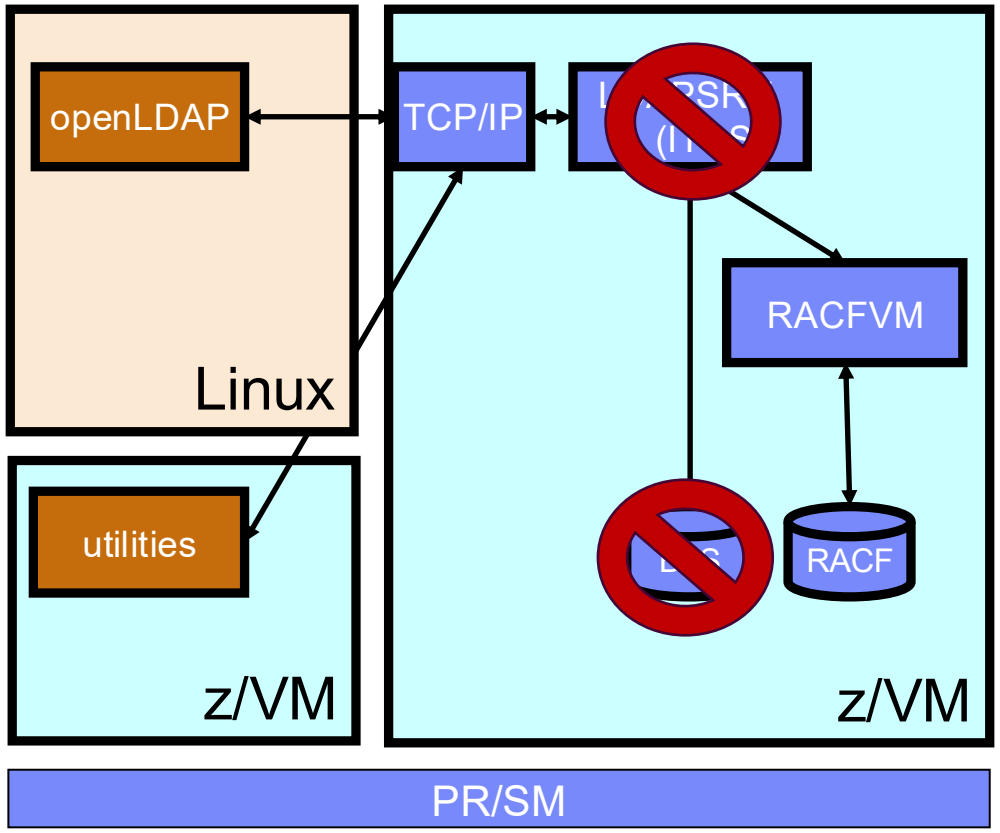
Looping back on LDAP for a moment…

- **Port of z/OS ITDS V2.2**
- **Enables remote hosts or applications to securely authenticate** users against the RACF database on z/VM
  - E.g. Linux PAM
- **Enables central management** of z/VM passwords
- **Remote audit** via LDAP extended operation
- **CMS client utilities**
  - ldapadd, ldapsrch, ldapmdfy, ldapmrdn, ldapdlet

