



IBM Multi-Factor Authentication for z/OS

Ross Cooper, *CISSP
IBM z/OS Security Software Design and Development
NewEra – The z Exchange
10/24/2017

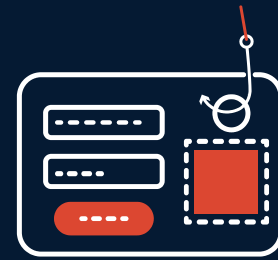
Current Security Landscape



1,935

Number of security incidents in 2016 with confirmed data disclosure as a result of stolen credentials.¹

(506 worse than prior year)



81%

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

(18% worse than prior year)



\$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 2017 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
 - Employees are selling their passwords
 - Password reuse
 - People write down passwords
 - Malware
 - Key log
 - Password cracking



Compliance

PCI DSS v3.2

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the Cardholder Data Environment (CDE) for personnel with administrative access.

*Note: This requirement is a best practice until **January 31, 2018**, after which it becomes a requirement.*

NIST SP 800-171

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

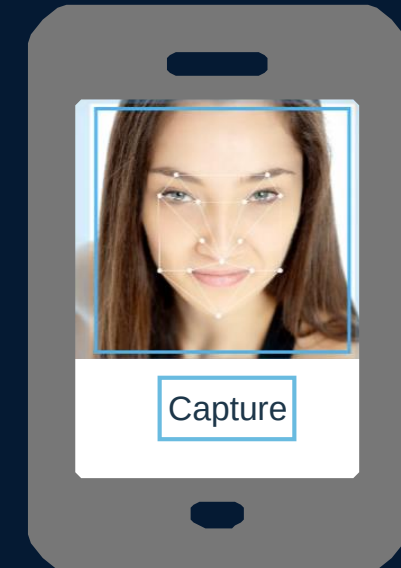
Note: Network access is any access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

*Note: This requirement is effective **December 31, 2017**.*



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 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
 - **NEW:** RADIUS-based factors
 - **NEW:** High Availability MFA Web Services

- Tightly integrated with SAF & RACF



gemalto
security to be free

*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

Must Protect...

System Administrator with access to sensitive data sets

RACF Administrator who controls system-wide authorization

Privileged User with access to patient health records

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

Support **NIST SP 800-171 Requirements**



Should Protect...

Law Clerk with access to corporate IP

Financial Analyst with access financial data prior to being made public

Executive with access to corporate strategy

Engineer who is developing the next product breakthrough

Everyone with access to data that you don't want released to the public!!



