

IBM Z Multi-Factor Authentication

- Let's put security everywhere, starting with your users

Julie Bergh

Americas z Security Technical Lead

jbergh@ibm.com

Joseph Kiss— Brand Technical
Specialist, System Z

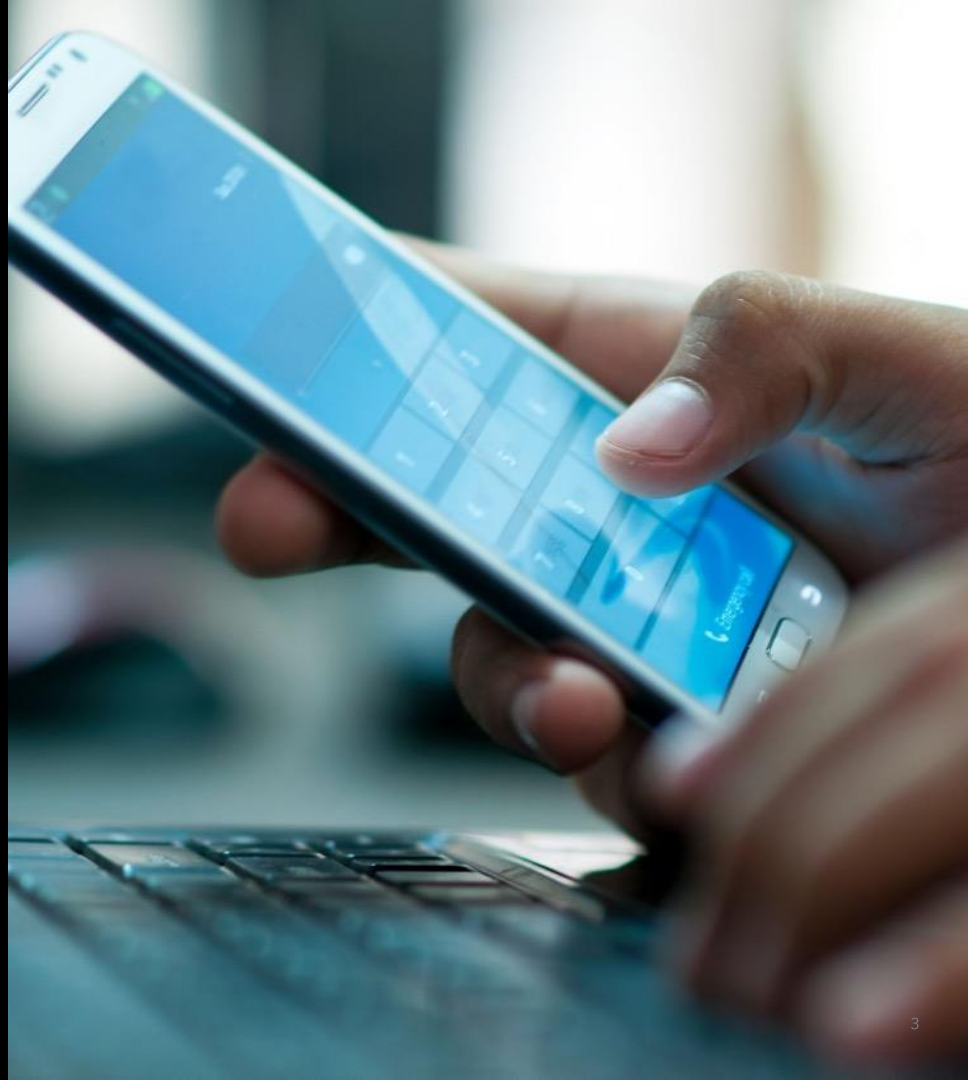
Joseph.Kiss@ibm.com

Agenda

Authentication is the beating heart of security. The most fundamental action in all of IT is to identify “who you are,” and authentication is the building block that answers that question. Now more than ever, businesses and governments across industries—and particularly those in highly regulated spaces—must do everything they can to detect threats to their mission-critical corporate information and applications.

In this session, we will discuss how leading businesses are deploying multi-factor authentication to stop hackers and protect their assets

Why is a multi-factor solution needed on IBM Z?



IBM Z systems are more connected than ever.

This has made them more vulnerable to outside threats.