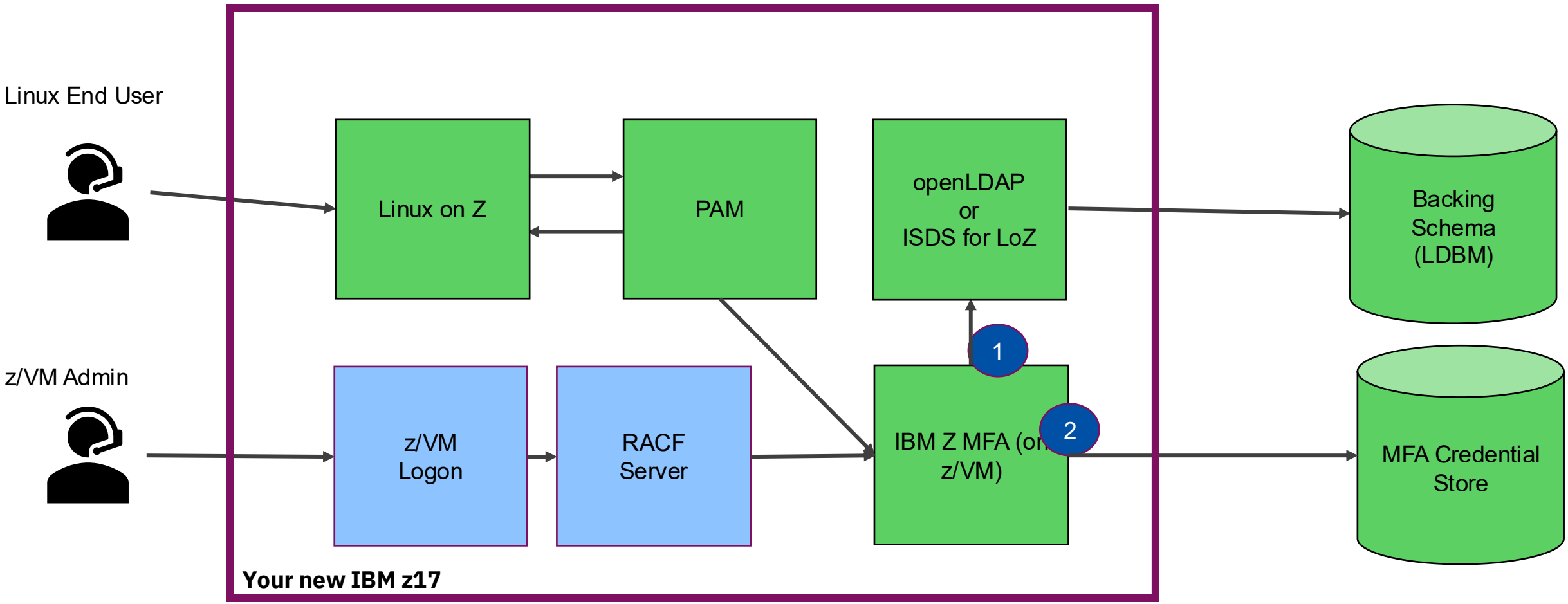


Looping back on LDAP for a moment…

- If the LDAP server goes away, then that impacts…
  - Anyone using LDAPSRV in LDBM for local **authentication**
  - Anyone using LDAPSRV with native authentication / SDBM for **authentication** via RACF
  - Anyone using LDAPSRV to automate VM guest **provisioning** / remove humans from the identity management flow
  - Anyone using LDAPSRV and SDBM to **fuel logon decisions**



What IBM proposed at the time



z/VM and Identity Management

- **There are immediate alternatives to z/VM LDAP under CMS**

- Linux ISDS and openLDAP do exist (does not talk to RACF)
- If SDBM schema matters to you, hooking into **IBM z/OS LDAP** (through IBM Z MFA, or directly via PAM) is an option
  - You can still copy a RACF/VM database over to z/OS RACF and have it function…
  - But you're back to worrying about collisions in name-space between z/OS and z/VM

- **IBM Z Multi-Factor Authentication** allows for an all-Linux solution and supports z/VM host logon as well
  - Out-of-band authentication (yes, I know, I know)
  - $$$

- ***No option is perfect, and IBM is looking to upgrade certain interfaces to enable new forms of support***

Concept: a Native Linux to VM RACF Interface (“VMRAC”)

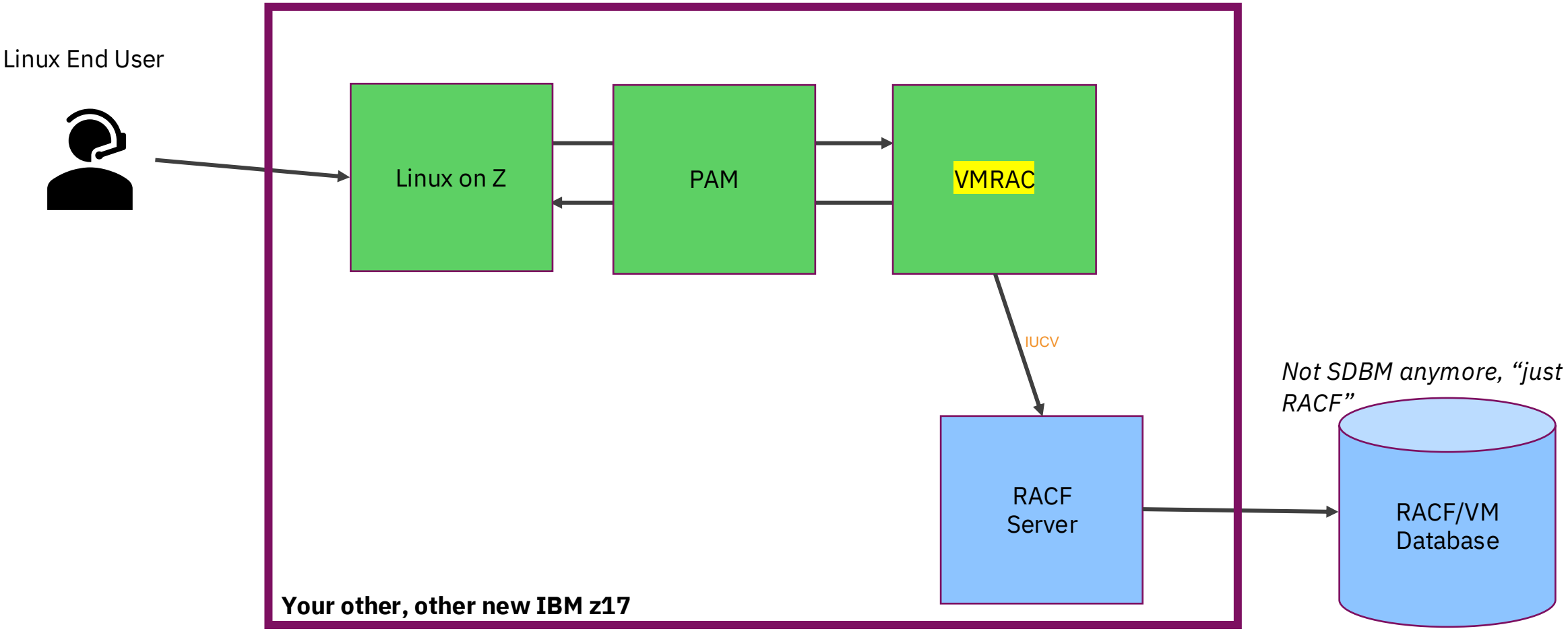
- “In theory…”

