

# Preparing your z/VM systems for IBM Z Multi-factor Authentication

Brian Hugenbruch, CISSP – [bwhugen@us.ibm.com](mailto:bwhugen@us.ibm.com)  
IBM Z Security for Virtualization & Cloud:  
z/VM Security Design and Development  
🐦 @Bwhugen

© 2020 IBM Corporation

you <sup>IBM</sup>

# Why am I here?

- What is MFA?
- Why MFA for z/VM?
  - How do I get MFA for z/VM?
  - Where do I put MFA for z/VM?
- What about **my** ESM?
  - What does MFA mean for your users?
  - What about my defaults?
- Sample policies
- FAQ and Documentation

## With thanks to:

- *Jared Hunter and Dan Martin (Rocket Software)*
- *Yvonne Demeritt and JR Imler (Broadcom)*
- *Frederik Hartmann (IBM)*

# What is MFA?

## “Multifactor” or “Two-Factor” Authentication

- Proving you are who you say you are by means other than (or in addition to) a traditional password or password phrase
- Made of “something you have” (mobile device), “something you know” (password), **and/or** “something you are” (thumbprint)

*MFA is not to be confused with:*

## “Multi-Step Authentication”

- Ask for userid and a password; if both are valid, then ask for more credentials

Pro Tip: asking for two passwords does not count as two-factor authentication

- The point is to avoid the weakness of that sticky note under your keyboard

# Security-nerd terminology cheat-sheet

- **“Multifactor” or “Two-Factor” Authentication**
  - Proving you are who you say you are by means other than (or in addition to) a traditional password or password phrase
  - Made of “something you have” (mobile device), “something you know” (password), and/or “something you are” (thumbprint)
- **“Multi-Step Authentication”**
  - Ask for userid and a password; if both are valid, then ask for more credentials
- **“Userid enumeration”**
  - Determining if a username is valid before you’re authenticated to the system
  - Considered bad – allows for spearphishing attacks or brute-force logon attempts
- **“In-band authentication”**
  - Provide userid and all authentication factors at time of direct logon (e.g. in a PComm window)
- **“Out-of-band authentication”**
  - Provide authentication factors to an external server (e.g., through a browser connection), then use a “derived credential” for traditional logon screens

## Why MFA for z/VM?

- **As-Is:** logging onto a z/VM virtual machine requires either a password or password phrase for authentication purposes
  - Difficult for modern security compliance
- **To Be:** a z/VM system administrator can authenticate to the system using non-password authentication tokens
- **Pain points:**
  - Mix of ESMs in use by support
  - Mix of authentication factor requirements (RSA, Yubikey, Duo, CAC...)
  - Mix of policy requirements (userid enumeration, multifactor vs multistep, replay concerns)
- How do we make this easy to use and near-transparent to the sysprog?

*Not quite as easy as putting your retina up to your 3270 window.*

```
z/VM ONLINE

      / VV          VVV MM      MM
     / VV          VVV  MMM     MMM
    / VV          VVV  MMMM    MMMM
ZZZZZZ / VV      VVV  MM MM MM MM
   ZZ  / VV      VVV  MM  MMM  MM
   ZZ  / VV  VVV  MM  MMM  MM
   ZZ  / VVVVV  MM   M   MM
   ZZ  / VVV    MM    MM
ZZZZZZ / V      MM    MM

      built on IBM Virtualization Technology

Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ==>  _
PASSWORD ==>
COMMAND  ==>
```

# Multifactor Authentication for z/VM

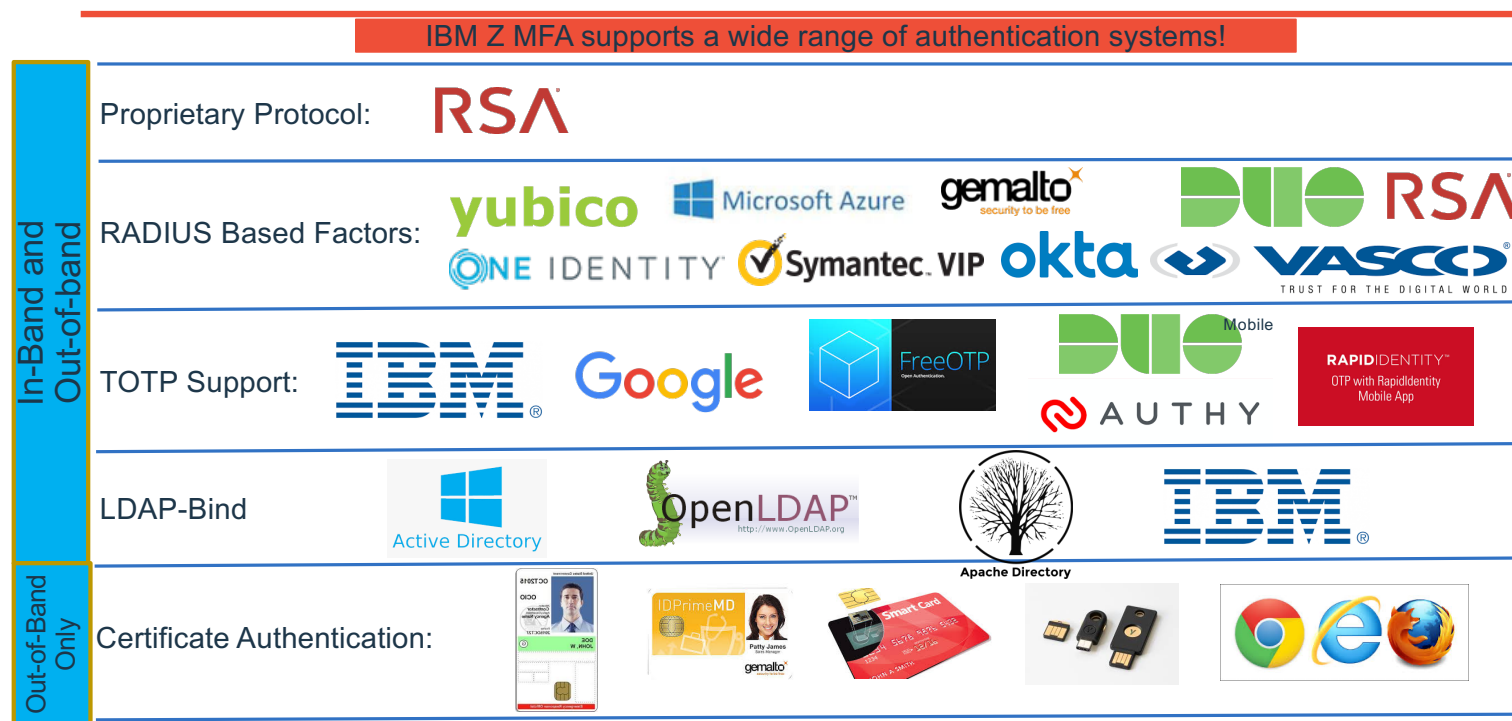
**MFA support** enables a system administrator to logon to the hypervisor without using a traditional password exclusively