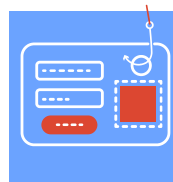
Current Security Landscape



81%

Number of breaches due to stolen and/or weak passwords.¹

(18% worse than prior year)



64%

Number of security incidents that are from insider threats.²



\$3.9 million

The average total cost of a data breach.³



\$8.8 million

The average total cost from **insider-caused** incidents.²



Criminals are identifying key employees at organizations and exploiting them with savvy phishing attacks to gain initial access to the employees' system and steal their account credentials. **This puts emphasis on the need for tighter restrictions on access privileges to key data repositories.¹**

¹ 2017 Verizon Data Breach Investigations Report

² Ponemon: IBM Security 2018 Cost of Insider Threats

³ Ponemon: IBM Security 2019 Cost of Data Breach Study

Compliance, Compliance, Compliance

PCI DSS v3.2

Note: This is a best practice until [January 31, 2018](#), after which it became a requirement



DFS 23 NYCRR 500

Note: Effective March 1, 2017, reporting required as of [February 15, 2018](#)

NIST SP 800-171

Note: This requirement is effective [December 31, 2017](#)



HITRUST 9.3

Note: This requirement is effective [February 20, 2020](#)



Regardless of specific compliance requirements, MFA on IBM Z is a security best practice

How are users authenticating without MFA?

Users authenticate with:

- Passwords
- Password phrases
- Digital Certificates
- via Kerberos

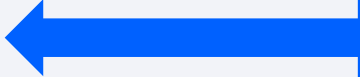
Problems with passwords:

- Common passwords
- Employees are selling their passwords
- Password reuse
- People write down passwords
- Malware
- Key log
- Password cracking



History of Authentication

- **1976:** User identification/verification
- **1981:** Password processing support
- **1984:** DES password encryption option
- **1994:** DES as password default
- **1999:** PROTECTED user IDs
- **2004:** Password enveloping and LDAP change log support
- **2005:** Mixed case passwords and Detect or prevent password recycling
- **2006:** Password phrases from 14 to 100 characters in length
- **2007:** Password phrases from 9 to 13 characters in length
- **2008:** Password phrase exploitation and more granularity on password reset
- **2013:** RACF_ENCRYPTION_ALGORITHM health check (Rolled back)
- **2014:** KDFAES password support, Additional special characters, Password phrase only users
- **2015:** Elimination of the need for an ICHDEX01 exit to eliminate the RACF masking algorithm, ADDUSER will no longer assign a default password, RACLINK support of password phrases
- **2016:** Multifactor Authentication



Majority of mainframe environments are using 35+ year old technology to protect their critical assets!

The majority of known data breaches on the mainframe are linked to a compromised password.



IBM Z Multi-Factor Authentication

Raise the assurance level of critical applications, data, identities and hosting environments



Achieve regulatory compliance and meet best practices (PCI-DSS, DISA-STIG...)

Gain flexibility with support and integration for the broadest array of factors and vendors

Extend IBM RACF with no changes to authenticate users with multiple factors

Fast, flexible, deeply integrated, easy to deploy, manage and use

What is multifactor authentication?

SOMETHING THAT YOU KNOW

- Usernames and passwords
- PIN Code



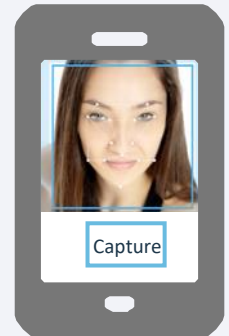
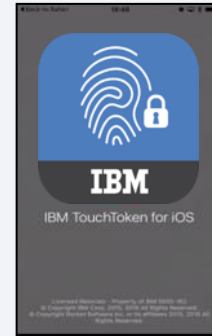
SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
- Time-based



SOMETHING THAT YOU ARE

- Biometrics



What works with IBM Z MFA?

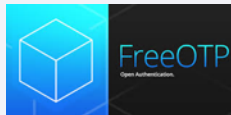
Proprietary Protocol:



RADIUS Based Factors:



TOTP Support:



Certificate Authentication:



Password/Passphrase:

RACF Password/Passphrase can be used in conjunction with all in-band authentication methods.



Target Personas for MFA

Question: Who should be covered with MFA?

Answer: Everyone



Employees that work with personally identifiable info.