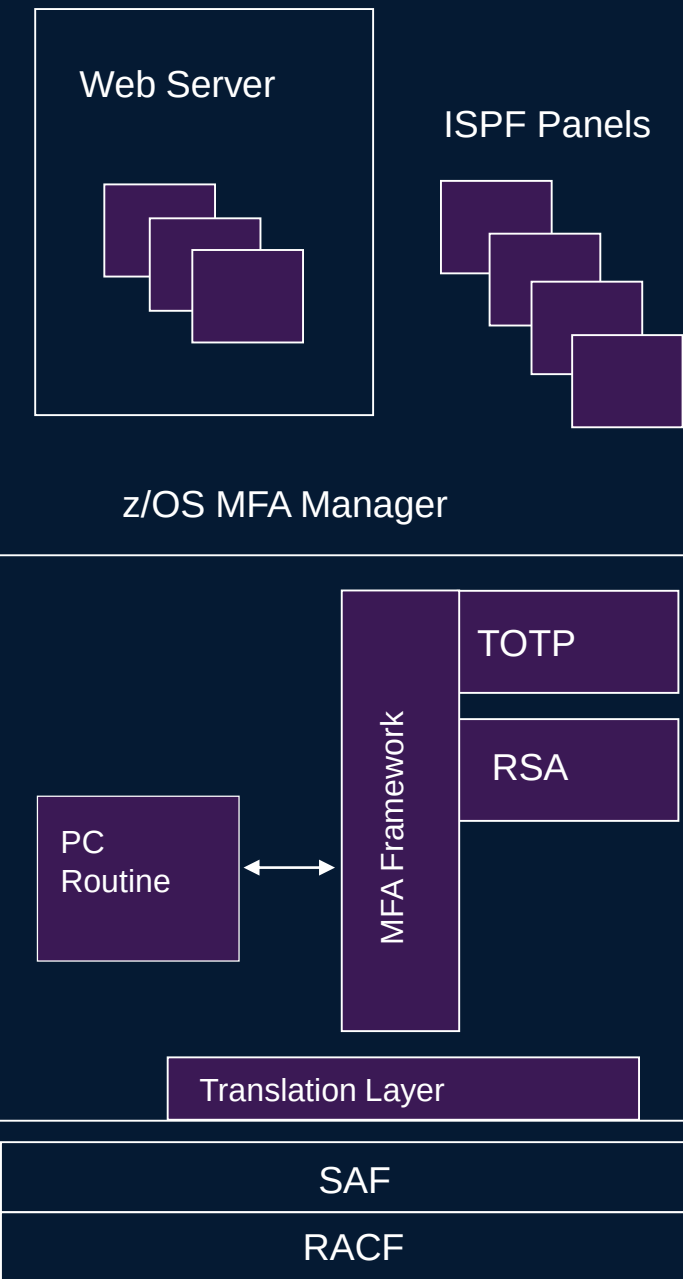
RACF Support

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

RSA SecurID Tokens Support



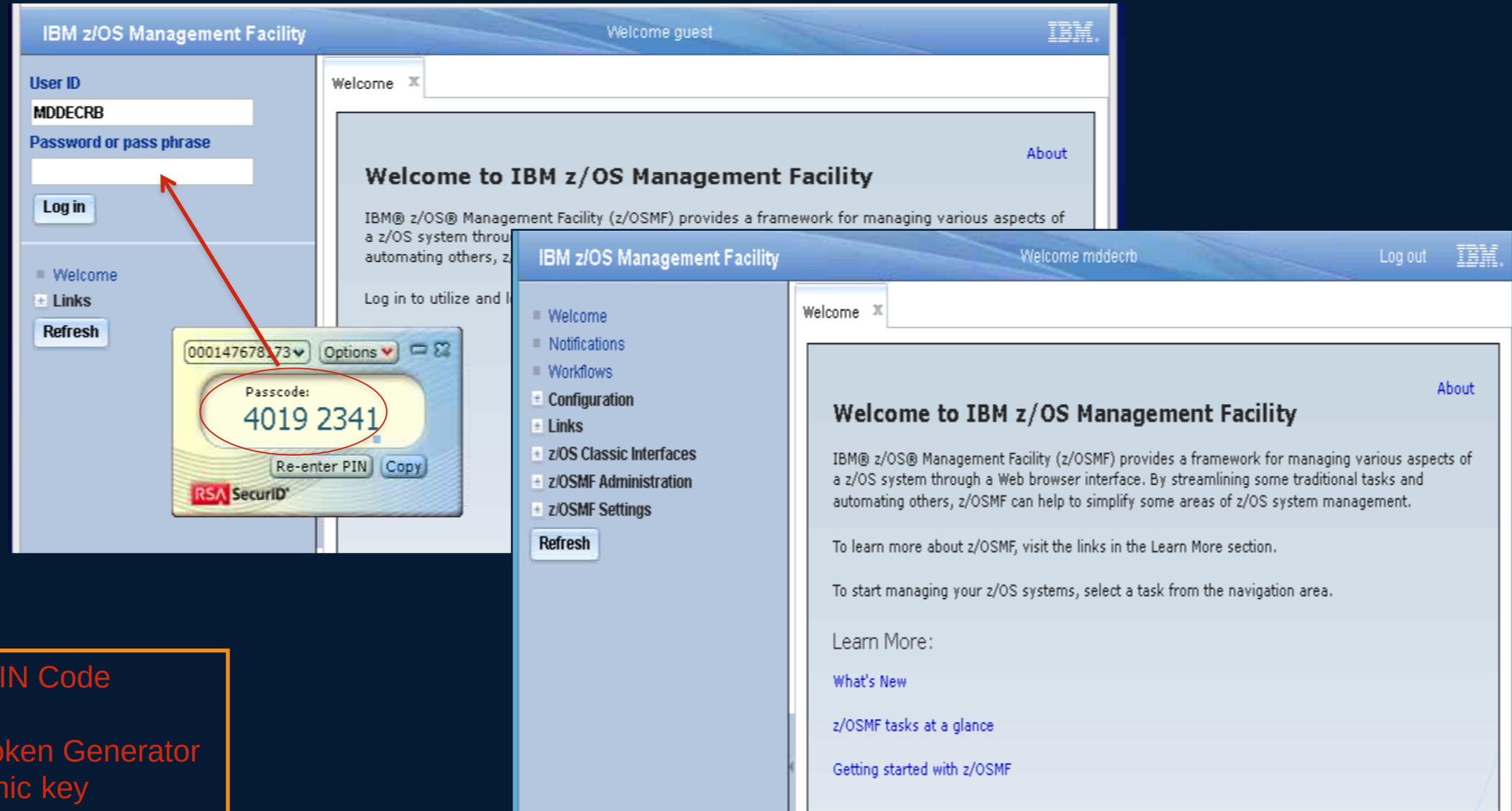
- Requires RSA SecurID server configured to the MFA Server
- Since the use of RSA SecurID requires an external configured server instance – this could represent a point of failure
- Supports both hard and soft RSA SecurID tokens



