



# IBM SystemZ Multi-Factor Authentication

  
**Günter Weber, [weberg@de.ibm.com](mailto:weberg@de.ibm.com)**

Techsales – IBM z Security Solutions

April 5, 2022

# What is multi-factor authentication ?

### SOMETHING THAT YOU KNOW

- Usernames and passwords
- PIN Code



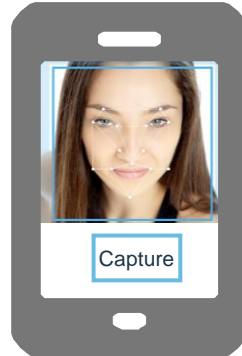
### SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
- Time-based



### SOMETHING THAT YOU ARE

- Biometrics



# Question: What factors may I use?

MFA can be used for z/OS and z/VM

IBM Z MFA supports a wide range of authentication systems!

In-Band and Out-of-band	Proprietary Protocol:	
	RADIUS Based Factors:	         
	TOTP Support:	     
	LDAP-Bind	   
Out-of-Band Only	Certificate Authentication:	    

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

# New with V2.2 - Multiple Factor Instances

---

- For service bureaus and other customers with segmented user populations
- Currently for factors that rely on external network services:
  - All RADIUS factors
  - All RSA SecurID variants
  - LDAP Simple Bind
  - AZFCKCTC (special factor for remote CTC checking)
- Example: Different user populations supported by the same RACF database can authentication against distinct RADIUS servers

# Terminology

## In-band authentication:

you present the credentials (e.g. Touchtoken) directly into the application (and via the application to e.g. RACF). For in-band authentication, you generate a token using IBM MFA with SecurID, IBM TouchToken, IBM MFA for generic RADIUS, IBM MFA for SafeNet RADIUS, or RSA SecurID RADIUS and use that token directly to log on

## Out-of band authentication:

allows you to authenticate on a user-specific web page with one or more factors (including the RACF Password !) to retrieve a cache token credential (of 8-characters) that you use to login (the cache token is used „in-band“)

Authenticating with two or more factors is called "**compound authentication.**"

The important thing to note about compound authentication is that **all** configured authentication factors must succeed for the user to retrieve the in-band authentication code.

## IBM MFA Compound In-Band authentication:

is combination of one of these factors\*, and a passphrase or password, separated by a valid separator [a colon (:), a forward slash (/) or a vertical bar (|)]

\*AZFSIDP1 ((RSA SecurID), AZFTOTP1 (IBMTouchToken)  
AZFRADP1 (generic RADIUS), AZFSFNP1 (SafeNet RADIUS)  
AZFSIDR1 (RSA RADIUS)



# Example Out-of-Band-Policy

- This policy requires two factors:
  - TOTP
  - MFA Password

OoB-policy created via RACF-Command:

```
RDEF MFADEF POLICY.SPIEZ-POLICY
MFPOLICY(FACTOR(AZFTOTP1,AZFPASS1) TOKENTIMEOUT(600)
REUSE(N))
```

A UID would be enabled to use the policy by running the following command: `ALU <RACF-UID> MFA(ADDPOLICY(SPIEZ-POLICY))`