- Human Resources
- Healthcare workers
- Law Clerks
- DMV Clerks



Employees that have authority over managing money

- Brokers, Traders, Analysts
- Tellers
- Payroll
- Credit Card Processing



Users that have knowledge of Corporate Intellectual Property

- Executives
- Engineers



Business Partners – that access YOUR data

- Agents – Travel, Insurance
- Contract organization – Outsourcers



Users managing key IT assets

- Systems Programmers
- Security Administrators
- Database Admins, Developers

Target personas for IBM MFA include anyone with access to data a client would *not* want released to the public

RACF Support

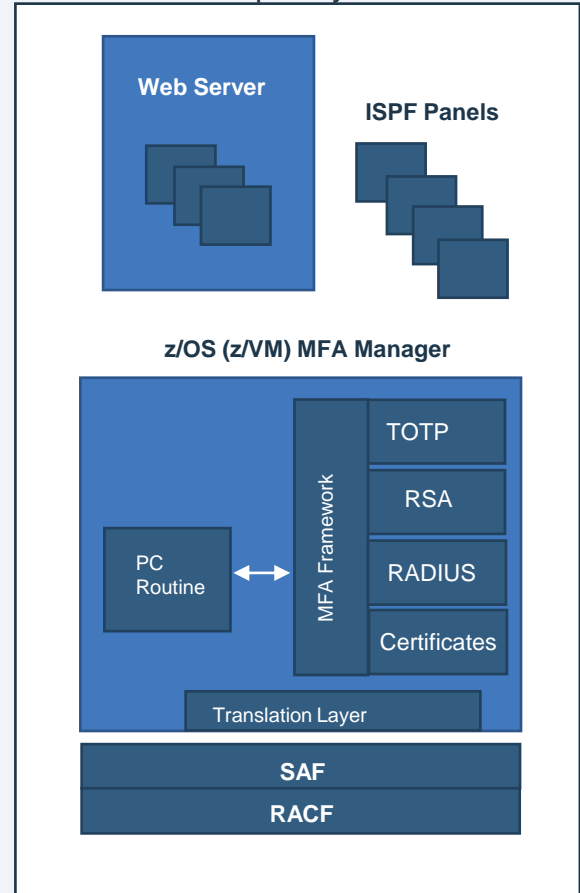
- RACF's MFA support introduces extensions to a variety of components of RACF
 - User related commands
 - Allow the provisioning and definition of the acceptable MFA tokens for a user
 - Extensions to authentication processing
 - Allows supported tokens to be used by any z/OS application
 - Extensions to SAF programming interfaces
 - Provides a new SAF service for IBM MFA allowing access to MFA data stored in the RACF database
 - Auditing extensions
 - Tracks that MFA was used during the authentication process for a given user
 - Utilities
 - RACF Database unload non-sensitive fields added to the RACF database used by MFA processing
 - SMF Unload – unloads additional relocate sections added to SMF records