- **Two fundamental use cases**
  - Handle general authentication requests to/from RACF
  - Provide RAC style management through a Linux interface

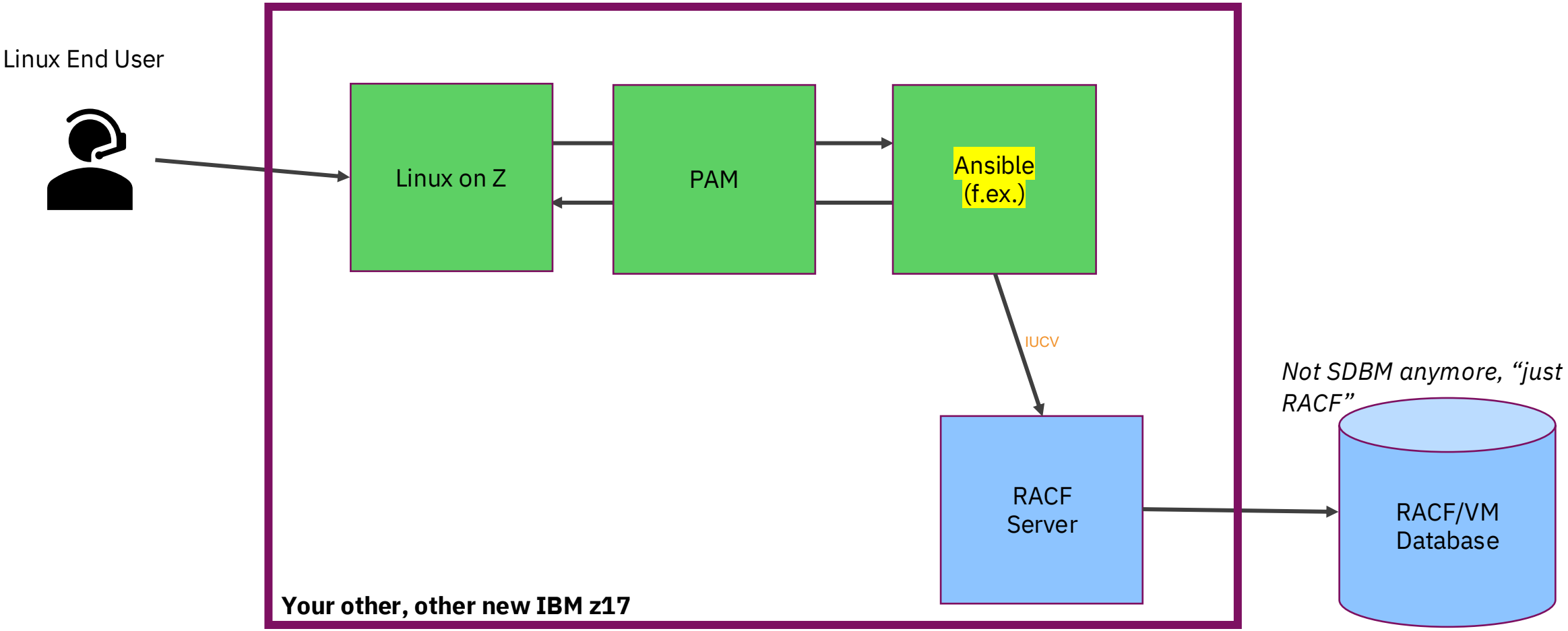
- **Pros**
  - Handle general authentication use cases
  - Make RACF management extensible by Ansible and Terraform
  - Over time, eliminate need for RACF knowledge for *general* system administration