**PASSTOTP**

**User ID**

**IBM TouchToken or Generic TOTP**

Enter your TOTP credential

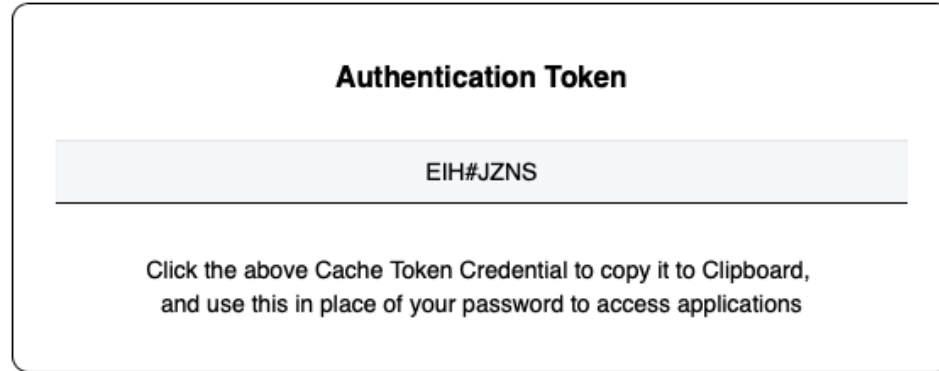
**Password Authentication**

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

# Example derived credential output

---

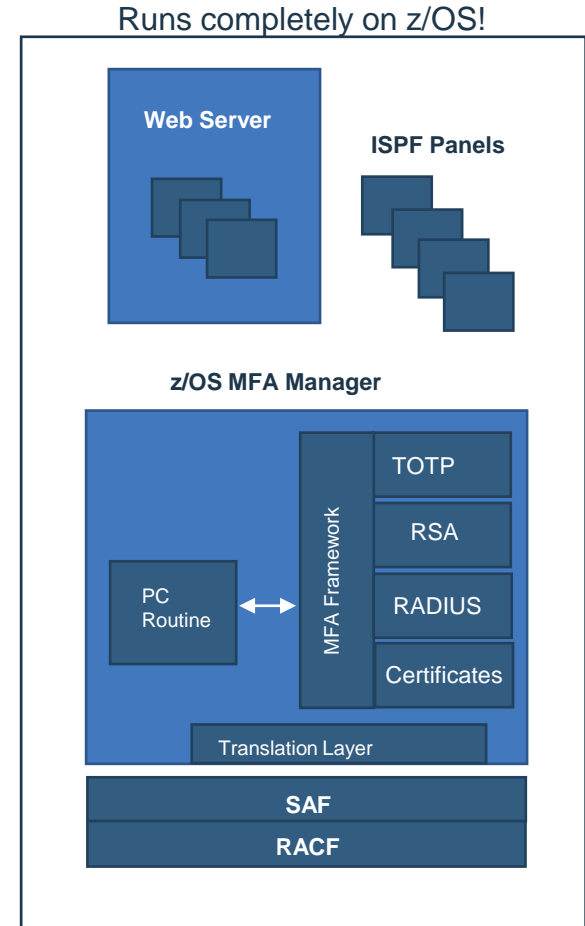
- In this example, an end-user has successfully authenticated to one of their configured **policies**, and the MFA Server has returned a Cache Token Credential (CTC).



- The user will paste the CTC in place of their ESM password when accessing a configured system.
- CTC-Masking is possible (Version 2.2)

# IBM SystemZ Multi-Factor Authentication

- MFA ISPF panels for configuration and management of authentication tokens
- MFA Web Interface
  - User Interface supports factors such as Smart Cards and serves as web interface for registration – depending on factor type
- MFA Manager Services
  - Provides MFA main logic
  - Register MFA Factor Data for a z/OS user
  - Validates a user provided factor against RACF MFA Data
  - Accesses MFA Data via SAF/RACF via callable services