Requires RSA Authentication Manager 8.1 or later for RSA® SecurID® exploitation

Using Soft RSA SecurID Tokens

- RSA SecurID 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**

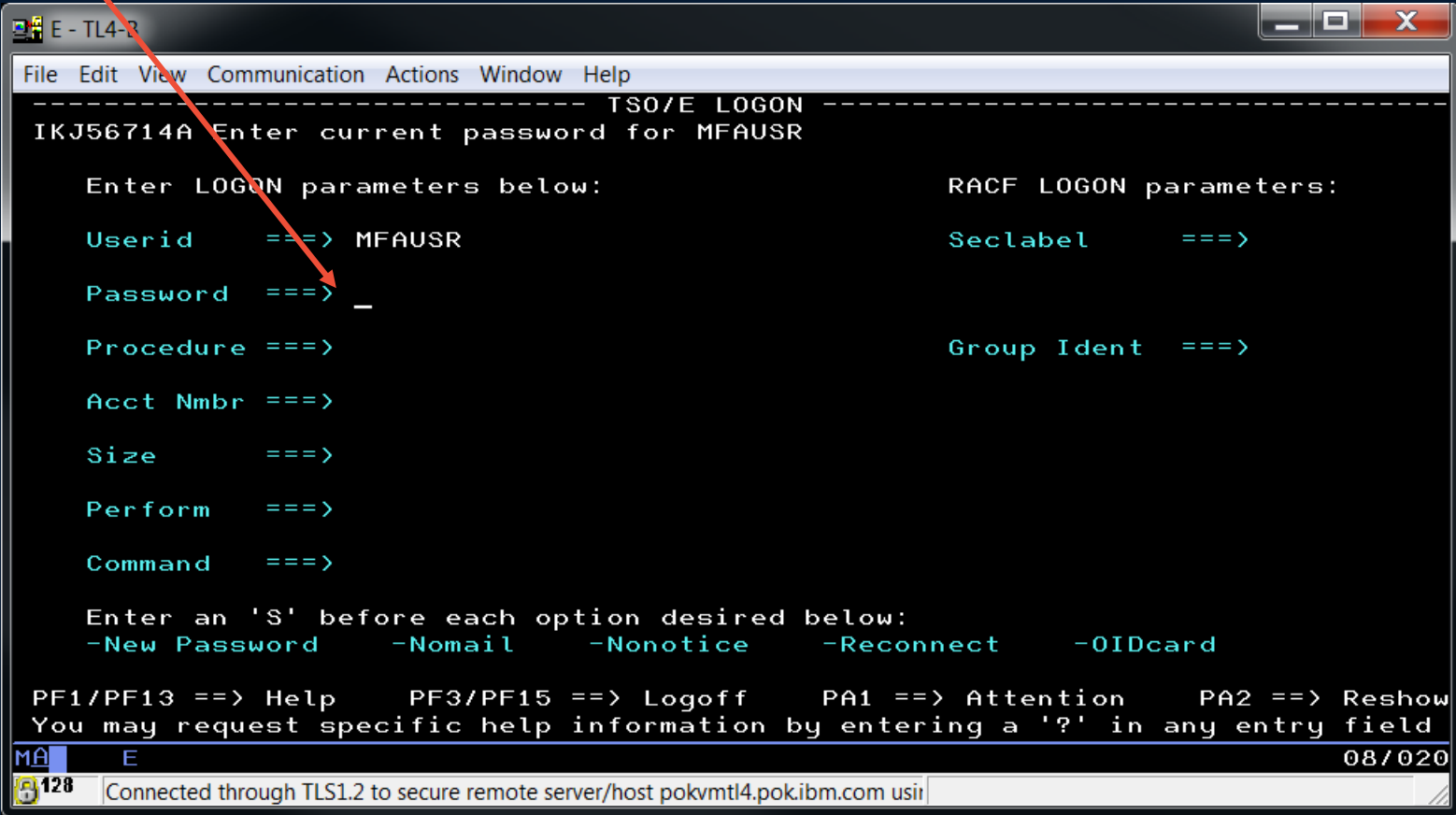
Something you have: **RSA Token Generator with your specific cryptographic key**

Using Hard RSA SecurID Tokens



Something you know: RSA PIN Code

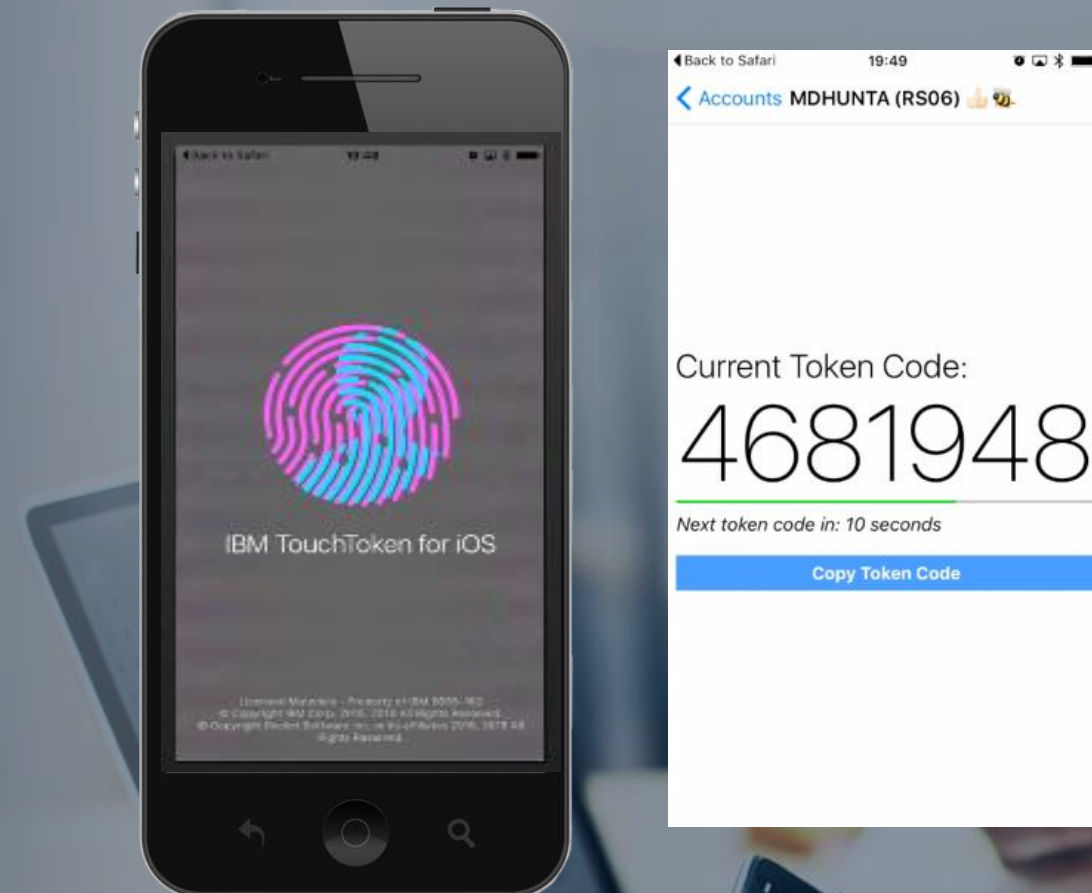
Something you have: RSA SecurID FOB
with your specific cryptographic key



