SHARE San Jose 2017

RACF Update: Multi-Factor Authentication is Here!

Ross Cooper, CISSP®
IBM Corporation

March 9, 2017
Session: 20369

#SHAREsjc

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

SHARE
EDUCATE • NETWORK • INFLUENCE

RACF & MFA Update

- **Read Only Auditor** - New type of auditor that can look but not change settings.
- **Granular Digital Certificate Authority** - New more granular digital certificate authority checking option.
- **Unix Search Authority** - Allows an administrator to search/list UNIX files regardless of individual directory settings.
- **FSEXEC** – Restricting UNIX execute access
- **New and Updated RACF Heath Checks**
- **Remote Sharing Enhancements:**
  - RRSF Dynamic Main Switch - Allows switching the RRSF main node
  - Unidirectional Connection - Deny In Bound support
  - RACF Remote Sharing Configuration Information API
- **Password Enhancements:**
  - New Special Characters Support
  - Phrase Only Users
  - Expire without setting password
  - New Encryption Algorithm Option – **KDFAES**
- **RACF 2.3 Preview**
- **Multi-Factor Authentication –** Require multiple factors during RACF authentication

RACF Update

Read Only Auditor

- **User with the AUDITOR Attribute:**
  - Can audit a RACF controlled system by viewing **RACF profiles** and **SETROPTS** settings.
  - Can **control** the logging of detected accesses to any RACF protected resources during RACF authorization checking and accesses to the RACF database.

- **User with the Read Only Auditor – ROAUDIT attribute:**
  - Can list RACF profiles and other security settings:
    Commands: LISTDSD, LISTGRP, LISTUSER, RLIST, SETROPTS LIST, SEARCH
    UNIX: ck_access honors ROAUDIT
    Utilities: DSMON, IRRUT100, IRRXUTIL
  - Can NOT control logging settings
  - RACF list commands and utilities are updated to permit users with **ROAUDIT** the same ability to list information that would be allowed to users with **AUDITOR**.

- Allows installations to create users that can view system information but not alter any system controls.
  - Suitable for use by an external auditor who may need to verify the current security state of a system – allows that user to view system information but does not unintentionally grant the user the ability to change (or sabotage) system settings.

Granular Certificate Administration

- **New RACDCERT Granular Administration:**
  - Provide RACDCERT granular control based on owner, certificate label, key ring name, and function
  - Enables the customers to segregate RACDCERT authorities among the administrators
  - Enforce a naming convention for naming the certificates and keyrings

- **Existing Digital Certificate RACDCERT authority checking:**
  - **IRR.DIGTCERT.<function>** profiles in **FACILITY** class
  - **<ring owner>.<ring name>.UPD** profiles in **RDATALIB** class (R_DataLib Only)

- **New controls to protect certificates:**
  - Access to certificates can be controlled by **RDATALIB** Profiles:

  IRR.DIGTCERT.<cert owner>.<cert label>.LST/UPD.<function>

- **RACF RACDCERT can now check RDATALIB profiles:**
  - Enabled by defining the **IRR.RACDCERT.GRANULAR** profile in the **RDATALIB** class

UNIX Search Authority

- **UNIX Security Administration:**
  - z/OS UNIX defines a set of **UNIXPRIV** class profiles to manage various UNIX privileges:
    SUPERUSER.FILESYS.CHANGEPERMS – Change file permissions
    SUPERUSER.FILESYS.CHOWN - Change file owners
  - These privileges lack the ability to read or search directories.
  - In order to search directories, the administrator must be granted one of:
    - Search authority to containing directories
    - RACF **AUDITOR** attribute
    - **BPX.SUPERUSER** in **FACILITY** Class / UID 0

- **New V2R2 UNIX Search Authority:**
  - Allow for directory read / search authorization to be granted via a new RACF profile:
    SUPERUSER.FILESYS.DIRSRCH - Allows a user to read and search all directories, without the authority to open other files.

Restricting UNIX Execute Access

- **Mark a z/OS File System as non-executable:**
  - Prevent unintentional execution of files in a shared file system such as **/tmp**

- **New FSEXEC Class:**
  - Prevent users from executing any file in a z/OS File System (zFS) file system or Temporary File System (TFS).
  - Can allow selected users and groups to remain eligible for execute access.
  - Supports an improved audit posture by enabling the RACF administrator to demonstrate a single point of control for restricting execute access to one or more file systems that might contain authorized code, or code of unknown origin.

- **Examples:**

```
RDEFINE FSEXEC /tmp UACC(NONE)
RDEFINE FSEXEC OMVS.ZFS.ADMIN.** UACC(NONE)
PERMIT OMFS.ZFS.ADMIN.** CLASS(FSEXEC) ID(FRED) ACC(UPDATE)
SETR RACLIST(FSEXEC) REFRESH
```

New and Updated Health Checks

- **ICSF Checks:**
  - **RACF_CSFKEYS_ACTIVE**
  - **RACF_CSFSERV_ACTIVE**
- **JES Checks:**
  - **RACF_JESJOBS_ACTIVE**
  - **RACF_JESSPOOL_ACTIVE**
  - **RACF_BATCHALLRACF**
    - Raise an exception if SETROPTS JES(BATCHALLRACF)) is not in effect
- **RACF_PASSWORD_CONTROLS**
  - Examines basic password controls
    - Mixed case passwords enabled
    - Number of consecutive logon attempts setting within recommended parameters (3)
    - A password/phrase can be valid for more than (90) days.
  - Clients can modify the IBM recommendation with a health check parameter
- **RACF_ENCRYPTION_ALGORITHM**
  - Examines the return code from the RACF encryption exit (ICHDEX01) exit for authentication and raises an exception:
    - V1R12, V1R13 & V2R1 - Anything other than DES is in use
    - V2R2 – Anything other than KDFAES is in use