# User Provisioning with RACF

---

- **Activate the MFADEF class:**

```
SETR CLASSACT (MFADEF)
```

- MFADEF Class must be active for MFA authentication processing to occur

- **Define the factor profile:**

```
RDEFINE MFADEF FACTOR.AZFSIDP1
```

- **Add the factor to a RACF user:**

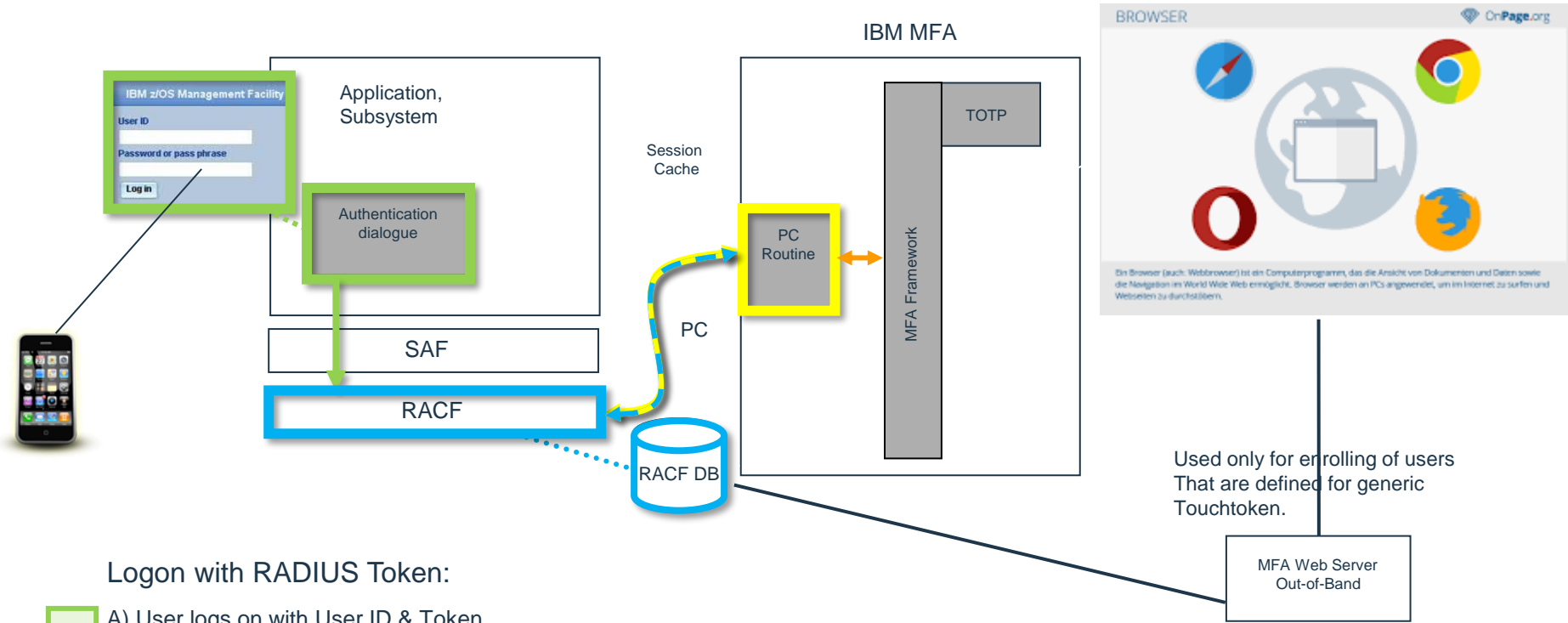
```
ALU JOEUSER MFA (FACTOR (AZFSIDP1) ACTIVE TAGS (SIDUSERID:JOE1)
```

- Adds factor to the user
- Activates the factor – JOEUSER is now required to authenticate to RACF with MFA credentials
- Adds a factor specific tag – SIDUSERID – Associates RSA SecurID user ID with z/OS user ID

- **User is provisioned:**

- JOEUSER must now authenticate to RACF with an RSA SecurID token and PIN

# Architecture Review: Logging on with MFA generic Touchtoken

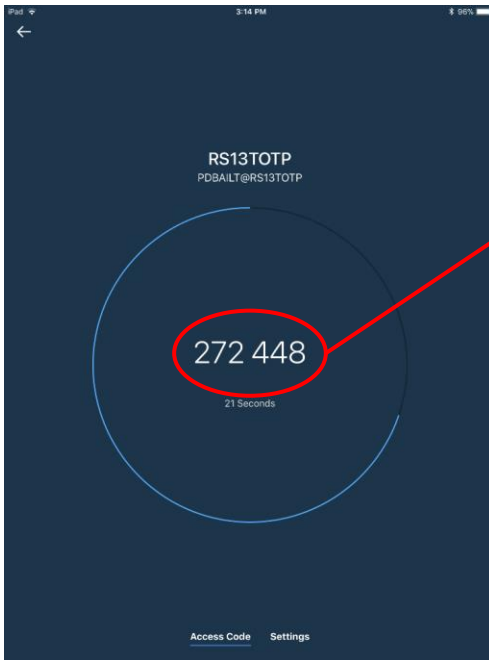


## Logon with RADIUS Token:

- A) User logs on with User ID & Token
- B) RACF determines if the user is an MFA user & calls the IBM MFA
- C) IBM MFA calls RACF to retrieve user's MFA factor details
- D) IBM MFA validates the users authentication factors calls the Authentication Server, gets OK/Fail back
- E) RACF uses IBM MFA status to allow or deny the logon