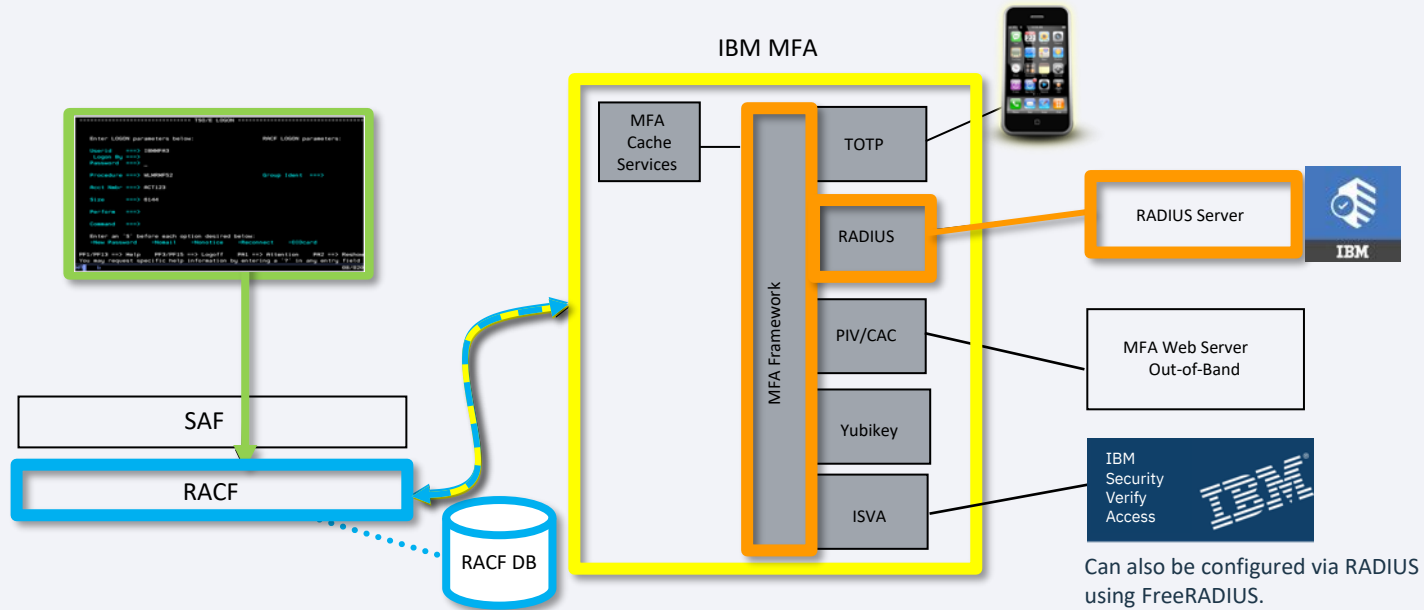
IBM Z Multi-Factor Authentication

- MFA ISPF panels for configuration and management of authentication tokens
- MFA Web Interface: Out-of-Band
 - 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 user ID
 - Validates a user provided factor against RACF MFA Data
 - Accesses MFA Data via SAF/RACF via callable services

Runs completely on IBM Z!!!



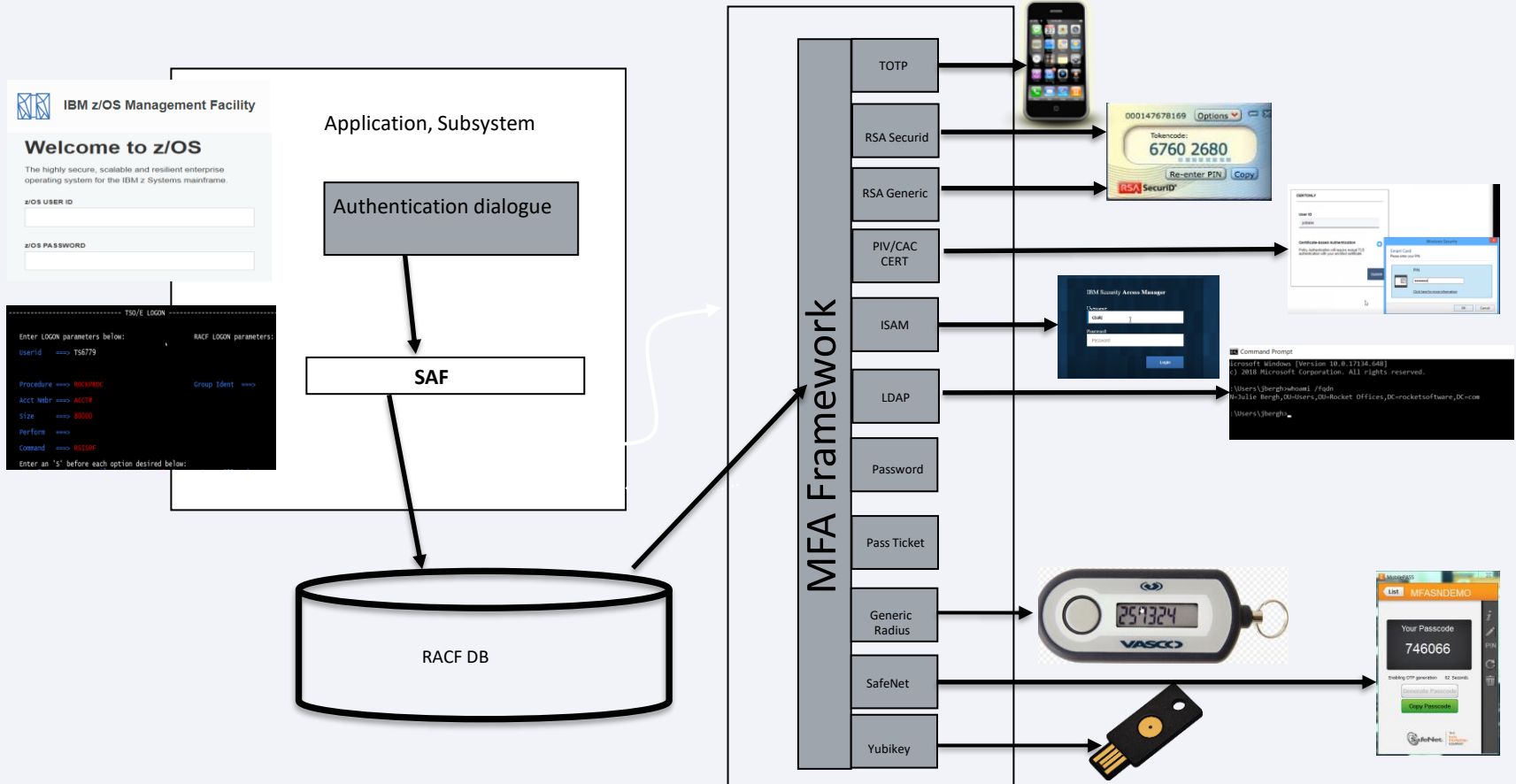
Architecture Review: Logging in with MFA credentials