New and Updated Health Checks

- **RACF_SENSITIVE_RESOURCES**
  - Reports on the protection status of ICSF TKDS, PKDS, and CKDS data sets
    - Check can be set INACTIVE when ICSF is not in use
  - Reports on the protection status of the RACF remote sharing (RRSF) work data sets
    - SYS1.MVSX.INMSG
    - SYS1.MVSX.OUTMSG
  - Report on the protection status of additional z/OS UNIX resources
    - **FACILITY class:**
      - BPX.POE
      - BPX.JOBNAME
      - BPX.FILEATTR.SHARELIB
      - BPX.SMF
      - BPX.STOR.SWAP
      - BPX.UNLIMITED.OUTPUT
    - **UNIXPRIV class:**
      - SUPERUSER.FILESYS.QUIESCE
      - SUPERUSER.FILESYS.PFSCTL
      - SUPERUSER.FILESYS.VREGISTER
      - SUPERUSER.IPC.RMID
      - SUPERUSER.SETPRIORITY
    - **SURROGAT class:**
      - BPX.SRV.<userid>

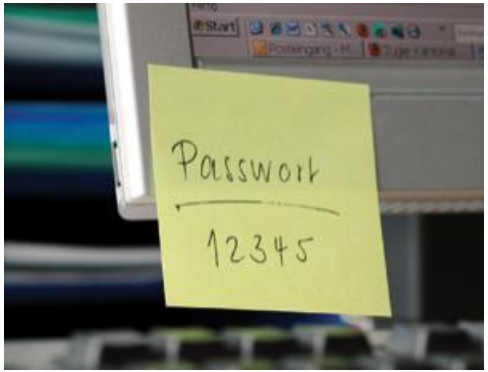
Remote Sharing Enhancements

- **RRSF – Synchronize database updates to separate RACF Databases.**

- **Updates:**
- **RRSF Unidirectional Nodes**
  - Ability to define a remote RRSF node which is not allowed to make updates
- **RRSF Dynamic Main Node Switch**
  - Ability to switch the RRSF Main Node
- **RRSF Configuration Information API**
  - Retrieve RRSF network configuration information programatically
  - R_Admin and IRRXUTIL

Password Enhancements (R13 & Up)

- **Available via APAR: OA43999**
- **RACF Password Special Characters**
  - Additional characters now supported for passwords
- **Password Phrase only users**
  - Ability to have a password phrase without a password



- **Expire a password without setting a new password**
  - Ability to expire a password without having to set a new password
- **New Password Encryption option**
  - Optionally encrypt / hash the password and password phrase using a new more modern algorithm - **KDFAES**

V2R2 Only Password Enhancements

- **Removal of Default Passwords:**
  - Removal of Default Group as Default password:
    - **ADDUSER** will not assign a default password

      `ADDUSER JOE TSO(…) OMFS(…)`

      Results in: `ICH01024I User JOE is defined as PROTECTED.`
    - **ALTUSER** and **PASSWORD** can not set a default password

- **RACLINK DEFINE(node.user/password):**
  - Support password phrases

- **ICHDEX01 Password Processing exit:**
  - Not needed unless implementing your own password encryption
  - Absence of ICHDEX01 will default to DES only

IRRDBU00: Require only READ authority

- Since its inception, IRRDBU00 has required UPDATE authority to the RACF data set(s) which are used as input
- With V2.2, if you specify PARM=NOLOCKINPUT, only READ authority is required
- Eliminates the need to use the “trick” of specifying LABEL=(,,,IN) on the input DD statement

Policy Driven Encryption

- **IBM US Software Announcement 216-392, 4 October 2016**
- "IBM plans to deliver application transparent, policy-controlled dataset encryption in IBM z/OS. IBM DB2 for z/OS and IBM Information Management System (IMS) intend to exploit z/OS dataset encryption."
- Policy is defined by the specification of an ICSF key label in **RACF data set profile**, **DATACLAS** definition, or **JCL**
- z/OS DFSMS encrypts/decrypts records via CPACF when written-to or read-from disk
  - Centralized changes enable multiple dataset types (BSAM/QSAM/VSAM/zFS/hsm/dss)
  - In-memory system or application data buffers will not be encrypted

IBM Statement of Direction:
IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

RACF 2.3 Preview - RFA

- **IBM UID(0) consistent mapping:**
  - Multiple users can have UID(0) - SUPERUSER(x) keyword of BPXPRMxx will be used
  - UNIX ls – l command
- **Field Level Access Checking (FLAC) Granularity:**
  - FLAC can grant authority to modify select fields in non-base segments.
  - Previously FLAC authority allows update of the granted field for any profile.
  - Now, FLAC authority can be scoped to only profiles that the command issuer can modify the base segment.
- **E-mail Address:**
  - New e-mail field in the user base segment
  - Allows applications to map between UserID and e-mail field and send notifications

Multi-Factor Authentication

Current Security Landscape

1,429

Number of security incidents in 2015 with confirmed data disclosure as a result of stolen credentials.[1]

63%

Number of breaches due to weak, default or stolen passwords.[1]

$4 million

The average total cost of a data breach.[2]

60%

Number of security incidents that are from insider threats. [3]

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] 2016 Verizon Data Breach Investigations Report
[2] Ponemon: 2016 Cost of Data Breach Study: Global Analysis
[3] IBM X-Force 2016 Cyber Security Intelligence Index

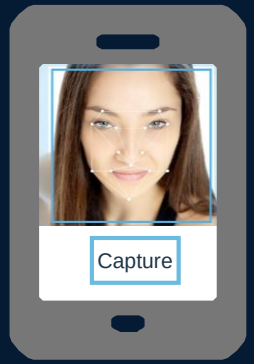
User Authentication Today on z/OS

- Users can authenticate with:
  - Passwords
  - Password phrases
  - Digital Certificates
  - via Kerberos