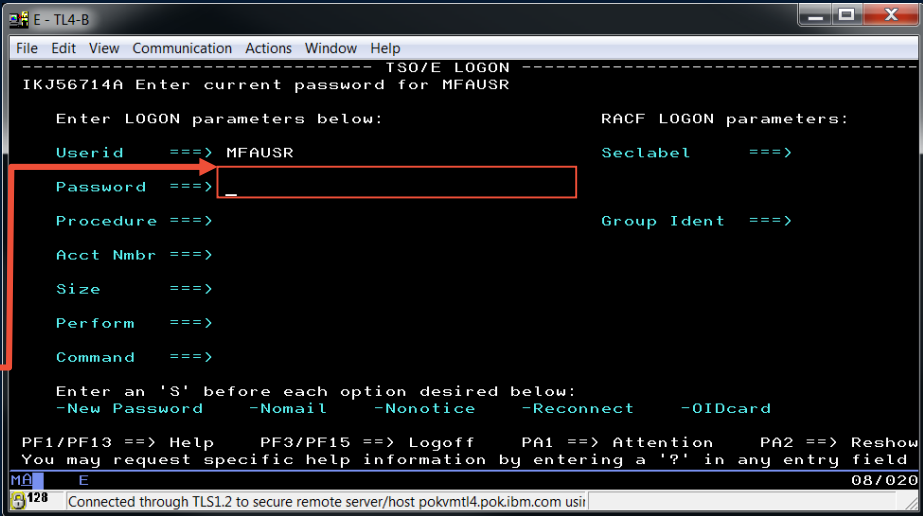
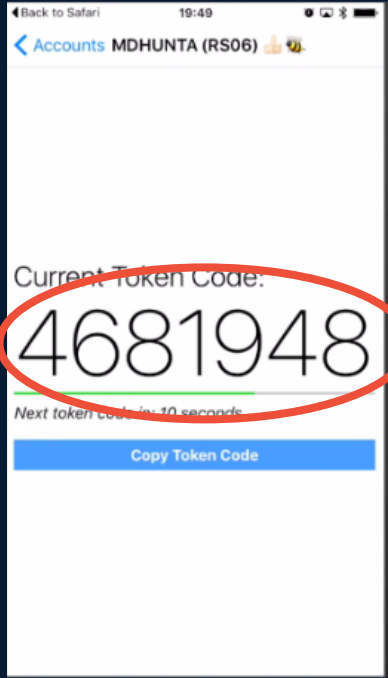
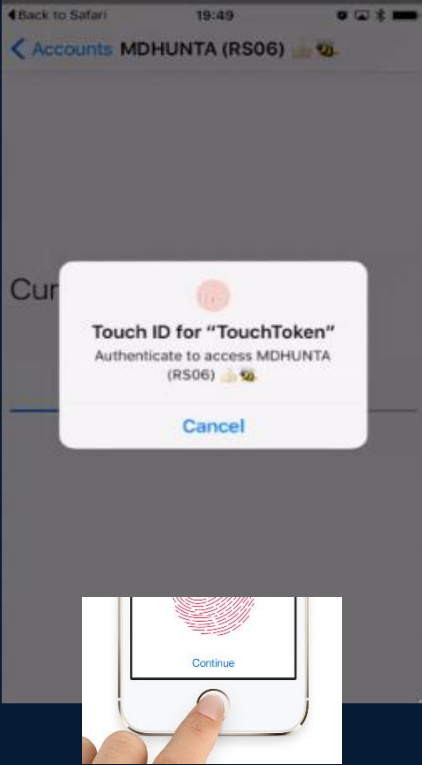
Note: Applications must be configured to support password phrases.

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



Using IBM TouchToken for iOS – Logon to TSO



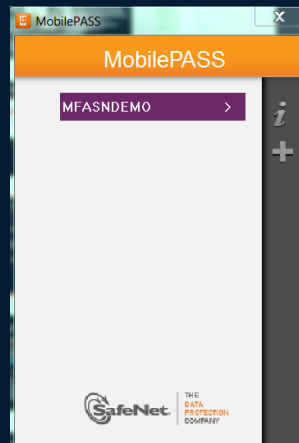
Something you have: **iOS device with your specific cryptographic key inside.**

Something you are: **Fingerprint**

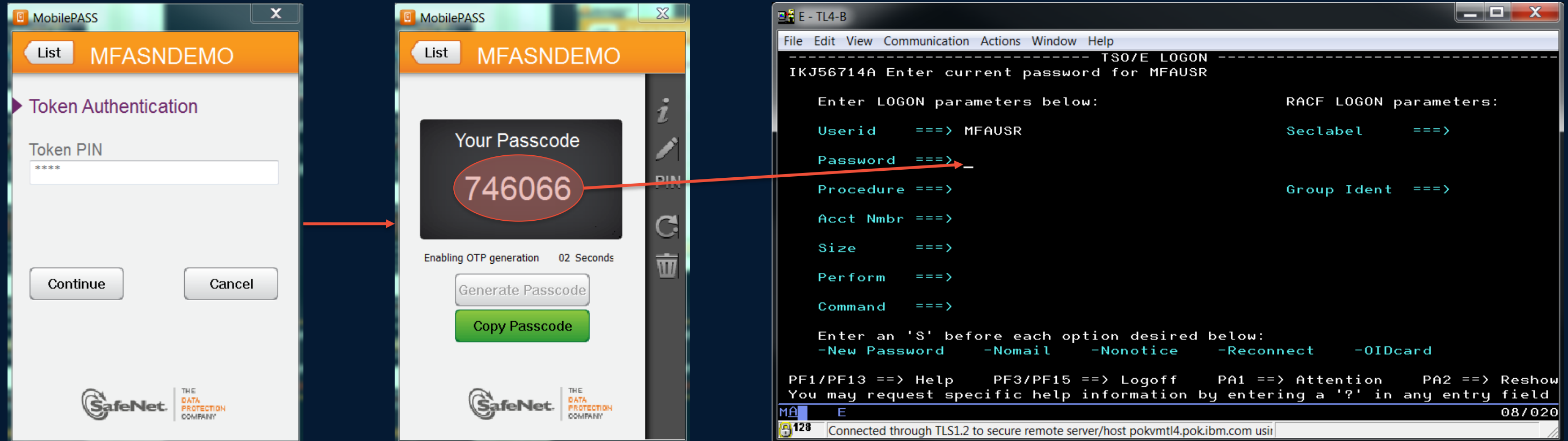
1. User selects the account that a IBM TouchToken will be used for Authentication
2. Authenticates with Touch ID, scan fingerprint.
3. IBM TouchToken app access the iOS key chain to generate a TouchToken code
4. User enter TSO user ID and current token

Gemalto SafeNet Token Support

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



Using Soft Safenet MobilePASS Tokens



Something you know: MobilePASS PIN Code

Something you have: MobilePASS Token Generator with your specific cryptographic key

- Safenet MobilePASS PIN code is entered into the MobilePASS application.
- User enters their RACF User ID and MobilePASS passcode in the password field.