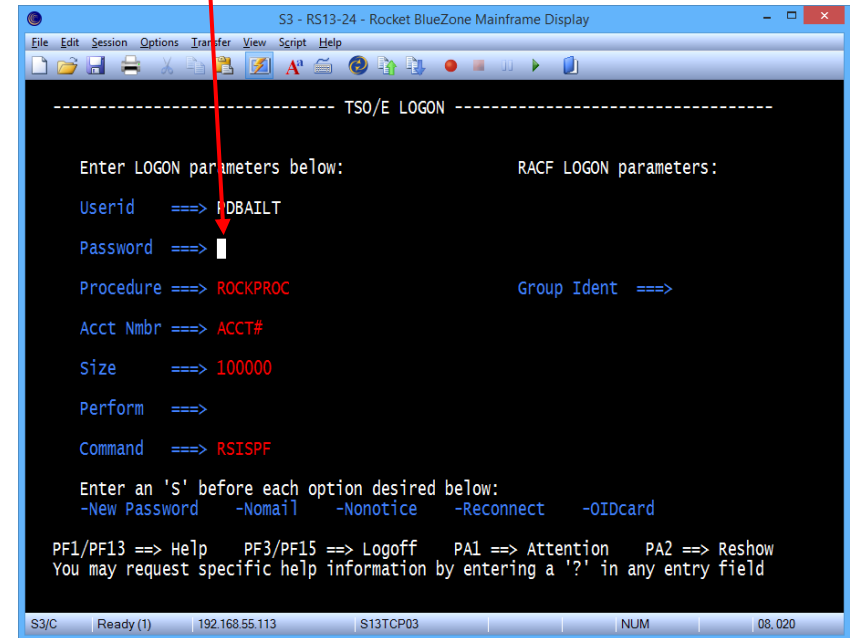


# Example – User log in w/ IBM Verify and RACF password



Password: `passw0rd`  
`272448`

`272448:passw0rd`



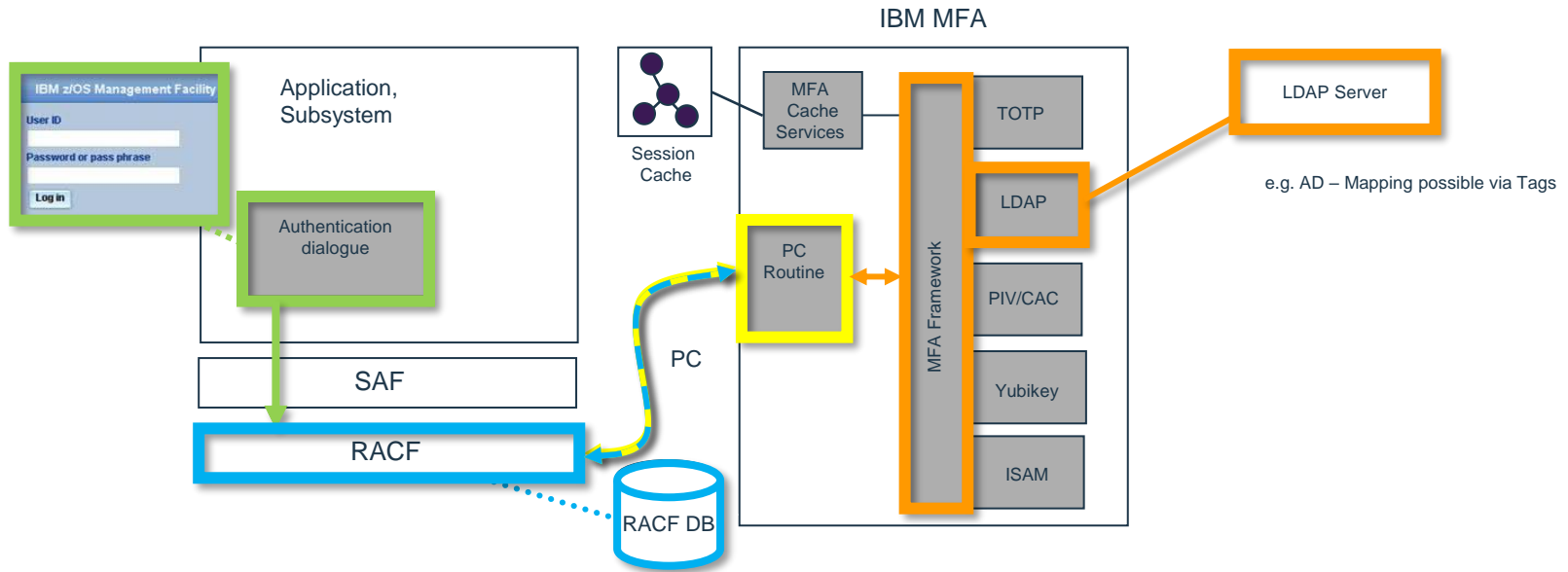
- User authenticates with compound in-band by entering:
  - The IBM Verify token code (or other TOTP App)
  - A colon (configurable separator character)
  - Their RACF password / password phrase
- All together in the password phrase field