- Problems with passwords:
  - Common passwords
  - Password reuse
  - People write down passwords
  - Malware
  - Key log
  - Password cracking

Authentication is a journey

Moving to stronger, easier authentication



SOMETHING THAT YOU KNOW
- Usernames and passwords
- PIN Code
- Knowledge questions

SOMETHING THAT YOU HAVE
- ID Badge
- One time passwords
  - Time-based
  - Email / SMS

SOMETHING THAT YOU ARE
- Biometrics

IBM Multi-Factor Authentication for z/OS

Higher assurance authentication for IBM z/OS systems that use RACF

IBM Multi-Factor Authentication on z/OS provides a way to **raise the assurance level** of z/OS, applications, and hosting environments by extending RACF to authenticate users with multiple factors.

- Support for third-party authentication systems
  - RSA® Ready supporting RSA SecurID® Tokens (hardware & software based)
  - IBM TouchToken – Timed One Time use Password (TOTP) generator token
  - PIV/CAC and Smart cards – Commonly used to authenticate in Public Sector enterprises
- Tightly integrated with SAF & RACF

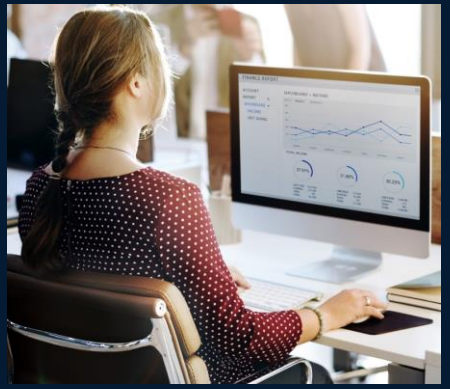
TECHNOLOGY RSA READY PARTNER

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

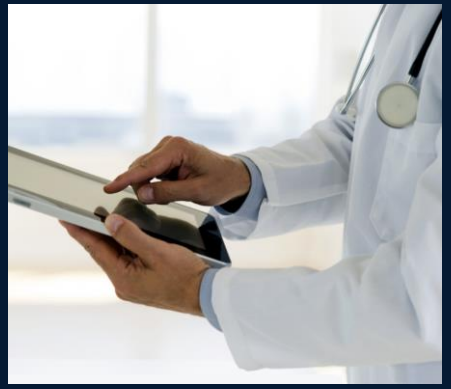
PCI-DSS
Achieve regulatory compliance, reduce risk to critical applications and data

Architecture supports multiple third-party authentication systems at the same time

Use cases



System Administrator with access to sensitive data sets



Privileged User with access to patient health records

RACF Administrator who controls system-wide authorization

Support **PCI-DSS Requirements** for personnel with non-console admin access to card data

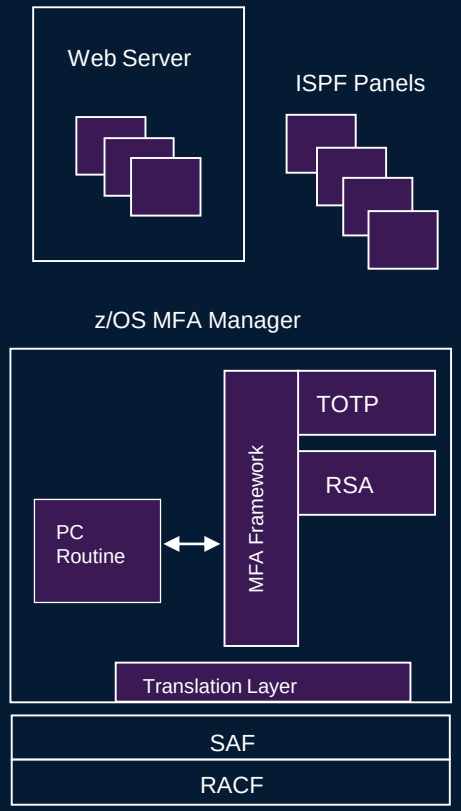
IBM MFA as an additional tier of defense to help ensure that only highly authenticated users can access the system

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 Multi-Factor Authentication for z/OS

- MFA Manager Web Interface
  - User Interface – supports factors such as smartphone apps and serves as web interface for registration – depending on factor type
- MFA ISPF panels for management of authentication tokens
- 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
  - Common MFA processing
- Translation Layer
  - Allows MFA components to invoke RACF callable services
    - "Wrap" SAF/RACF database access APIs