## This allows:

- An administrator to present authentication factors to the MFA Server via web browser or mobile app
- “Time-valid” and “times-used” for derived credentials configurable (1 use, 1 minute, 1 day...)
- Support for LOGONBY/SURROGAT (for userids that don’t have their own logon credentials)
- Support for nearly all out-of-band factors available today for z/OS version of IBM Z MFA
  - No ESM passticket support available
  - Digital certificates and CAC cards are “out-of-band-only” anyways

# What factors work with IBM Z MFA V2.1?

MFA on z/VM will support the same factors as the **out-of-band** z/OS solution



On z/OS only, RACF Password/Passphrases, and Passtickets, can be used in conjunction with all **in-band** authentication methods.



## What we've done (a few more details)

- IBM Z Multi-factor Authentication V2.1
  - Same product as the one which runs on z/OS, but...
  - Really a new MFA server which runs as a **Linux on Z guest**
  - Serves as “policy decision point” for z/VM authentication
    - Authentication “policy enforcement point” remains your ESM
  - Supports all **out-of-band authentication** factors supported by the z/OS version
    - Cannot use ESM passwords for MFA authentication
    - Passwords/phrases remain viable for non-MFA users and/or FALLBACK support for emergencies
- z/VM support for V7.1 and later (with appropriate CP PTF or RSU applied)
- Updates to External Security Managers
  - CA VM:Secure
  - RACF for z/VM feature
  - An ESM is required as part of this solution

## What does this mean for the z/VM System Programmer?

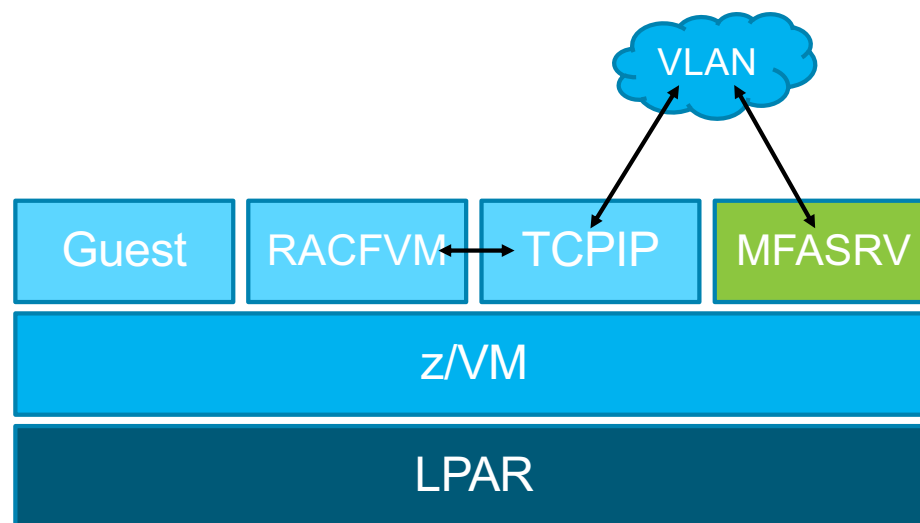
1. You acquire and set up IBM Z MFA V2.1
2. You enable support inside your ESM
3. You enable this support per user
  - Actual auth **policies** are managed in IBM Z MFA V2.1
    - This may be you or your security people
4. You logon to your z/VM system... with a slightly different flow.
  - We'll walk through this.

## (1) You acquire and set up IBM Z MFA V2.1

- Product 5655-MA1
  - If you own the "z/OS" MFA solution from IBM, it's the same product. Go ahead and download the z/VM version, too!
  - *You cannot use the z/OS version for z/VM authentication, or vice versa*
- Install into a Linux on Z guest
  - SLES 15 or later; or
  - RHEL 8.x or later
  - *Specific packages (e.g. openCryptoki, postgresql-server, openssl) will be needed in addition to the MFA package itself*
  - ***These levels are a hard requirement, not a support/test statement***
- *You may require more software if using a third-party authentication factor such as RSA SecurID. Refer to documentation for details.*

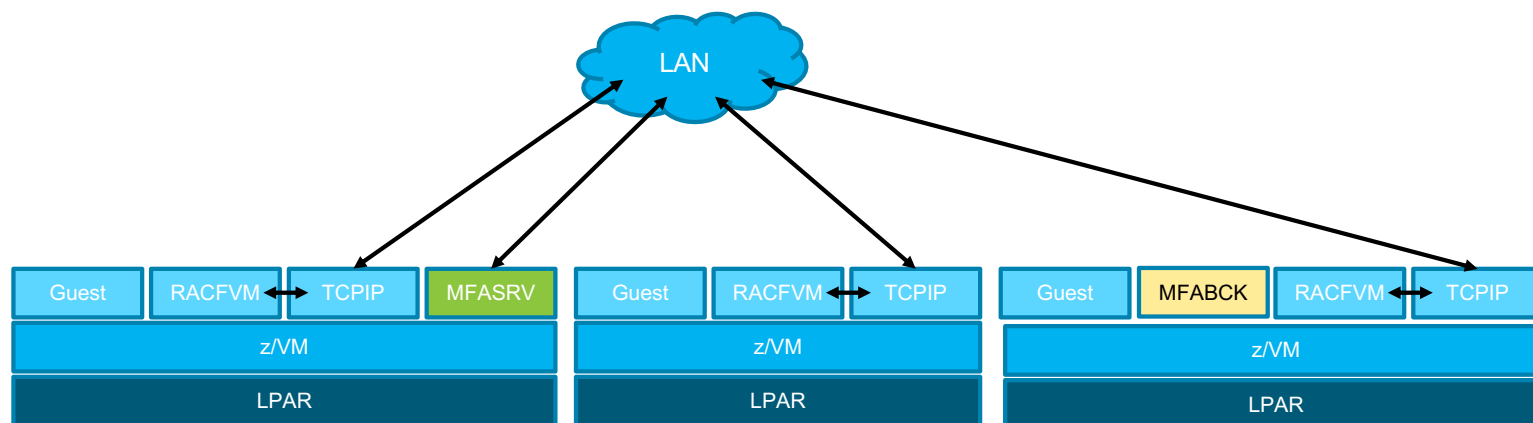
## Where do I set up IBM Z MFA V2.1 on under z/VM?