# LDAP Simple Bind

---

- **What?:** Factor for authenticating to a variety of LDAP servers, including Microsoft™ Active Directory, using Simple Bind.
- **Value**
  - New factor to leverage an Active Directory password
  - Use AD password with another token via out-of-band support
  - Eliminate home grown tools to sync AD and RACF Passwords

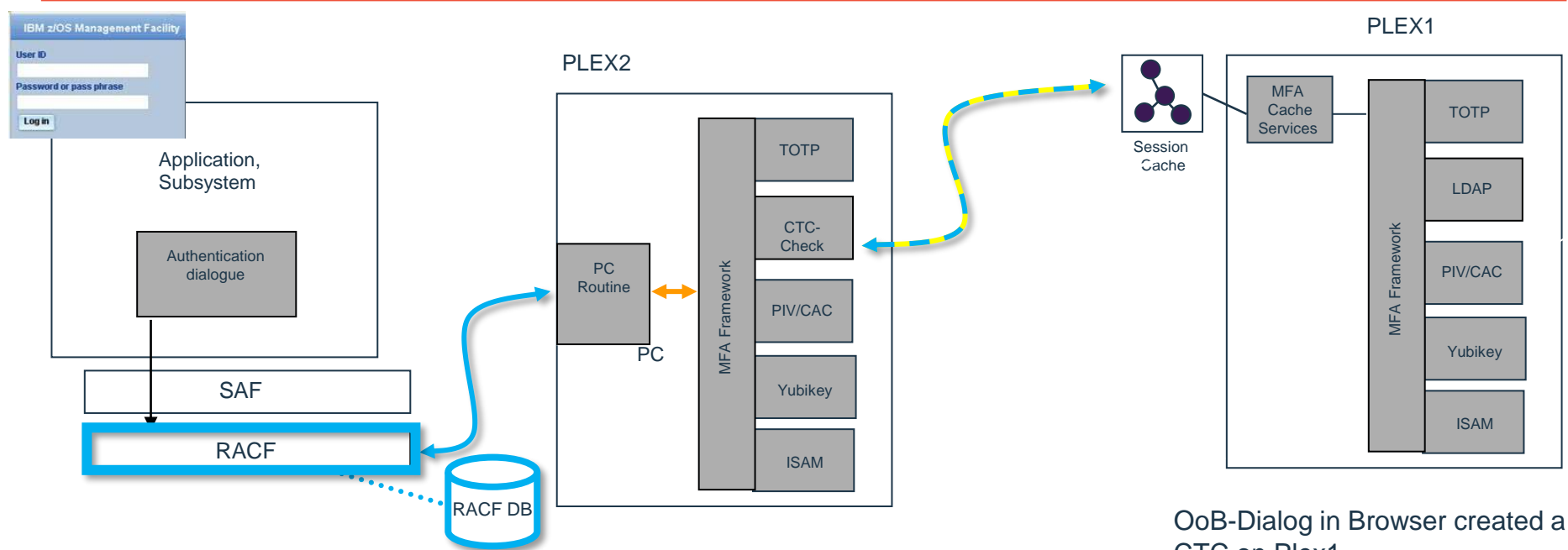
# Architecture Review: Logging on with MFA credentials (LDAP)



## Logon with RADIUS Token:

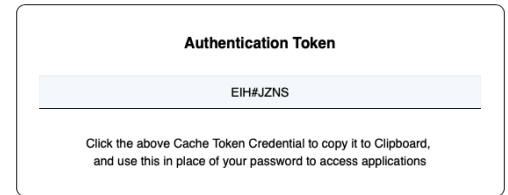
- A) User logs on with User ID & LDAP PW
- B) RACF determines if the user is an MFA user & calls the IBM MFA
- C) IBM MFA calls RACF to retrieve user's MFA factor details
- D) IBM MFA validates the users authentication factors calls the Authentication Server, gets OK/Fail back
- E) RACF uses IBM MFA status to allow or deny the logon