RACF User Provisioning for MFA

- **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:**

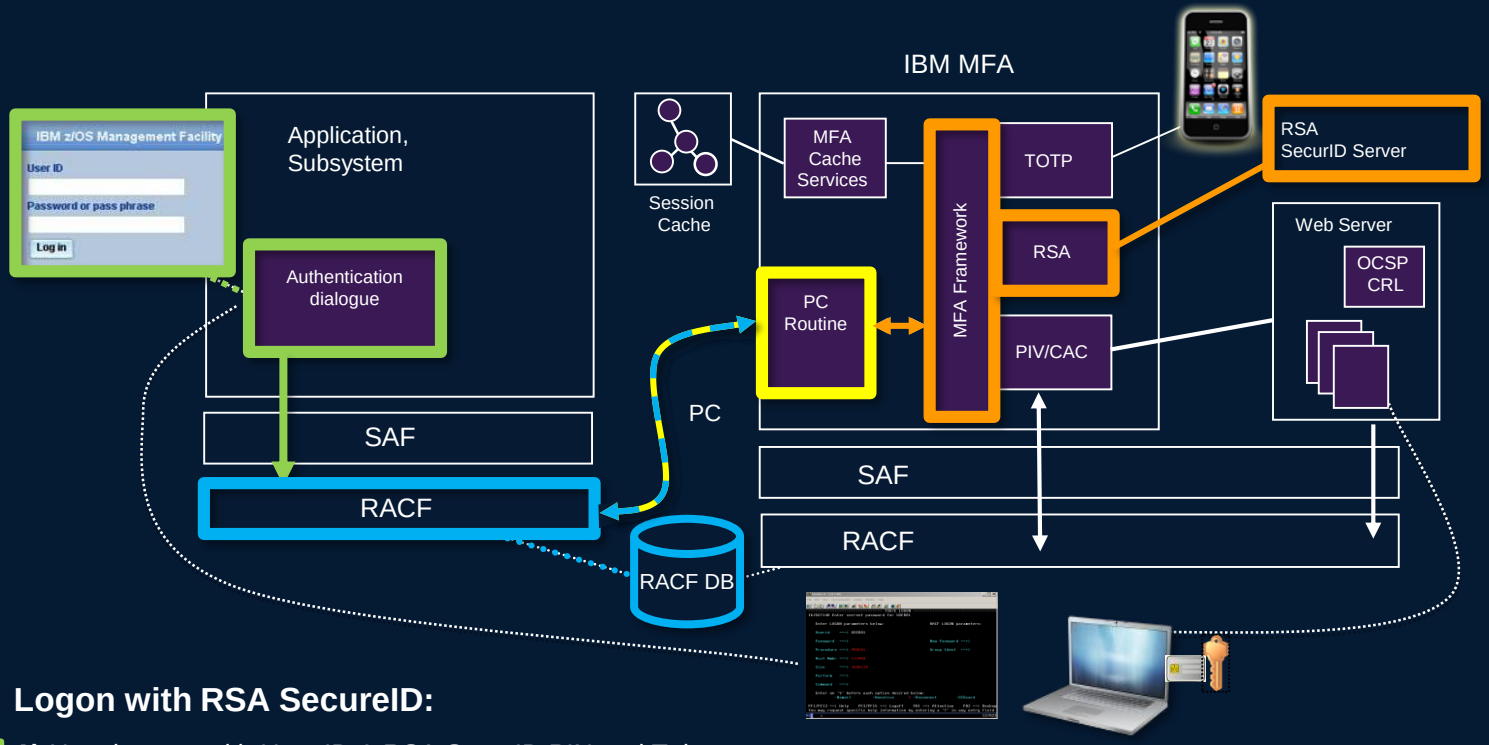
```
ALU JOEUSER MFA(FACTOR(AZFSIDP1) ACTIVE TAGS(SIDUSERID:JOE1) PWFALLBACK)
```

  - 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
  - Password fallback – When MFA is unavailable, the user can logon with their password / phrase

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

RSA SecureID Tokens Support

- Requires RSA SecurID server configured to the MFA Server
- Since the use of RSA SecurID requires an external configured server instance – this could represent a point of failure
- Supports both hard and soft RSA SecurID tokens



Logon with RSA SecureID:

- **A)** User logs on with User ID & RSA SecurID PIN and 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 RSA Server, gets OK/Fail back from RSA
- **E)** RACF uses IBM MFA status to allow or deny the logon

Using Soft RSA SecureID Tokens

- RSA SecureID PIN code is entered into the RSA Soft Token generator
- User enters their User ID and token generated code in the password field