- The constraint is "one ESM database to one MFA server."
- So you could do a single system...



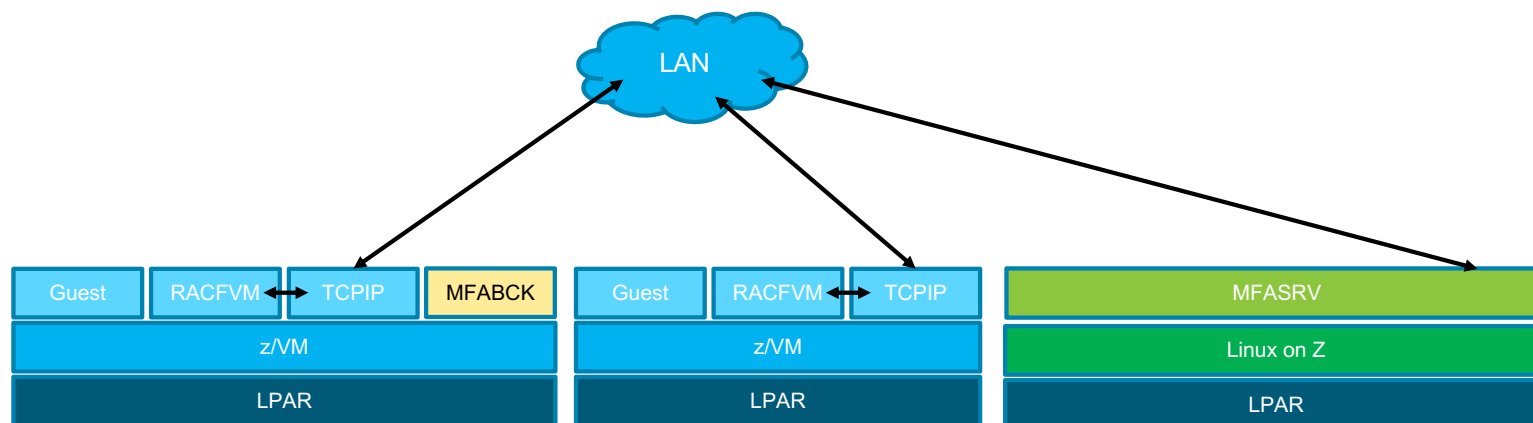
## Where do I set up IBM Z MFA V2.1 on under z/VM?

- ...or many systems. Since it runs as a Linux on Z guest, you could put the primary and back-up on different LPARs or CECs.



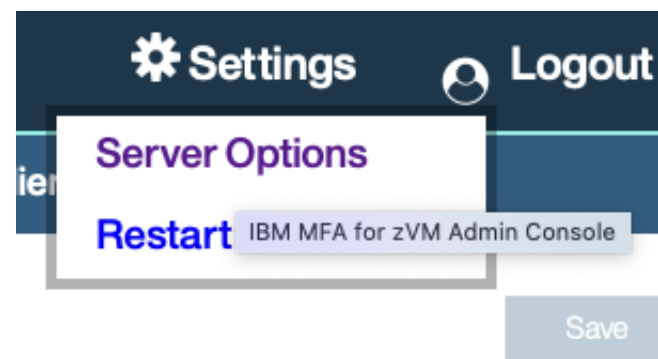
## Where do I set up IBM Z MFA V2.1 on under z/VM?

- ...since the requirement is Linux on Z, and communication is TCP/IP, you could even put the Linux guest in its own partition. Your ESM only cares about an IP address.



## IBM Z MFA: Server configuration

- Verify the z/VM Listener Port setting in the MFA Server Options matches the outbound port specified in the **MFA CONTROL** file

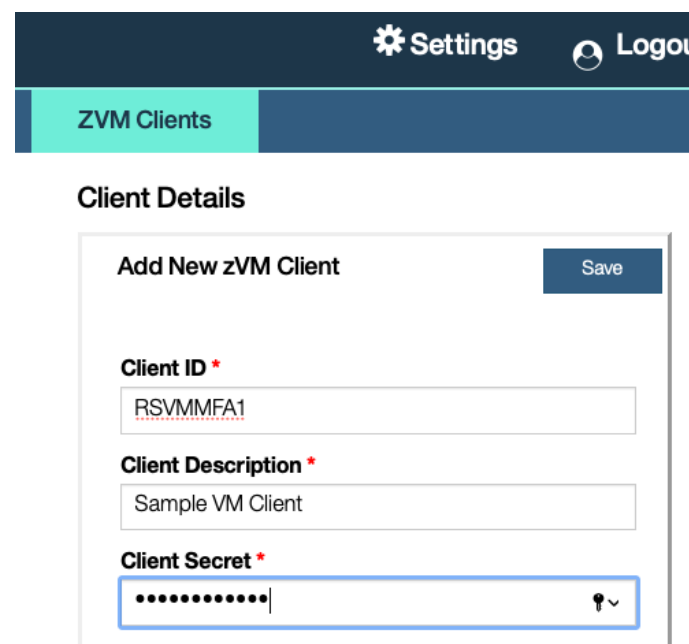


**ZVM Listener Port \***

6787

## IBM Z MFA: Server configuration

- MFA Administrator creates a z/VM Client entry whose Name and Client Secret match the **MFA CONTROL** file contents



The screenshot displays the IBM Z MFA Administrator web interface. At the top, there is a dark blue header with a gear icon for 'Settings' and a user icon for 'Logout'. Below the header, a teal sidebar contains the 'ZVM Clients' menu item. The main content area is titled 'Client Details' and features a form to 'Add New zVM Client'. The form includes three input fields: 'Client ID \*' with the value 'RSVMMFA1', 'Client Description \*' with the value 'Sample VM Client', and 'Client Secret \*' which is currently masked with dots. A 'Save' button is located in the top right corner of the form.