MFA Out-of-Band Support

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



- Supports factor types which are not well suited to text entry
 - Smart cards, biometrics
- Provides a foundation for *combining* or “*compound factors*” which can be used to authenticate a user
 - Authenticate with both RACF password phrase and RSA SecurID 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

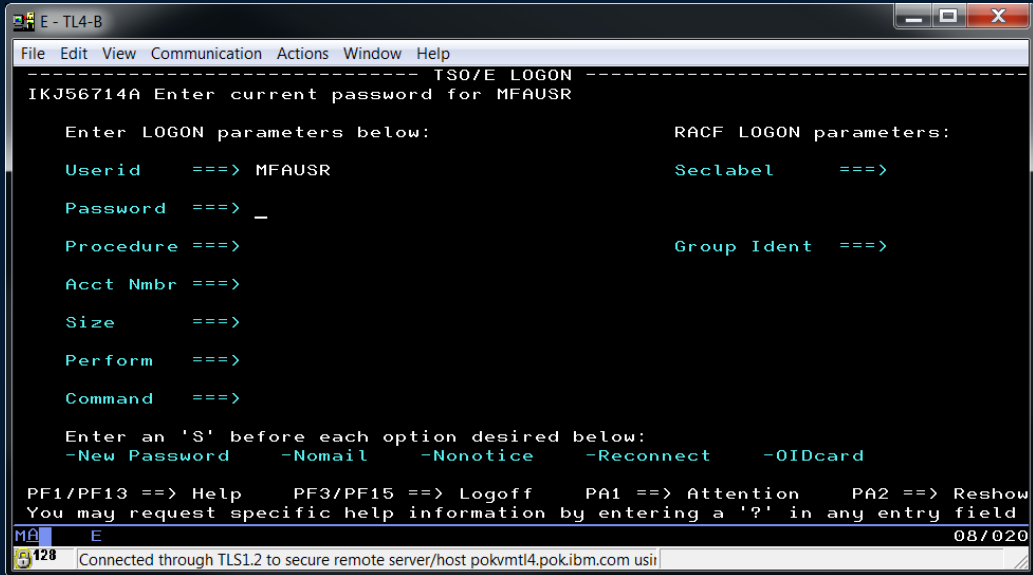
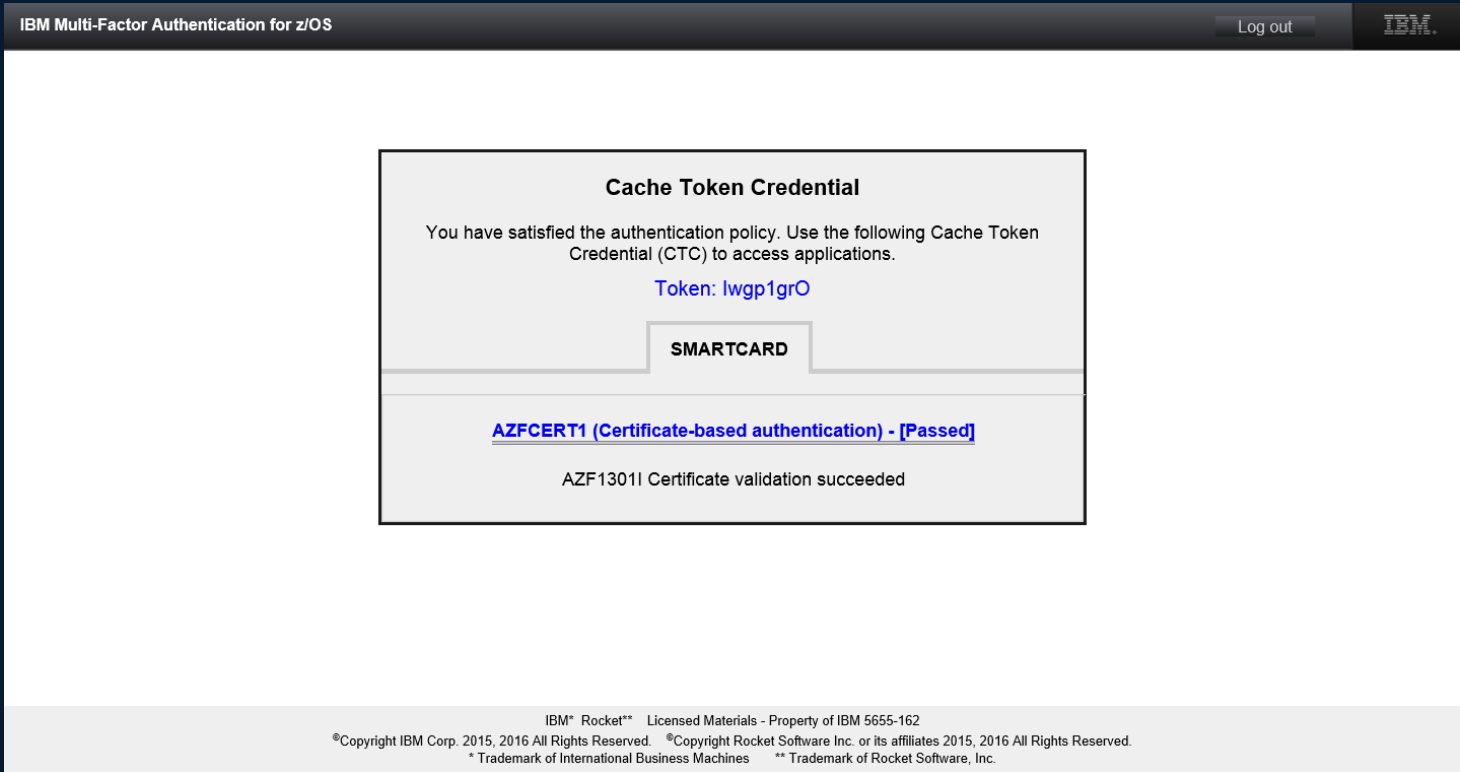
IBM MFA PIV/CAC Support