Something you know: RSA PIN Code

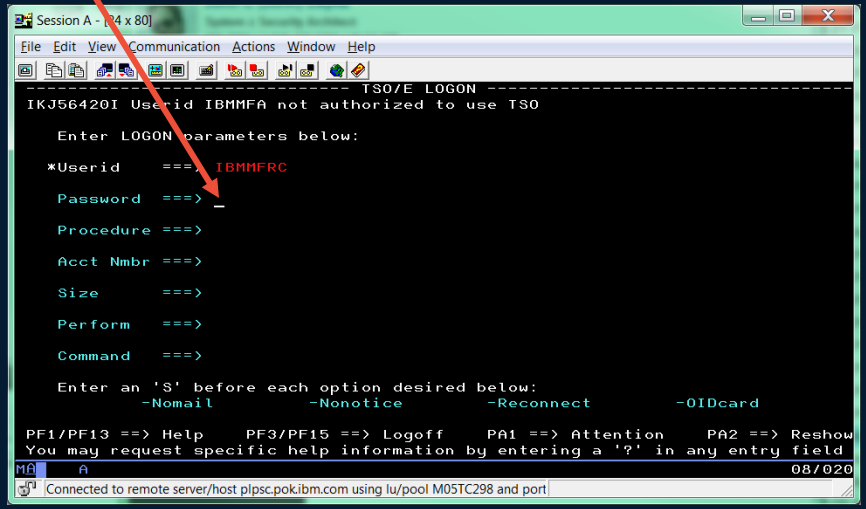
Something you have: RSA Token Generator

Using Hard RSA SecurID Tokens

Pin Code: **1234**

159759

1234159759



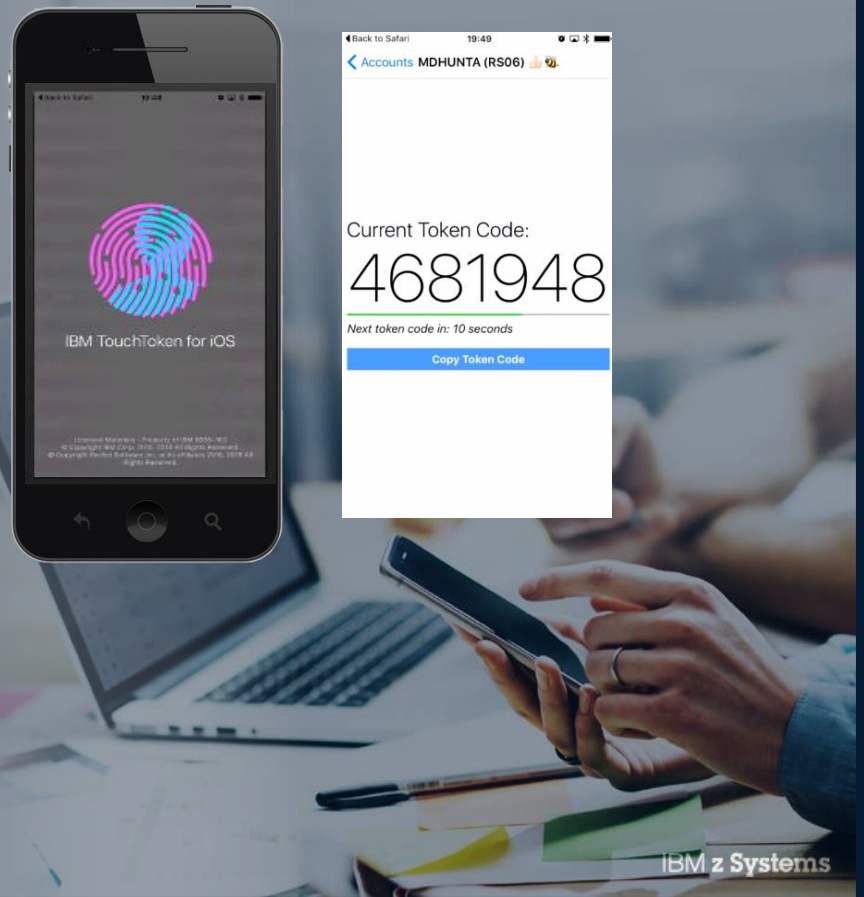
Something you know: RSA PIN Code

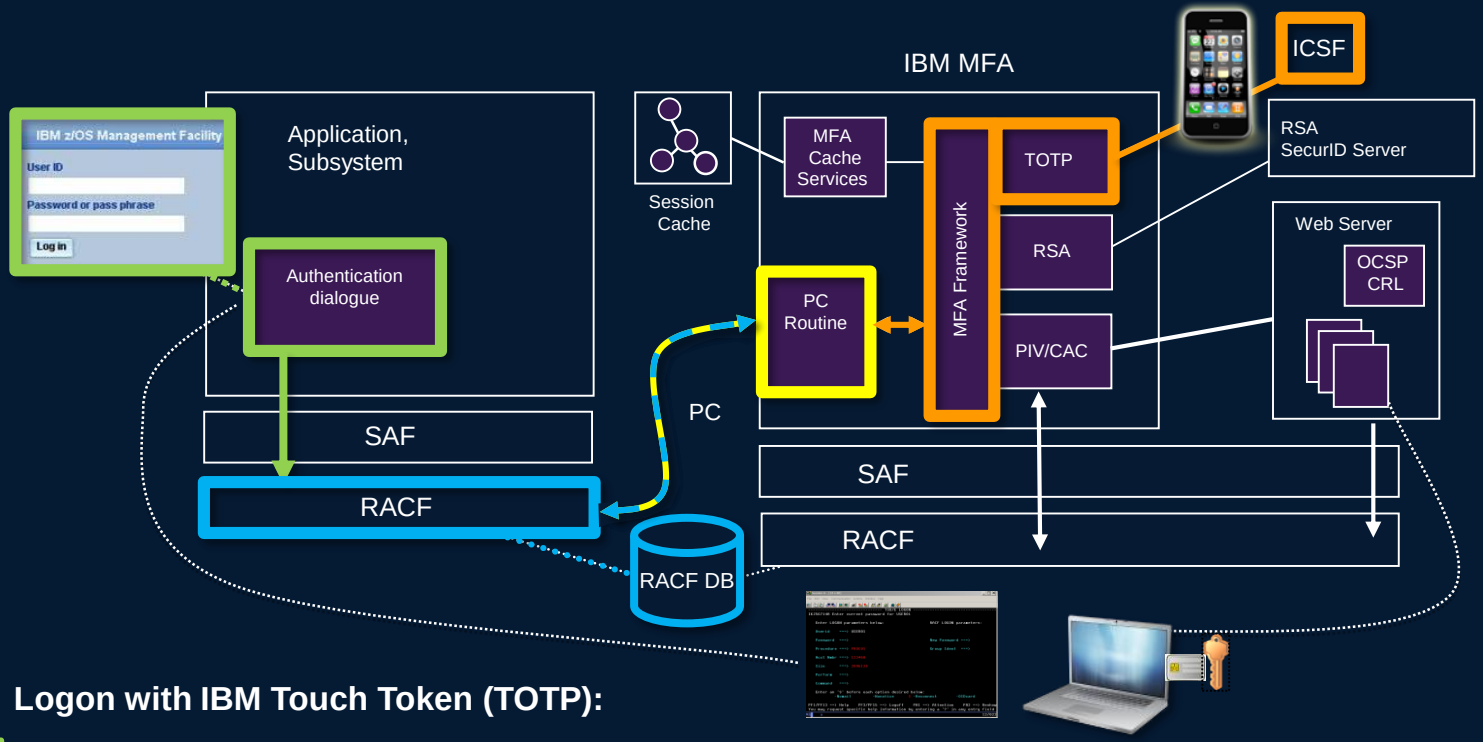
Something you have: RSA SecureID FOB

Note: Passphrases must be enabled.