Logon with RADIUS Token:

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

Logging on with MFA credentials



Example: User logs in w/ IBM Security Verify and RACF password

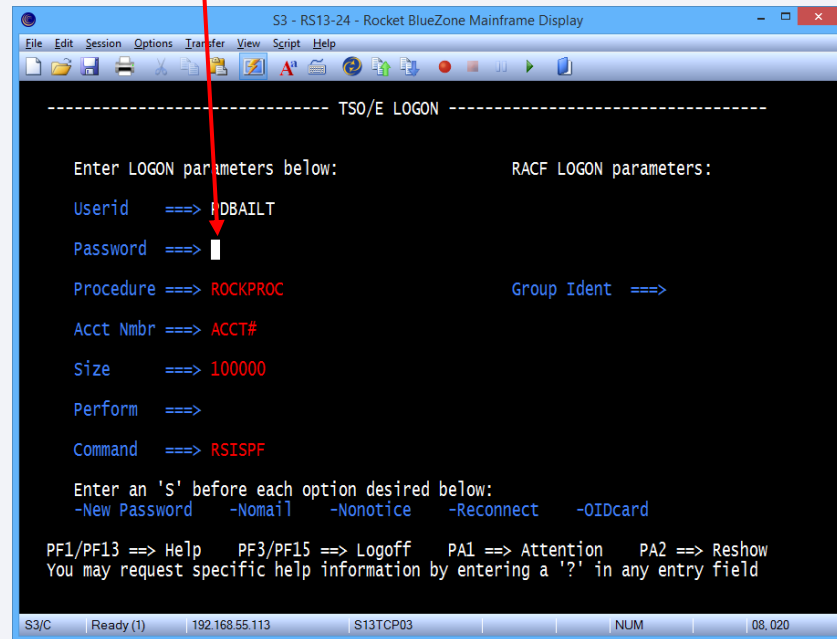


Password: passw0rd

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



User Provisioning with RACF

- Activate the MFADEF class:
 - MFADEF Class must be active for MFA authentication processing to occur

```
SETR CLASSACT(MFADEF)
```

- Define the factor profile:

```
RDEFINE MFADEF FACTOR.AZFSIDP1
```

- Add the factor to the RACF userID:
 - Adds factor to the userID
 - Activates the factor – JOEUSER is now required to authenticate to RACF with MFA credentials
 - Adds a factor specific tad – SIDUSERID – associates RSA SecurID userID with RACF userID

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

- User is provisioned:
 - JOEUSER must now authenticate to RACF with RSA SecurID token and PIN

What if something doesn't work?

Some applications have authentication properties which can prevent MFA from working properly:

- **Length of password field** – Some MFA credentials are longer than 8 characters
- **Replaying of passwords** – MFA credentials are one time use

IBM Z MFA was architected with this in mind and provides a variety of accommodation mechanisms.