- 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



- 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

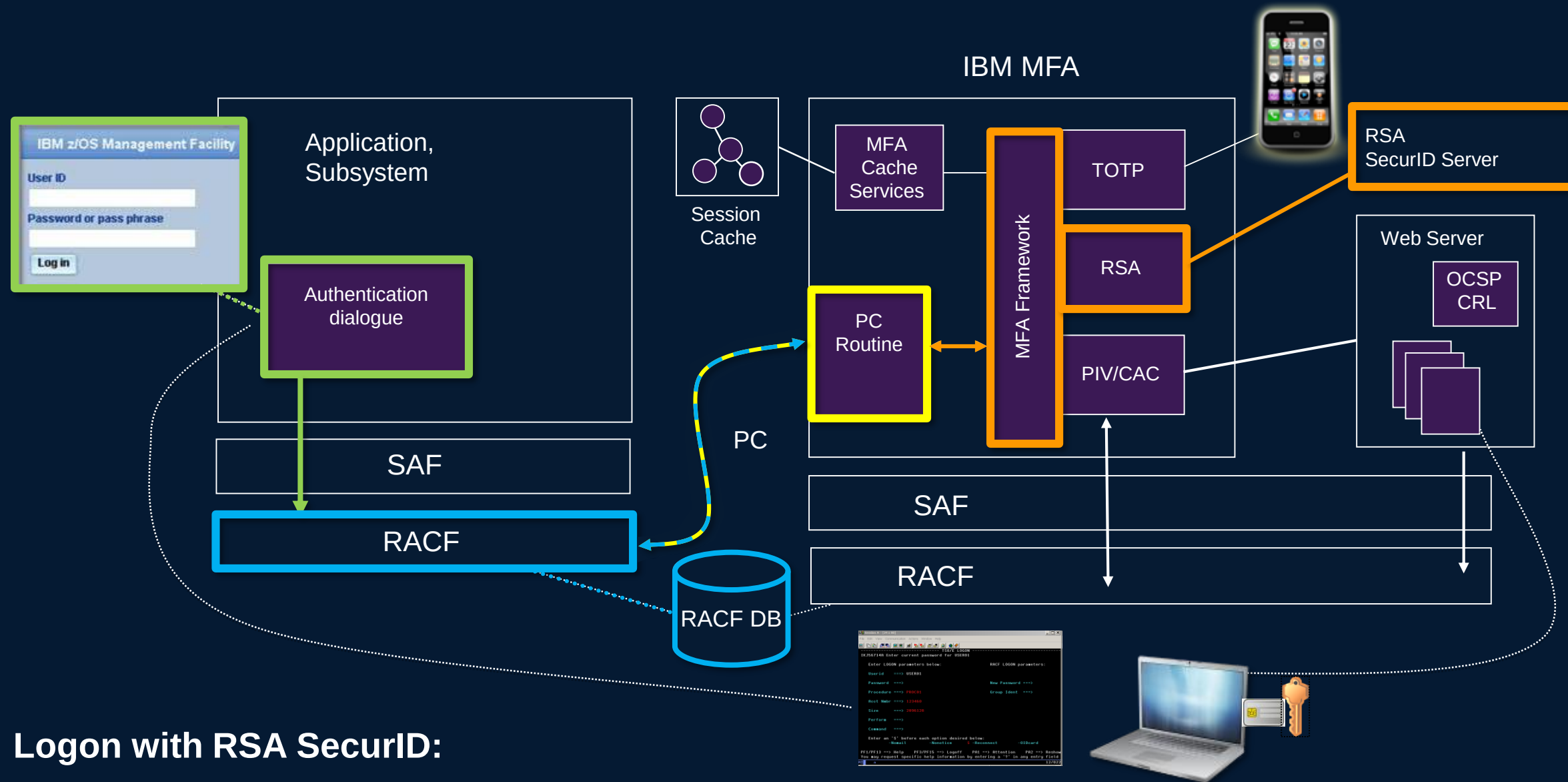
Using PIV/CAC support – Logon to TSO



Something you have: **Smart Card**

Something you know: **RACF Password & PIN**

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



Logon with RSA SecurID:

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

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

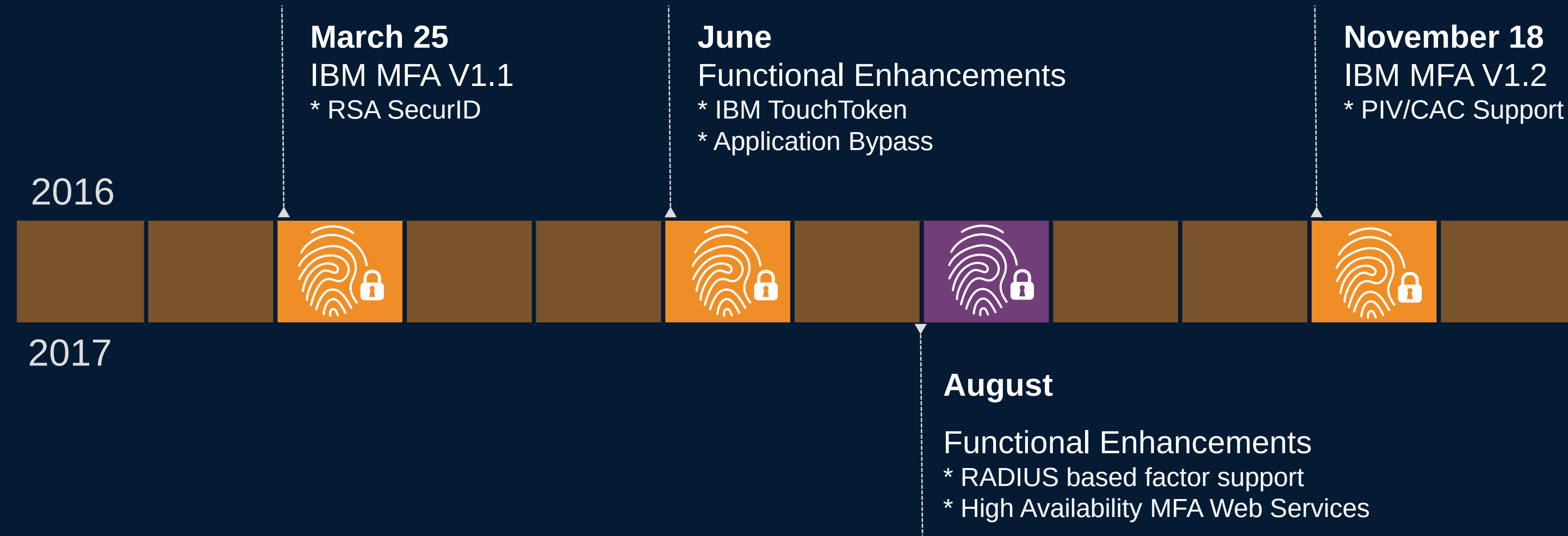
```
RDEFINE MFADEF FACTOR.AZFPTKT1  
ALTUSER JOEUSER MFA (FACTOR (AZFPTKT1) ACTIVE)
```

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

Product Timeline

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

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



What's new in IBM MFA? – Functional Enhancement

Remote Authentication Dial-In User Service (RADIUS) based factor support

- Generic RADIUS factor that enables inter-operability with generic RADIUS servers
- SafeNet RADIUS factor that is designed to operate with Gemalto SafeNet Authentication Service servers

High Availability MFA Web Services

- IBM MFA now supports running multiple instances of the MFA Web Services started task in a Sysplex. Thus if an LPAR running MFA Web Services has to be re-IPL'ed or is otherwise out of service for planned maintenance, users can continue to pre-authenticate with MFA web services on one of the remaining instances running within the Sysplex.

This support was made available on 08/16/2017 via PTF UI49610.

What's new in IBM MFA? – Functional Enhancement

Compound In-band Authentication support

- Ability to authenticate with both a token code and a RACF password
- Enabled per MFA factor (AZFSIDP1, AZFTOTP1, AZFRADP1, AZFSFNP1)

Express Logon Facility (ELF) support

- New integration has been provided, through a new SAF API, that enables Express Logon Facility users to interface with the IBM MFA smart card support.
- This enhancement requires the presence of a user's smart card when authenticating.
- It prevents RACF user ID-only authentication attempts

This support will be made available via APARs PI86469 and PI86470.

What's new in IBM MFA? – Version 1 Release 3

Generic TOTP

- The time-based, one-time password factor has been enhanced to support more generic TOTP token applications.
- This introduces support for standard-compliant TOTP third-party applications that run on Android and Microsoft™ Windows™ devices.

Bulk provisioning

- Scripts that enable a large number of users to be easily provisioned.
- In particular, this simplifies provisioning PIV/CAC users who can be provisioned and enabled immediately, eliminating the self-service provisioning step.

Strict PCI Compliance

- Ability to configure IBM MFA to operate in a strict PCI-compliant mode. When this mode is activated, messages that "leak" information are not returned.
- The out-of-band pre-authentication process always requires entry of all factor credential data before returning any information about the pre-authentication attempt.

This support will be made available November 17, 2017.

CA Technologies Support

CA Technologies Security Products and IBM Multi-factor Authentication for z/OS

- CA ACF2 R16: PTF RO92884 provides support.
- CA Top Secret R16: PTF RO92696 provides support.
- See CA Technologies document TEC1202485 which discusses the preparation for implementation of CA Advanced Authentication Mainframe (AAM) or IBM's Multi-Factor Authentication (MFA) support.
- Check with CA Technologies support for the most current information.

Works with....

Token types

- IBM TouchToken
- RSA
- SafeNet
- Token types which supports the RADIUS protocol

Session Managers

- CL SuperSession
- Macro 4 Tubes
- IBM Session Manager

Other products

- | | |
|---|--------------------------------|
| – RDz | – TKE |
| – CICS, CICSplexSM | – TSO |
| – IMS-DC | – USS |
| – ftp | – Websphere Application Server |
| – sftp | – LDAP |
| – OMVS telnet | |
| – ssh | |
| – z/OSMF | |
| – IBM HTTP Server powered by Apache | |
| – CO:Z | |
| – Connect Direct | |
| – DB2 DRDA | |
| – Netview v6.2 | |
| – Tivoli Monitoring (OMEGAMON) - 3270 interface | |

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

Resources

- [Introduction to IBM MFA](#)
- [IBM MFA Solution Brief](#)
- [IBM Multi-Factor Authentication for z/OS V1.3 Announcement Letter](#)
- [IBM Multi-Factor Authentication for z/OS Product Page](#)

Contacts

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

Thank you

Frequently Asked Questions

Q & A

Q: What systems software is needed to run IBM MFA?