IBM TouchToken – Timed One Time use Password generator

- Authentication factor that can be directly evaluated on z/OS to ensure that there is always a means of enforcing 2 factor authentication for users
- Provisioned with a shared secret key into the iOS key chain
- Does not rely on an external server, eliminates an external point of failure

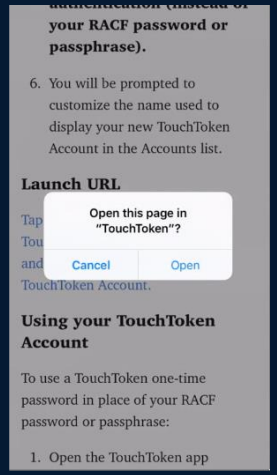




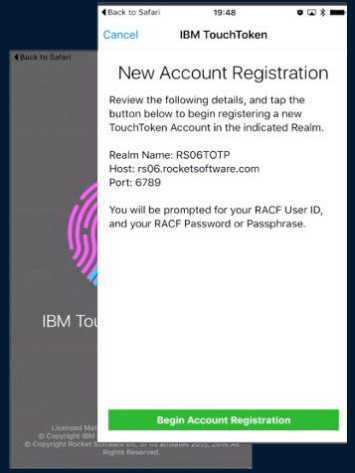
Logon with IBM Touch Token (TOTP):

- **A)** User logs on with User ID & TouchToken (generated on provisioned iOS device)
- **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 user's authentication factors in this case the IBM TouchToken code (ICSF Call)
- **E)** RACF uses IBM MFA status to allow or deny the logon

Using IBM TouchToken for iOS – Registration

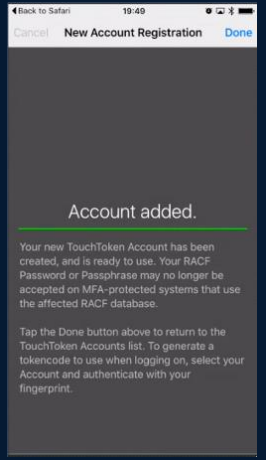


1. RACF admin sends registration email to user



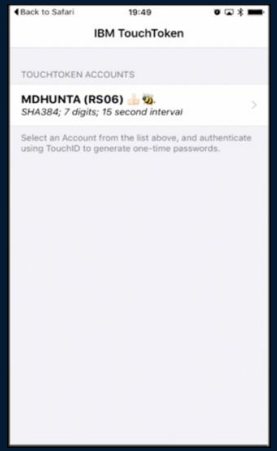
2. User receives email and clicks link to open TouchToken App

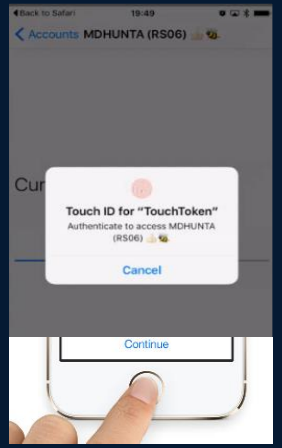
3. User confirms registration by using their RACF credentials to authenticate

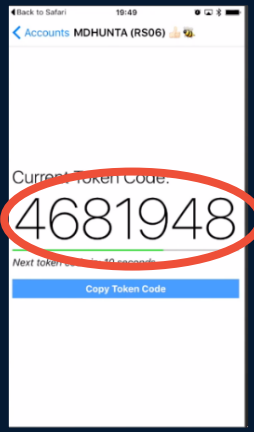


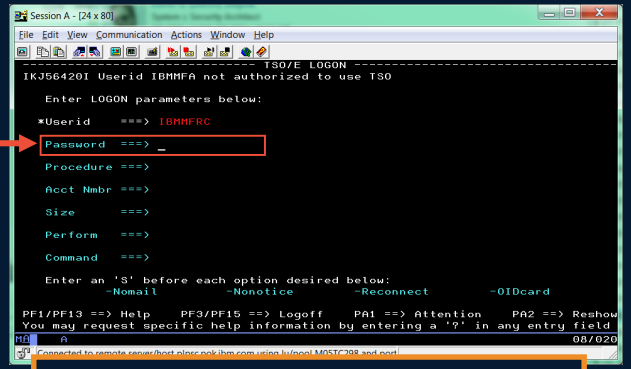
4. Device is provisioned for TouchToken

Using IBM TouchToken for iOS – Logon to TSO









Something you have: Token Code

Something you are: Fingerprint

1. User selects the account that a IBM TouchToken will be used for Authentication
2. Authenticates with Touch ID, scan fingerprint.
3. IBM TouchToken app access the iOS key chain to generate a TouchToken code
4. User enter TSO user ID and current token

MFA Out-of-Band Support

IBM MFA Out-of-Band support is a feature which allows users to authenticate to multiple factors directly to IBM MFA and receive a logon token