# IBM Z Multi-factor Authentication (Summary)

- New z/VM support under the IBM Z MFA product which already exists on z/OS
- Linux-based server which runs the MFA application (Linux on Z)
  - SLES and RHEL supported; some crypto library requirements
  - Web-based UI for administering users, factors, and policies
- **Out-of-band authentication factors** supported
  - Present all credentials to a web browser interface
  - Receive a "derived credential" (CTC) which is valid for **nn** minutes/hours for **mm** use(s)
  - Type in credential on CP LOGON where you would have used a password/phrase
  - In-band authentication factors (e.g. RACF passwords) not supported
- Can run as a guest of z/VM or in its own LPAR
  - Communicates over secure TCP/IP to your ESM
- **Policies are meant for human users**
  - Automated virtual machines don't necessarily need passwords

## (2) Configure z/VM .....and your ESM

- z/VM must be at RSU7104 or have the PTF for CP APAR VM66324
  - Or, install z/VM 7.2 when it GA's
  - Please make sure (if possible) all members of an SSI are updated!
- RACF for z/VM:
  - Apply the PTF for APAR VM66338 to z/VM 7.1
- Broadcom CA VM:Secure
  - CA VM:Secure 3.2 with the following required PTFs:
    - SO11972 - CA VM:Secure 3.2 - RSU-2001 - Recommended Service
    - SO12552 - ENH: Multifactor Authentication (MFA) support

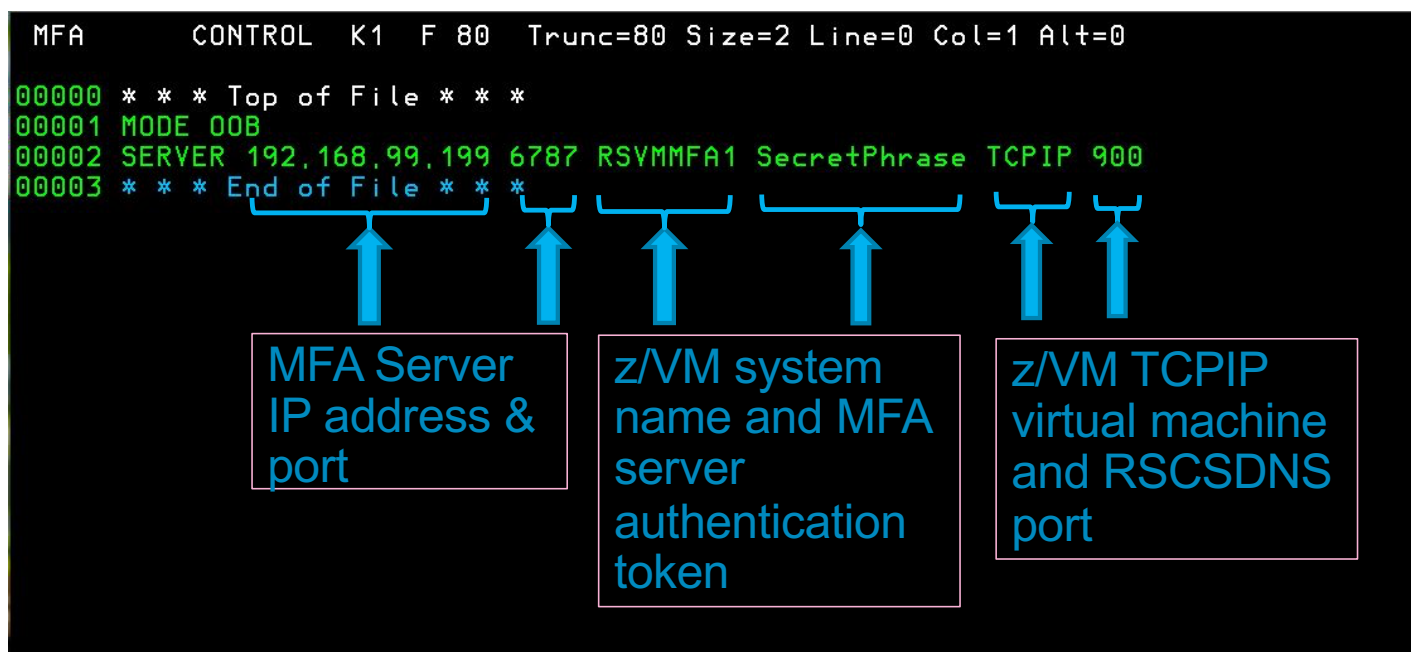
# Overview – VM:Secure MFA Support

- Out of Band (OOB) Authentication with interface to IBM Z MFA server
  - User authenticates with MFA server to receive token to logon to zVM
  - VM:Secure authenticates user/token to MFA server
    - Good – logon allowed
    - Not Good – logon not allowed (treated like invalid password)
- MFA logon is default – rules to allow FALLBACK and NOMFA
- Product Changes
  - New Configuration File and records
  - New SYSTEM level rules
  - New MFA Command
  - New CONFIG command operand
  - New Audit records and record changes
  - New processes to handle the traffic

# Overview – RACF for z/VM Support

- Changes to userid management
  - ADDUSER, ALTUSER: MFA|**NOMFA**, PWFALLBACK|**NOFALLBACK**
  - LISTUSER updates
  - SMF record support for tracking MFA logon
- Changes in broader management
  - Updates to SETROPTS LIST
  - TCP/IP interface for RACF
  - **MFA CONTROL** file for specifying server TCP/IP address, port, shared secret
  - Messages to System Operator for out-of-policy usage (e.g. PWFALLBACK)
- RACF serves as the Policy Enforcement Point for a z/VM system
  - Validates derived credential provided by the user
  - RACF passwords only required for fallback / NOMFA users
  - Can configure MFA server / failover MFA server