1. Selective Application Exclusion

- Exempting MFA processing for certain applications:
 - Allows a Security Administrator to mark certain applications as excluded from MFA
 - Allows a user to logon to that application using their non-MFA credentials

2. PassTicket Support

- Allows the Security Administrator to indicate that an MFA user can authenticate with a PassTicket instead of an ACTIVE MFA factor. New special MFA PassTicket Factor

3. Out-of-Band Support

- Allows users to authenticate with multiple factors directly to IBM MFA and receive a logon token
- The pre-authentication logon tokens behavior can be customized as needed
 - Controls to allow tokens to be single use or re-useable and how long a token is valid

Session Managers

Provides a nice single sign-on experience on the mainframe

- Session Manager needs to be configured to work with PassTickets
- User logs on to the Session Manager with MFA credentials
- Subsequent calls to other applications, Session Manager will generate a PassTicket to authenticate
- Requires an additional factor for the user: AZFPTKT1

NOTE: Session Manager must support PassTickets

What's new in IBM MFA thru the years

- ISAM Integration (ISAM pick up OTP, CIV Integration via RADIUS)
- Native Yubikey
- LDAP Simple Bind
- Policy First Update
- JWT Support
- Out of Band - National Language Support & Customization
- Self-Service Password Change

New Operating System – z/VM

- In addition to z/OS we now support z/VM
- Leverages Out-of-Band channel
- Most factors that are supported on z/OS will work on z/VM
- **One Solution – One License**
- Innovative Packaging
 - Order via ShopZ, get both operating systems
 - Pick and choose which one to install

Why is this important?

- z/VM is not exempt from MFA requirements
- IBM is the only vendor who can support both z/OS and z/VM with the same solution
- One vendor is more desirable
- Leverage existing MFA infrastructure

Protection beyond the z/OS Sysplex Boundary

- Support the production of secure credentials that can be used both within and beyond the boundary of the sysplex where the credential was generated.
- New factor AZFCKCTC

Why is this important?

- Most clients will be interested in cross sysplex support
- Simplifies MFA configurations in large environments

New Operating System – Linux on Z

- In addition to z/OS and z/VM we now support Linux on Z
- Supported on Red Hat and SUSE Linux Enterprise Server (SLES)
- Use MFA web services to present an in-band authentication flow to PAM-enabled applications for Linux
- Enabled on a per-application basis by editing the PAM configuration
- **One Solution – One License**
- Innovative Packaging
 - Order via ShopZ, get all three operating systems
 - Pick and choose which one to install

Why is this important?

- Linux on Z is not exempt from MFA requirements
- IBM is the only vendor who can support both z/OS, z/VM and Linux on Z with the same solution
- One vendor is more desirable
- Leverages existing MFA infrastructure

Multiple Factor Instances (z/OS only)

- Support for multiple instances of certain factors
 - Eg. Multiple, different, RADIUS factors
- 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)

Why is this important?

- For service providers or other customers with segmented user populations
- Different user populations supported by the same RACF database can authentication against distinct RADIUS servers

New Factor for RSA REST API (z/OS and Linux on Z)

- Recent RSA Authentication Manager servers (8.2 or later) support an HTTPS API called the SecurID Authentication API
- Three methods for provisioning RSA
 - AZFSIDP1 - proprietary UDP protocol
 - AZFSIDR1 - RADIUS
 - AZFSIDP3 - New REST API
- For new customers that already use RSA SecurID, recommend they start here

Why is this important?

- Superior ease of configuration
- From a crypto perspective, this offers strong and industry-standard security for user credentials

Policy Authentication Web Interfaces (z/OS and Linux on Z)

- Provides formal support and documentation for the MFA Web Interface APIs
- Fully documented in Appendix C (Installation and Customization Guide)

Why is this important?

- Allows you to write applications to interface with MFA Web Services
- Ability to provide custom interfaces

Certificate Auto-approval (z/OS only)

- New configuration setting
- This setting has three options:
 - N – for “Never”, default, require admin approval
 - E – for “ESM”
 - Uses InitACEE to test for a pre-existing mapping that confirms a match between the presented X.509 certificate and the enrolling User ID
 - If a match is confirmed, the enrollment is auto-approved
 - A – for “Always”
 - A user who successfully completes self-service enrollment (by providing a trusted certificate and a correct User ID / Password combination) is immediately placed into REGSTATE:APPROVED.

Why is this important?

- For large scaled deployments at customers using certificates
- Reduces administrator overhead (avoid approval step)

New CTC Features

1. CTC Masking (z/OS and Linux on Z)

- When enabled in STC settings, changes the end-user display so that the CTC value is initially hidden (but easily copied or revealed if needed)
- Previously CTC was displayed in clear text (default behavior)

2. Invalidate CTC (z/OS only)

- 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 APAR PH43579 when available

Why is this important?