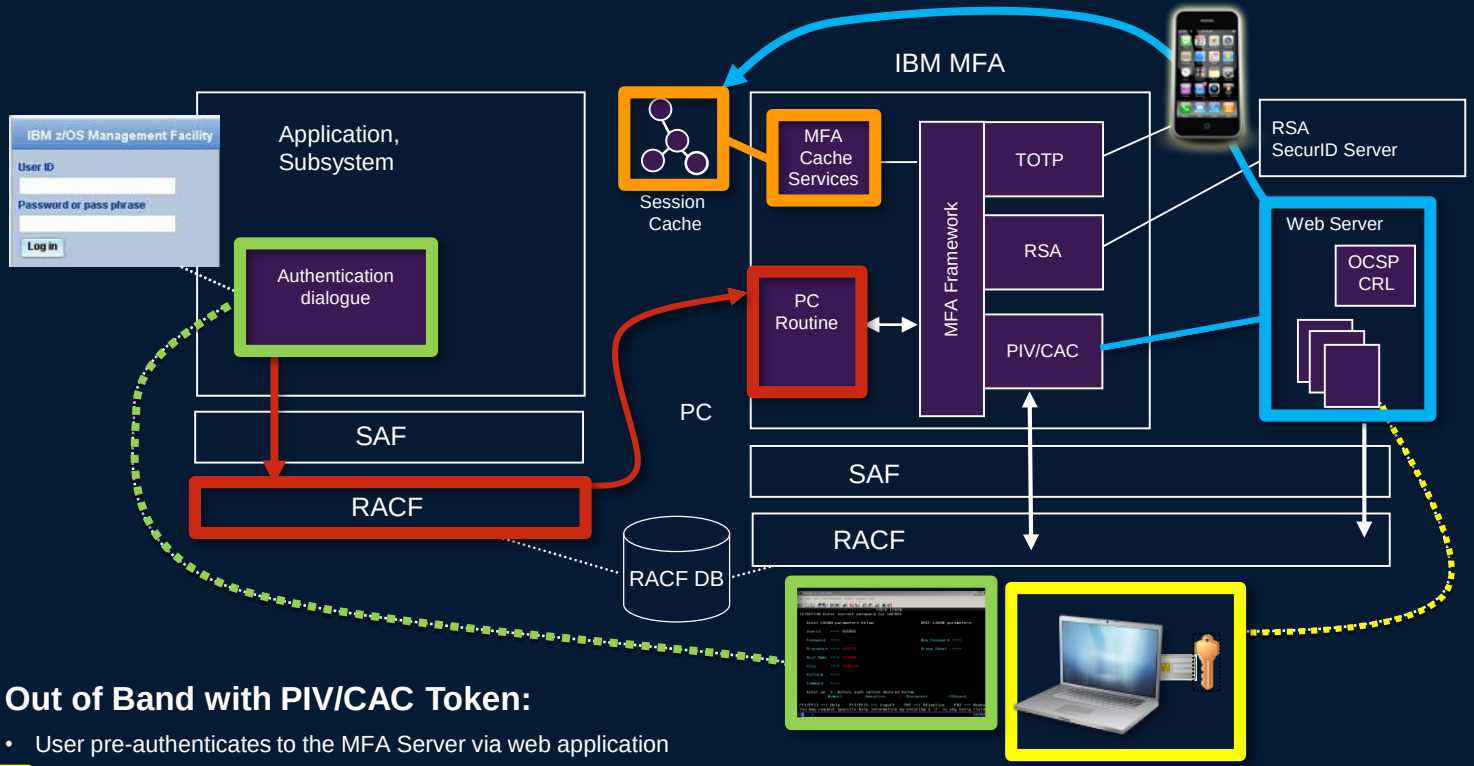
Out-of-band authentication allows for a number of improvements to IBM MFA & RACF

- Allows greater control over the user authentication experience
  - e.g.: Via webpage, mobile smartphone app, or other future supported token types
- Supports factor types which are not well suited to text entry
  - Smart cards, biometrics
- Lays the foundation for *combining or "compound factors"* which can be used to authenticate a user
  - Which otherwise would not fit in-band without significant application changes
    - e.g.: Authenticate with both RACF password phrase and RSA SecureID token
- The pre-authentication logon tokens behavior can be customized as needed
  - Controls to allow tokens to be single use or re-useable
  - Control how long a token is valid

IBM MFA PIV/CAC Support

- A personal identity verification (PIV) or Common Access Card (CAC) is a United States Federal Government smart card
- Contains the necessary data for the cardholder to be granted to Federal facilities and information systems
- They are standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel
- Provides the foundation for supporting other certificate based smart card authentication tokens

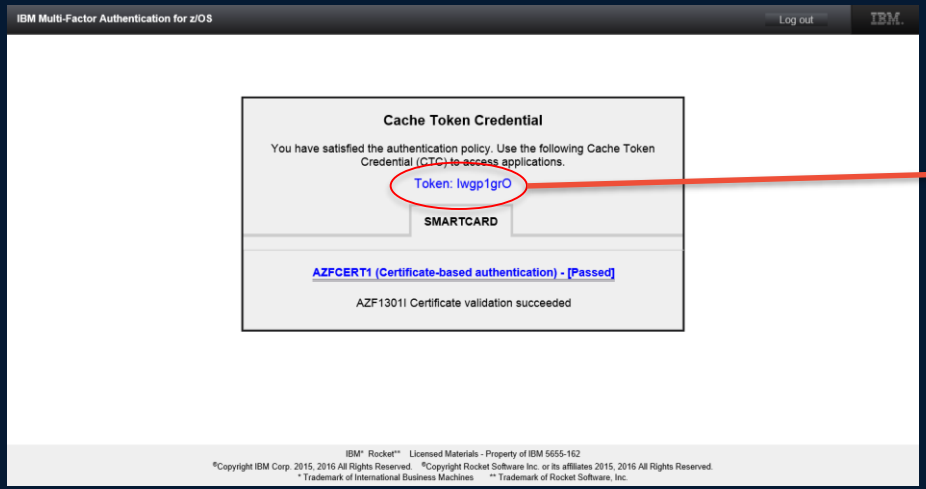
- PIV/CAC cards are the latest token types supported by IBM MFA
- Treated as PKCS#11 tokens
- Certificate chain stored in the RACF database in a key ring associated with the user that is defined to require PIV/CAC card token types
- Leverages the out of band support