## Create the MFA CONTROL file



# RACF per-user MFA requirements

```
rac altuser dmartin mfa(pwfallback)
Ready; T=0.01/0.01 08:41:13
rac listuser dmartin mfa
USER=DMARTIN  NAME=DANIEL MARTIN          OWNER=MAINT710  CREATED=20.031
DEFAULT-GROUP=SYS1      PASSDATE=20.204  PASS-INTERVAL=120  PHRASEDATE=N/A
ATTRIBUTES=SPECIAL OPERATIONS
ATTRIBUTES=AUDITOR
REVOKE DATE=NONE      RESUME DATE=NONE
LAST-ACCESS=20.205/08:04:06
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED      (DAYS)          (TIME)
-----
ANYDAY
GROUP=SYS1      AUTH=USE      CONNECT-OWNER=MAINT710  CONNECT-DATE=20.031
CONNECTS=      45  UACC=NONE      LAST-CONNECT=20.205/08:04:06
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE      RESUME DATE=NONE
GROUP=SYSPROG  AUTH=USE      CONNECT-OWNER=MAINT710  CONNECT-DATE=20.031
CONNECTS=      00  UACC=NONE      LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE      RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
MULTIFACTOR AUTHENTICATION IS ENABLED
PASSWORD FALLBACK IS ALLOWED
Ready; T=0.01/0.01 08:41:19
```

## Example: End user LOGON with FALLBACK

```
logon dmartin fallback  
  
Enter your password,  
or  
To change your password, enter: ccc/nnn/nnn  
      where ccc = current password, and nnn = new password  
  
ICH70001I DMARTIN  LAST ACCESS AT 07:06:36 ON WEDNESDAY, JULY 22, 2020  
z/VM Version 7 Release 1.0, Service Level 2001 (64-bit),  
built on IBM Virtualization Technology  
There is no logmsg data  
FILES: 0002 RDR, 0002 PRT,   NO PUN  
LOGON AT 08:04:06 CDT THURSDAY 07/23/20  
z/VM V7.1.0      2020-01-28 13:46  
  
Ready; T=0.01/0.01 08:04:08
```

## Example: OPERATOR messages when FALLBACK used

```
06:22:19 GRAF 1200 LOGON AS MAINT710 USERS = 27
DVHRLY3886I Hourly processing started; with 0 log
DVHRLY3886I files.
DVHRLY3886I Hourly processing started; with 0 log
DVHRLY3886I files.
RPILGN100I User DMARTIN logged on with parameter FALLBACK.
08:04:06 GRAF 1201 LOGON AS DMARTIN USERS = 28
```



## (2) Configuring your ESM (continued)

- Your ESM should use z/VM TCP/IP and TLS to connect secure to MFA
  - Shared secret in pertinent config file
  - Failover address for your back-up MFA server
- MFA is enabled on a per-user basis
- Password fallback is enabled on a per-user basis
- MFA should be enabled for human users
  - Service machines should be AUTOONLY or LBYONLY anyway
  - Linux guests won't have or need hypervisor-level passwords

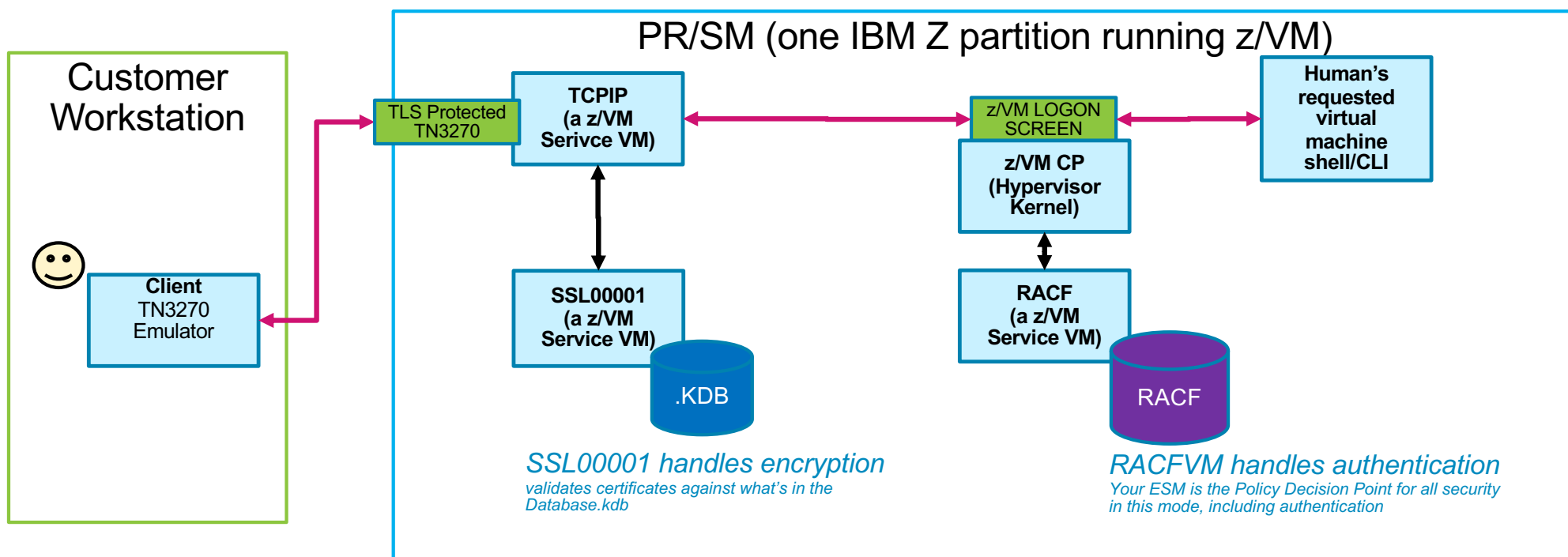
## What servers is this protecting?