- Reduces the chance of a CTC being compromised
- Improved security; provides a mechanism to remove all CTC's to reduce a potential threat

Factor/Instance Statistics Collection (z/OS only)

- New console modify command for diagnostic purposes
- In SDSF, for example:
 - /f AZF#IN00,PLUGSTATS <factorName>
 - /f AZF#IN00,PLUGSTATS <factorInstanceName>
 - /f AZF#IN00,PLUGSTATS *ALL*
- Currently only logs details to SYSPRINT when the STC is running at trace level 3
- A foundation for future work

Why is this important?

- Better diagnostic data

IBM Z MFA Support in zSecure

zSecure Admin and Audit

- Selection and display of MFA fields in RACF profiles. Extra fields and formatting added for easier display.
- Selection and display of new relocate section and MFA information in SMF records.
- New field available in SYSTEM report about presence of RACF MFA support.

zSecure Access Monitor

- Detection and reporting of use of MFA for every RACINIT, including TSO logon.

zSecure Command Verifier

- Support for parsing new command syntax.
- New Policy Profiles to control management of MFA information, and updates to command recording in Command Audit Trail.

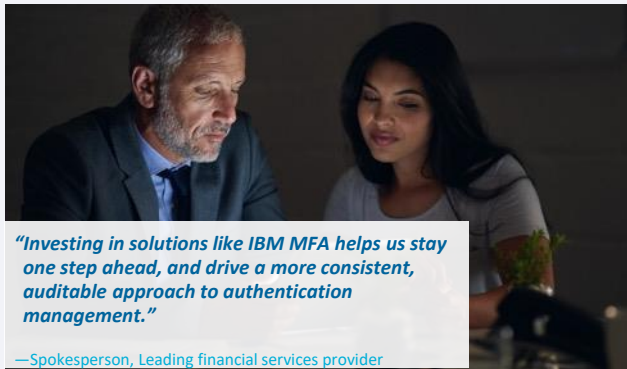
zSecure Adapters for SIEM

- Include MFA information to QRadar for analytics

zSecure Visual

- User context menu extensions for MFA factors and policies; MFPOLICY edit

Reference Material - Banking



Business challenge

Given that a single security breach can cost USD 4 million on average, isn't it time to stop relying on passwords alone? This financial services firm sought a better way to keep key systems protected.

Transformation

When clients put their financial future in your hands, security has to be one of your top priorities. This financial services provider uses IBM® Z Multi-Factor Authentication to reduce the risk of unauthorized access to sensitive data and systems, helping protect the company from costly and damaging security breaches.

Business benefits:

Helps

ensure that only authorized users have access to key data and systems

Reduces

risk of costly and reputation-damaging security breaches

Simplifies

authentication management to save IT teams time and effort

Leading financial services provider

Building a stronger line of defense against security threats with multi-factor authentication

This financial services firm provides solutions and services to meet the needs of institutional investors, including investment servicing, investment management, and investment research and trading. It manages trillions of dollars in assets for clients all over the world.

Solution components

- IBM® Z Multi-Factor Authentication

IBM Security Community

An online digital platform to support all aspects of community

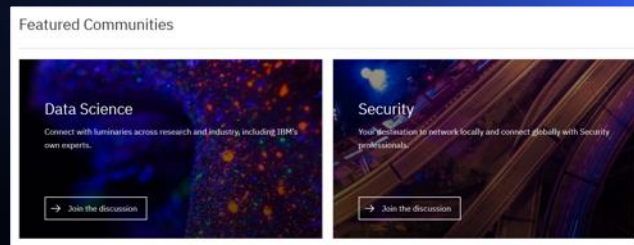


Learn: Come to one place where IBM Security customers, experts, teams and a broader audience converge to share, solve, synergize

Network: Connect with the IBM Security ecosystem through engagement, education & the championing of users and their work

Share: Get equipped to solve business challenges today to deliver tomorrow's business outcomes.

4,000+ Members Strong!



community.ibm.com/security

Questions?



Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://www.youtube.com/user/ibmsecuritysolutions)

<https://www.ibm.com/security/mainframe-security/zsecure>

<https://www.ibm.com/us-en/marketplace/ibm-multifactor-authentication-for-zos>

<https://community.ibm.com/community/user/security/communities/zsecurity>

<https://www.ibm.com/security/mainframe-security/zsecure>

IBM Security

© Copyright IBM Corporation 2019. 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.