# Architecture Review: Logging on with MFA credentials (Check CTC)



OoB-Dialog in Browser created a CTC on Plex1

CTC on Plex1 can be used for in\_band authentication in Plex2



# New with V2.2 - CTC Invalidation

---

- New console modify command for emergency use
  - In SDSF, for example:  
`/f AZF#IN00,CLEARCTCS <UserID>`
- Works differently depending on the cache mode
- Scoped to the Cache Name used by task that was targeted by the command
- Not available at GA; customers will need to apply an APAR to enable this function

# zMFA can also be used for z/VM

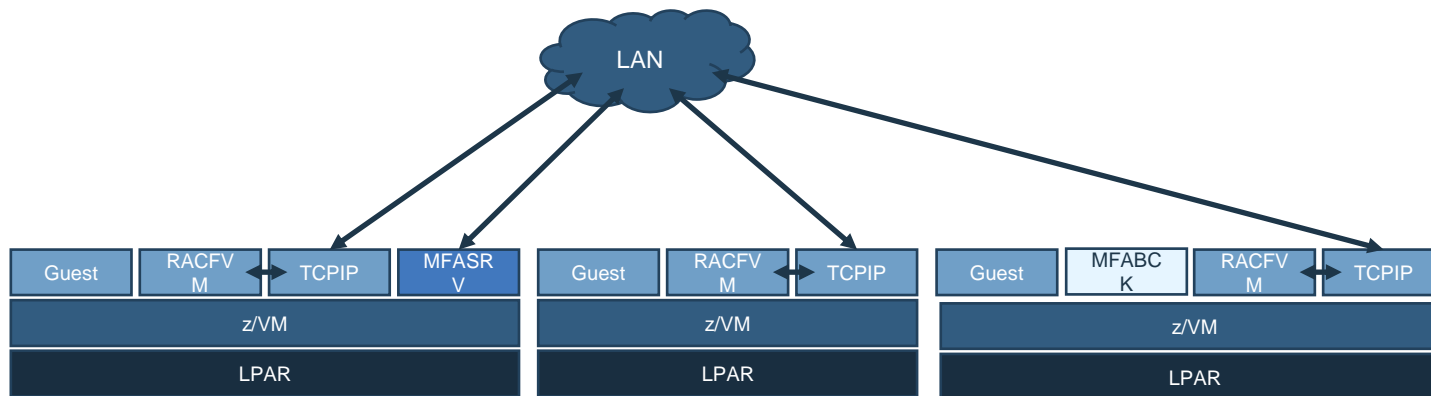
*MFA for z/VM supports the same factors as the **out-of-band** z/OS solution*

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	The SUSE Linux Enterprise Server on IBM Z must be at the following versions: <ul style="list-style-type: none"><li>➤ <b>SLES 15 or later</b></li></ul> The Red Hat Enterprise Linux Server on IBM Z must be at the following versions: <ul style="list-style-type: none"><li>➤ <b>8.x or later</b></li></ul>
Postgres database	For SUSE Linux Enterprise Server on IBM Z: <ul style="list-style-type: none"><li>➤ <b>libpq5</b></li><li>➤ <b>postgresql10-server</b></li></ul> For Red Hat Enterprise Linux Server on IBM Z: <ul style="list-style-type: none"><li>➤ <b>postgresql-server</b></li></ul>
openCryptoki	For SUSE Linux Enterprise Server on IBM Z: <ul style="list-style-type: none"><li>➤ <b>openCryptoki</b></li><li>➤ <b>openCryptoki-64bit</b></li></ul> For Red Hat Enterprise Linux Server on IBM Z: <ul style="list-style-type: none"><li>➤ <b>openCryptoki</b></li><li>➤ <b>opencryptoki-swtok</b></li></ul>
openssl	For SUSE Linux Enterprise Server on IBM Z -- <b>1.1.0</b> For Red Hat Enterprise Linux Server on IBM Z -- <b>1.1.1</b>



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

- MFA for z/VM runs on a Linux on Z guest, you could put the primary and back-up on different LPARs or CECs.



---



# Demo / Fragen ?





# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube.com/user/ibmsecuritysolutions](https://youtube.com/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.