- z/VM userids (primary beneficiary)
  - **Meant for human users**
  - Not meant for automated task servers (SVMs) or “technical users”
    - Works for SURROGAT/LOGONBY users!
- HMC (RSA SecurID only)
  - **Also meant for human users**
  - As previously provided for the z/OS version
- Future: expand PAM so Linux on Z guests can use this support, too
  - IBM Z MFA on z/OS can already support Linux on Z guests; next logical step for us

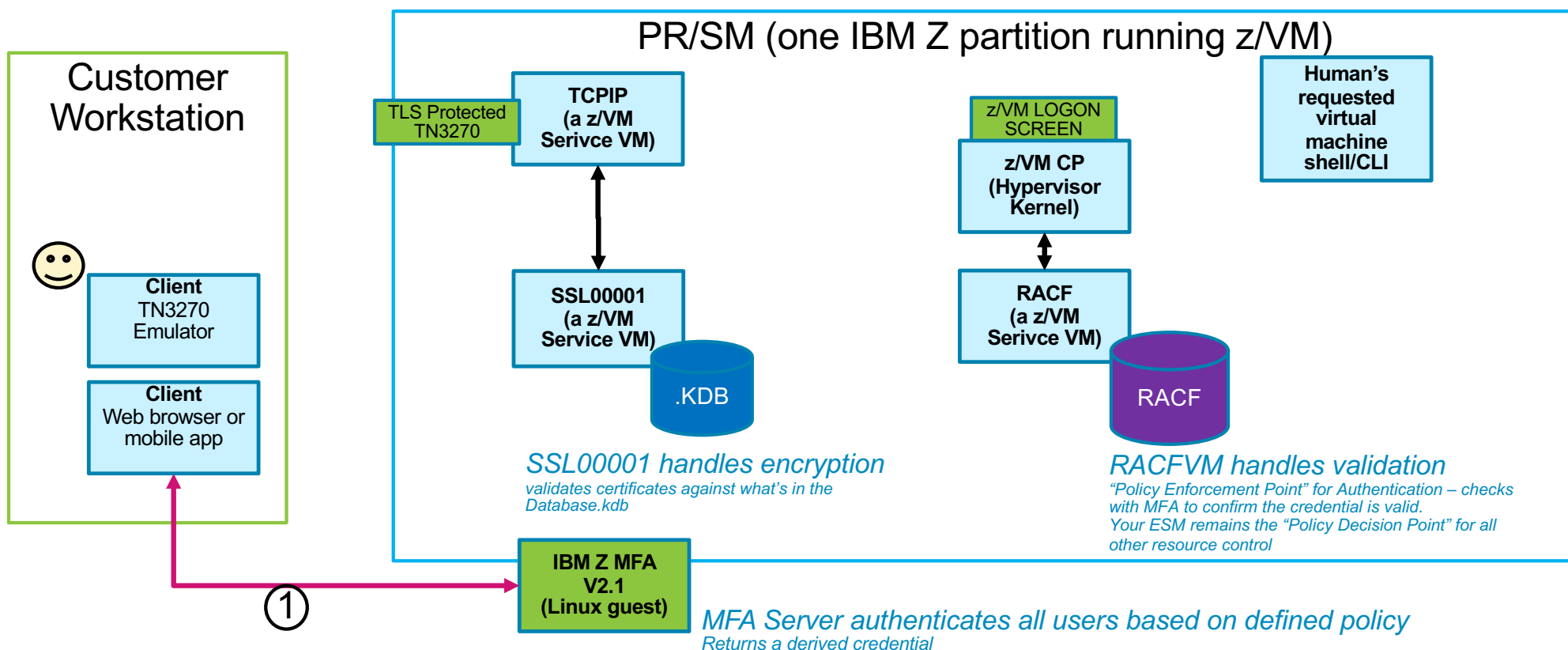
## Setting an MFA policy or policies

- Users, factor configuration, and policies are defined via web browser
  - Users may have multiple policies associated with them
  - Use of factors may be limited based on defined policies
- 
- *Note: tooling included to help identify and migrate z/VM userids for inclusion in the MFA server—you don't have to do all this by hand!*

## Authentication Flow (z/VM in the Before Times)



# Authentication Flow (z/VM with MFA)



## How does out-of-band authentication work? (1/2)

Browser address bar: <https://yourmfa.ipaddress.com/policy/dual/>

**DUAL**

User ID:

[AZFYUB1 \(YubiKey RADIUS Auth\)](#)

[Enter Your Yubikey string](#)

Passcode:

[AZFSIDP1 \(RSA SecurID\)](#)

[Enter your SecurID passcode](#)

Passcode:


## IBM Z MFA: Example Policy #1

- This policy requires two factors:
  - TOTP
  - Password controlled by the IBM Z MFA server

**PASSTOTP**

**User ID**

**IBM TouchToken or Generic TOTP**  
Enter your TOTP credential

**Password Authentication**  
Enter your MFA password. If you wish to change it, also enter and confirm a valid replacement.  
 

**Submit**


## IBM Z MFA: Example Policy #2

- This policy requires two factors:
  - Yubico OTP
  - Password controlled by the IBM Z MFA server

**PASSYUBI**

**User ID**

**Yubico OTP**  
Enter your Yubico OTP credential

**Password Authentication**  
Enter your MFA password. If you wish to change it, also enter and confirm a valid replacement.  
 

**Submit**



## How does out-of-band authentication work? (2/2)

Browser address bar: [https://yourmfa.ipaddress.com/policy/dual/yourtoken\\_returned\\_here](https://yourmfa.ipaddress.com/policy/dual/yourtoken_returned_here)

### Authentication Token

**S+L\*Vyzu**

Click the above Cache Token Credential to copy it to Clipboard,  
and use this in place of your password to access applications

Password:

**AZFSIDP1 (RSA SecurID)**

Enter your SecurID passcode

Passcode:

## Take that derived credential and use it in CP LOGON

```
z/VM ONLINE

      / VV      VVV MM      MM
     / VV      VVV MMM      MMM
    / VV      VVV MMMM     MMMM
   / VV      VVV MM MM MM MM
  / VV VVV      MM  MMM  MM
 / VVVV      MM  M   MM
/ VVV      MM      MM
V      MM      MM

built on IBM Virtualization Technology

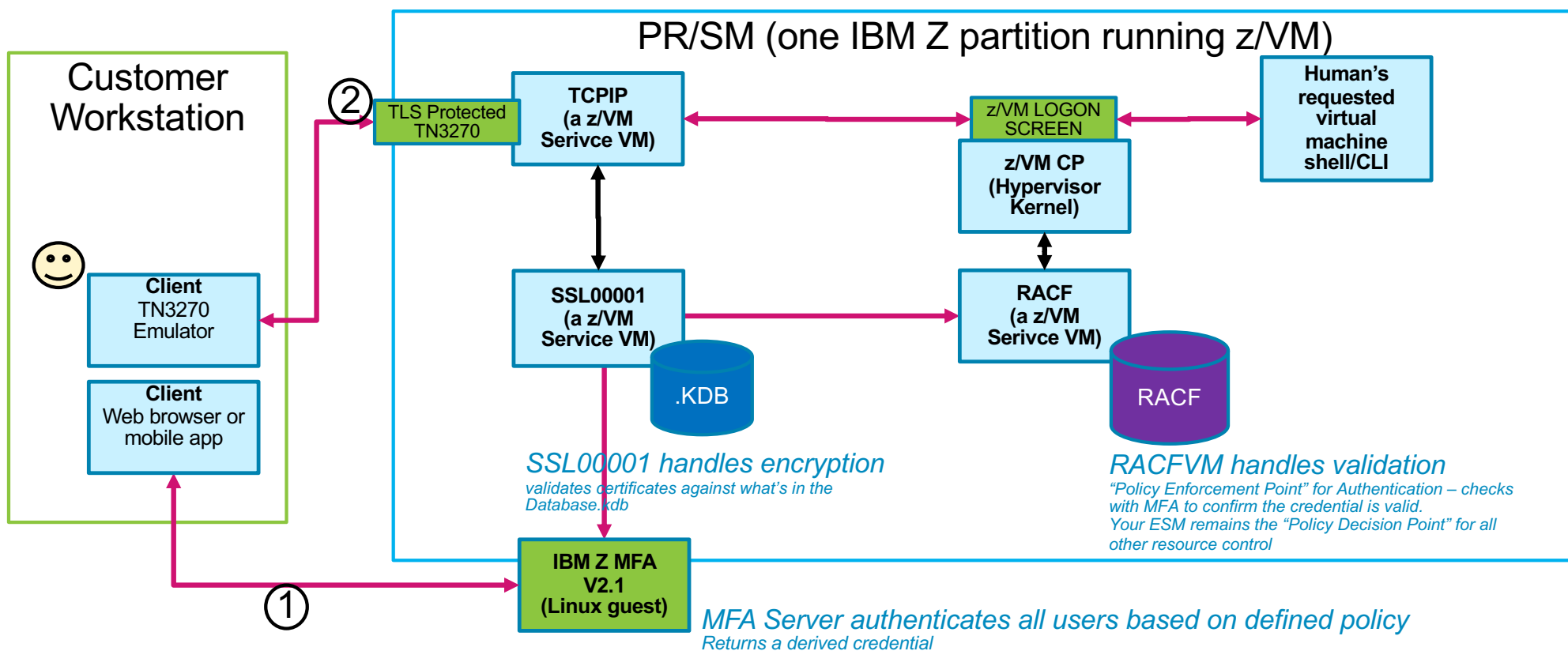
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ==> myuserid
PASSWORD ==> _
COMMAND  ==>
```

```
LOGON MYUSERID

Enter your password,
or
To change your password, enter: ccc/nnn/nnn
      where ccc = current password, and nnn = new password

_
```

# Authentication Flow (z/VM with MFA)



## Logging On (Summary)

- You authenticate to MFA directly, based on the URL of your policy
  - You provide all factors on one screen
  - You are given a derived credential for use in z/VM
- The features of this credential are configurable
  - Number of uses
  - Time of validity (seconds, minutes, up to 24 hours)
  - Length and character set (8-16, alphanumeric, special)

# Sample Policy Discussion

- **FACT:** You can have more than one policy per human user
  - E.g., if you forget your physical RSA SecurID at the office, you can authenticate with a second policy that does not require RSA SecurID
- **FACT:** Your ESM will determine Surrogate / Logonby applicability
  - E.g., logging onto **MAINT710 by BWHUGEN** will call out for the MFA credentials associated with BWHUGEN, not MAINT.
  - Also true if we logon **GSKADMIN by BWHUGEN**.
  - This is part of why replaying the derived credential, or keeping it valid for 24 hours, may be pertinent to your environment.
- **FACT:** You can have different policies for different types of human users
  - Because not all humans have the same security requirements or access the same types of virtual machines
  - Even true when logon-by – **MAINT710 by BWHUGEN** may require a different authentication policy than **MAINT710 by ROMNEY**

## Sample Policy (Example)

- **Hartmann-Co** configures its z/VM instances with an ESM and the MFA Server for four LPARs in a Single System Image
  - It uses Yubikeys elsewhere in the enterprise
  - It has Active Directory for enterprise identity management
  - **Their administrator configures two MFA policies:** one with a digital certificate and a Yubikey, and one with a digital certificate and an ldap-bind into Active Directory
    - They've **decided** tokens last 12 hours and are replayable
- **Human User Brian** logs onto z/VM at Hartmann-Co when he arrives at the office (08:00am)
- He authenticates at **Browser Address 1** with a **digital certificate and a Yubikey**. He receives a token and uses it to issue:
  - LOGON MAINT710 by BWHUGEN (09:00am)
  - LOGON GSKADMIN by BWHUGEN (09:30am)
  - LOGON TCPMAINT by BWHUGEN (03:00pm)
- When he returns home (09:00pm), he realizes he needs to issue one more command, but he's left his Yubikey at the office.
  - He authenticates at **Browser Address 2** with a **digital certificate and his Active Directory password** (09:00pm)

## Frequently Asked Questions

- **Is my preferred factor supported?**

Maybe! The developers have put a lot of work into adding new factors with each version. And the slide earlier in this deck is generic—RADIUS support, for example, is meant to interoperate with several flavors of the standard. Similarly with Yubikey.

Is something missing? Let us know!

- **Can't I just use the (z/OS or z/VM) version for (z/VM or z/OS)?**

No. Communication styles and ESM interactions are different. Besides which, we want to avoid namespace collision and policy conflict between systems.

# Your Turn!

*Do you have any “infrequently asked questions” to ask?*




## Summary

- Multi-Factor Authentication support is ready for z/VM 7.1!
  - Multiple ESMs supported by new IBM Z MFA V2.1
  - Runs in a Linux on Z guest (on z/VM or in LPAR)
  - Secure TCP/IP connection between ESM and MFA
- Allows z/VM to meet modern security policies
- Your feedback is important!
  - Factors, policy configuration, z/VM-side or ESM support
  - We want to make this as easy and intuitive to use as possible

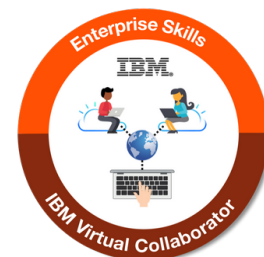
# For More Info about MFA for z/VM...