- **Cons**
  - Not a direct replacement for ldap to RACF SDBM identity management schema
  - Some use cases may not function at GA 1

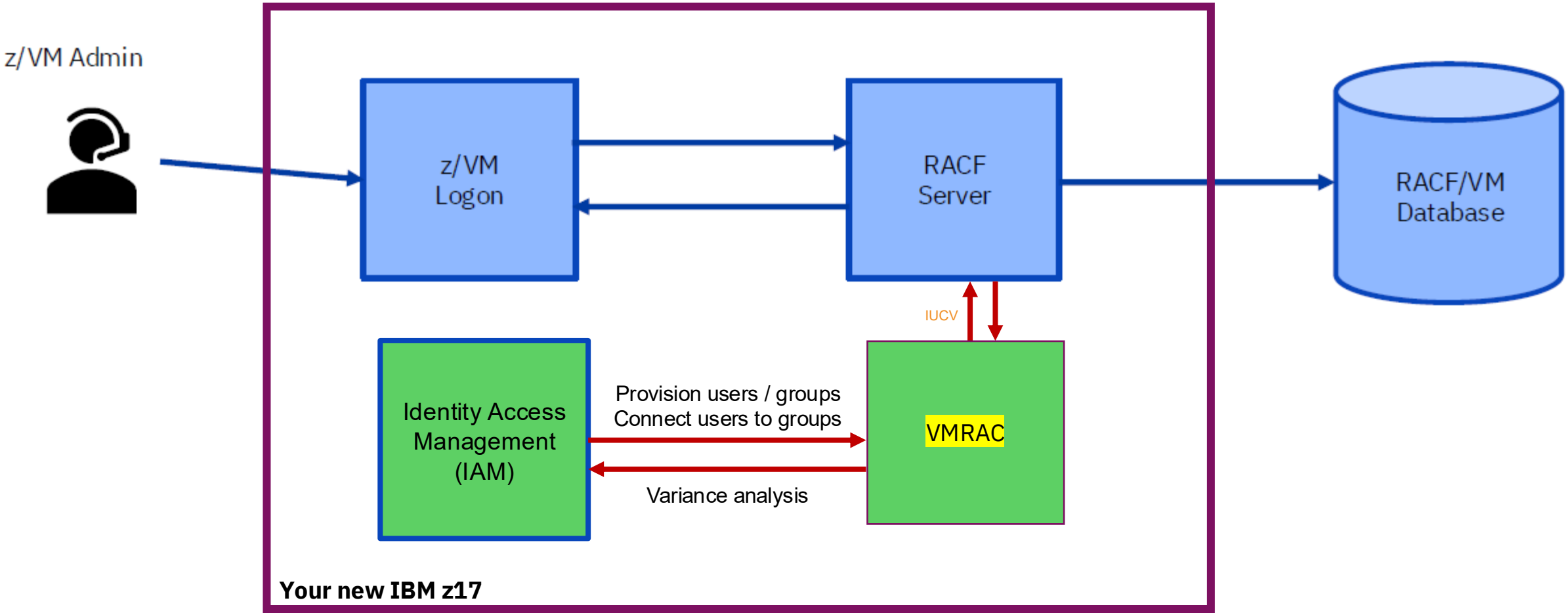
Logging onto a Linux guest using VMRAC (in theory)



Managing RACF through a Linux guest using VMRAC (in theory)



RACF identities managed via IAM through VMRAC interface (in theory)



Questions?

Summary

- **Security continues to move quickly**
  - Supply chain
  - Networking security
  - Ease of use and automation

- **Closing a door, opening a window**
  - LDAP/VM was load-bearing, heard
  - vmrac will position z/VM for a more automated future

- **More to come**
  - The move to quantum cryptography
  - The move toward compliance as code

Thank you!

Brian W. Hugenbruch

IBM Z and LinuxONE Security Certification Lead &&
IBM LinuxONE Resiliency Lead &&
IBM z/VM Security and Cryptography Product Owner

VM Security Page: https://www.ibm.com/support/pages/zvm/security/

VM New Function Webpage: https://www.ibm.com/support/pages/zvm/newfunction/

Brian's Technical blog: https://bwhugen.github.io

Social Media:

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

@the_lettersea

@apictureofaman@infosec.exchange

44


Fin