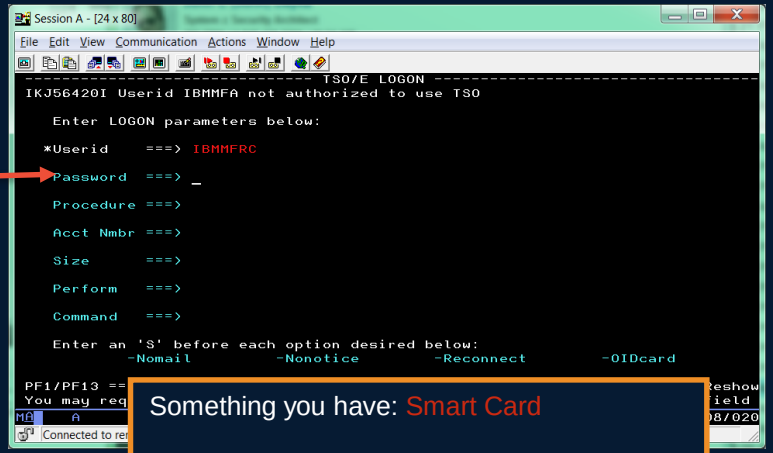


Out of Band with PIV/CAC Token:

- User pre-authenticates to the MFA Server via web application
  - Leverages web browser support for PKCS#11 HW tokens
  - User enters PIN to unlock the smart card, TLS session with client authentication used to prove knowledge of the private key
  - User authenticates to the Web application and passes to MFA authenticated client cert. MFA matches cert components in the User profile and if valid and generates a Cache Token Credential (CTC) and returns to the web application. The CTC is displayed on the user's browser window
- User enters CTC in the password field on the application authentication dialogue
- Application calls RACF to evaluate the user's credentials, and in turn calls IBM MFA
- MFA checks the session cache to ensure that the user had pre-authenticated and evaluates the CTC. If valid, MFA returns to RACF and logon processing continues

Using PIV/CAC support – Logon to TSO





1. User logs on with RACF Credentials
2. User chooses Authentication Policy from list and selects a certificate
3. User enters their Smart Card PIN code
4. User enter TSO user ID and current token

Selective MFA Application Exclusion

- Allows users to authenticate to z/OS applications with multiple authentication factors
- Some applications have authentication properties which can prevent MFA from working properly:
  - **No phrase support** – Some MFA authenticators can be longer than 8 chars
  - **Replay of passwords** – Some MFA credentials are different at every logon and can't be replayed
- 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 password, password phrase or PassTicket

IBM MFA PassTicket Support

- Some classes of applications authenticate a user initially with their password/phrase or perhaps using MFA credentials, and make subsequent calls to SAF/RACF using PassTickets to authenticate a given user.

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

- Controls to enable PassTickets
  - New special MFA PassTicket Factor

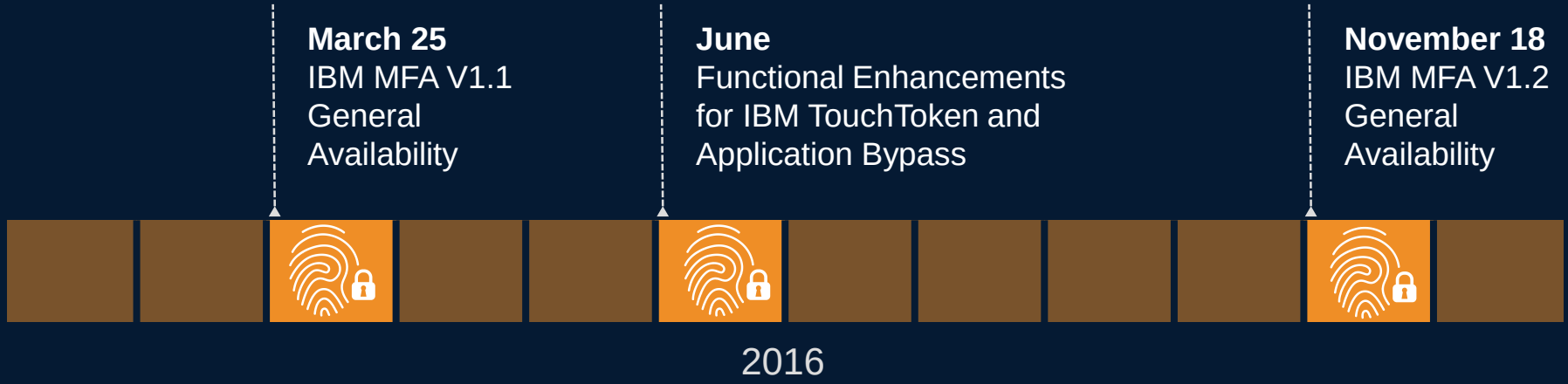
```
RDEFINE MFADEF FACTOR.AZFPTKT1
ALTUSER JOEUSER MFA(FACTOR(AZFPTKT1) ACTIVE)
```

- MFA processing will call SAF/RACF during authentication when the PassTicket factor is ACTIVE and input is a valid RACF PassTicket.

A new z/OS product has become available

IBM Multi-Factor Authentication for z/OS (5655-162)

IBM Multi-Factor Authentication for z/OS S&S (5655-163)



Requirements:

- z/OS 2.1 or later
- RSA Authentication Manager 8.1 or later for RSA® SecurID® exploitation

Requests For Enhancements (RFE)

It is strongly recommended that clients identify their requirements for IBM MFA through this channel.

In particular, please open RFEs for additional authentication tokens that are used in your shop that would provide value if supported by IBM MFA for z/OS.

Link: *https://www.ibm.com/developerworks/rfe*

Additional Resources and Events

Resources

- Introduction to IBM MFA
- IBM MFA Solution Brief
- IBM Multi-Factor Authentication for z/OS V1.2 Announcement Letter
- IBM Multi-Factor Authentication for z/OS Product Page

Contacts

- Michael Zagorski – IBM MFA Offering Manager (zagorski@us.ibm.com)

SHARE
EDUCATE • NETWORK • INFLUENCE

Thank You for Attending!
Please remember to complete your evaluation of this session in the SHARE mobile app.

RACF Update: Multi-Factor Authentication is Here!

Session: 20369

SHARE San Jose 2017