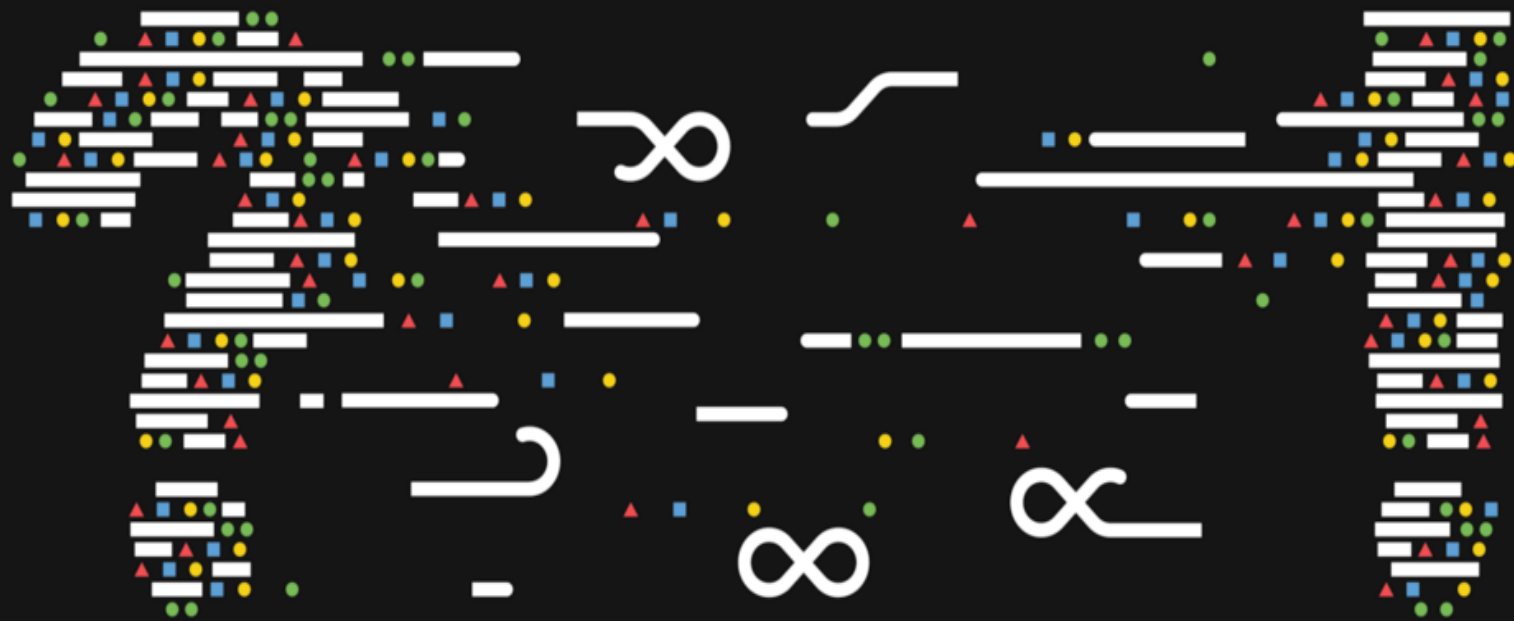
- **IBM Z MFA V2.1 Announce Letter:**  
[https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep\\_ca/5/897/ENUS220-175/index.html&lang=en&request\\_locale=en](https://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/897/ENUS220-175/index.html&lang=en&request_locale=en)
- **IBM Z Multi-factor Authentication for z/VM Manual (SC27-4938-40):**  
[https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zMFAv210sc274938/\\$file/azfv100\\_v2r1.pdf](https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zMFAv210sc274938/$file/azfv100_v2r1.pdf)
- **MFA for z/VM on the New Function Webpage:**  
<https://www.vm.ibm.com/newfunction/#mfa>
- **APAR VM66338 Details:**  
<https://www.ibm.com/support/pages/node/6205541>
- **“Preparing for Multi-Factor Authentication on z/VM” presentation (recorded live at the VM Workshop):**  
<https://www.youtube.com/watch?v=AFkOtqEZxAc>

Contact Information:

**Brian W. Hugenbruch**  
**IBM Z Security for Virtualization & Cloud**  
**[bwhugen at us dot ibm dot com](mailto:bwhugen@us.ibm.com)**  
 **[@Bwhugen](https://twitter.com/Bwhugen)**

CISSP®





## Question: “What level of software do I need?”

Component	Requirement
IBM z/VM	z/VM 7.1 with RSU 7104 and/or the PTF for CP APAR VM66324
IBM RACF for z/VM feature	z/VM 7.1 with the PTF for RACF APAR VM66338
Broadcom CA VM:Secure	<b>CA VM:Secure 3.2</b> with the following required PTFs: <ul style="list-style-type: none"> <li>• SO11972 - CA VM:Secure 3.2 - RSU-2001 - Recommended Service</li> <li>• SO12552 - ENH: Multifactor Authentication (MFA) support</li> </ul>
IBM MFA Server and GUI Components	<p>The SUSE Linux Enterprise Server on IBM Z must be at the following versions:</p> <ul style="list-style-type: none"> <li>➤ <b>SLES 15 or later</b></li> </ul> <p>The Red Hat Enterprise Linux Server on IBM Z must be at the following versions:</p> <ul style="list-style-type: none"> <li>➤ <b>8.x or later</b></li> </ul>
Postgres database	<p>For SUSE Linux Enterprise Server on IBM Z:</p> <ul style="list-style-type: none"> <li>➤ <b>libpq5</b></li> <li>➤ <b>postgresql10-server</b></li> </ul> <p>For Red Hat Enterprise Linux Server on IBM Z:</p> <ul style="list-style-type: none"> <li>➤ <b>postgresql-server</b></li> </ul>
openCryptoki	<p>For SUSE Linux Enterprise Server on IBM Z:</p> <ul style="list-style-type: none"> <li>➤ <b>openCryptoki</b></li> <li>➤ <b>openCryptoki-64bit</b></li> </ul> <p>For Red Hat Enterprise Linux Server on IBM Z:</p> <ul style="list-style-type: none"> <li>➤ <b>openCryptoki</b></li> <li>➤ <b>opencryptoki-swtok</b></li> </ul>
openssl	<p>For SUSE Linux Enterprise Server on IBM Z -- <b>1.1.0</b></p> <p>For Red Hat Enterprise Linux Server on IBM Z -- <b>1.1.1</b></p>