A: IBM MFA for z/OS is a new product that requires z/OS 2.1 or later releases and z/OS Security Server RACF with PTF for APAR OA50930. In addition, RSA Authentication Manager 8.1 for RSA SecurID exploitation is required for SecurID token support. To enable IBM TouchToken support, clients will need ICSF configured for enabling PKCS#11 Tokens and configure and enable AT-TLS with z/OS Communication server.

Q: Does IBM MFA Support Android device?

A: This will be supported in IBM MFA V1R3, available November 17, 2017.

Q: How is IBM MFA priced?

A: The charge is per user ID per RACF DB, excluding backups and DR copies. IBM MFA has Value-Unit based pricing. Value units use a sliding scale approach based on the number of user IDs requiring IBM MFA support. There is also a charge for subscription and support (S&S).

Q: Can passphrases be used with MFA?

A: Passphrases and passwords cannot be used to authenticate to the system once a user is enabled with MFA. If a user is enabled with MFA, the ALTUSER command can be used to disable MFA and then the user can fall back to using password or passphrase authentication. If application bypass is used for an application, those users that have been given the appropriate authority will be allowed to authentication with their RACF password or passphrase. UPDATE: Passphrases and Passwords can be used with the new Compound In-band support.

Q: Where can I get the IBM TouchToken App?

A: IBM TouchToken application can be found in the Apple Appstore. Search on 'IBM TouchToken' or use this link:

<https://itunes.apple.com/us/app/ibm-touchtoken/id1135457433?ls=1&mt=8>

Q: Can I have a TOTP generator for my administrator's ID on multiple IOS devices?

A: No, at this time, only one iOS device can be registered per user.

Q & A

Q: Does MFA support the coupling facility?

A: Yes, you can share the IBM MFA cache using the CF

Q: Is ICSF required?

A: ICSF is required if you use IBM MFA TouchToken or Out of Band. The z/OS communication server and AT-TLS must already be installed and configured.

Q: Does MFA use traditional passtickets as the mechanism underneath? If yes, do they support replay protection?

A: IBM MFA does NOT use PassTickets itself, but it can optionally support applications which use PassTickets such as session managers. In this case replay protection is supported.

Q: If the password or passphrase expired MFA logon will still succeed?

A: Yes. Note that your RSA credentials can expire and when that happens with a PIN, you will be prompted to change your RSA PIN through the TSO logon panel.

Q: Is web server IHS (IBM Http Server (Apache)) based?

A: No, it is a custom socket application that implements HTTP

Q: Does IBM resell the RSA server?

A: No.

Q: Is RSA always on an x86, is there a solution that runs on z?

A: There is not a z based solution for RSA.

IBM Multi-Factor Authentication for z/OS

Part II - Technical Information for RACF

RACF MFA Documentation

- **RACF APAR Doc:**
 - <ftp://ftp.software.ibm.com/s390/zos/racf/pdf/oa48359.pdf>
- **Security Administrators Guide:**
 - Introduction and overview of MFA support
- **Command Language Reference:**
 - ALTUSER Command syntax for new MFA keywords
 - LISTUSER new MFA output information
- **Messages and Codes:**
 - New MFA related Messages
- **RACROUTE Macro Reference:**
 - RACROUTE REQUEST=VERIFY – PASSCHK=NOMFA
- **Callable Services Guide:**
 - R_Admin – Details of new MFA related fields
 - R_Factor – Details of new MFA callable service
 - R_GenSec & R_TicketServ – Option to return more detailed PassTicket evaluation failure Reason Codes
- **Macros and Interfaces:**
 - MFA fields in Database Unload records
 - SMF Records: ALTUSER new command keywords & RACINIT Authentication Information bits
 - Updated Database templates – new MFA fields
 - New MFADEF class
 - RCVT MFA function is available bits
 - ACEE MFA required / authenticated bits

MFA Data Stored in RACF Profiles

- The RACF database serves as the data repository for MFA data.
- MFA data is accessed via RACF commands and via the R_Factor SAF/RACF callable service.
- **User Specific MFA Data:**
 - Contains general MFA user policy information and factor specific data for the user.
- **Authentication Factor Definition:**
 - Defines an authentication factor and contains factor configuration – used by IBM MFA
 - New RACF general resource class: MFADEF
 - Profile naming conventions: FACTOR.<factorName>
- **Out-of-Band Authentication Policy:**
 - Defines a set of authentication factors a user is required to satisfy
 - Stored in the MFADEF class
 - Profile naming conventions: POLICY.<policyName>
 - Contains OOB token configuration

MFA RACF User Profile Management

- User provisioning via the ALTUSER Command:

```
[ MFA (
  [ FACTOR(factor-name) | DELFACTOR(factor-name) ]
  [ ACTIVE | NOACTIVE ]
  [ TAGS(tag-name:value ...) ]
    | DELTAGS(tag-name ...)
    | NOTAGS ]
  [ ADDPOLICY(policy-name ...)
    | DELPOLICY(policy-name... | *) ]
  [ PWFALLBACK | NOPWFALLBACK ]
)
| NOMFA ]
```

- **FACTOR(*factor-name*) | DELFACTOR()**
 - Identify the factor being added / modified / deleted for the user
- **ACTIVE | NOACTIVE**
 - Users with an ACTIVE factor must authenticate with that factor instead of their password/phrase.
- **TAGS | DELTAGS | NOTAGS**
 - Modify the list of factor specific tag name/value pairs. Used to add factor specific data associated with a user.
- **ADDPOLICY | DELPOLICY**
 - Modify the list of Out-of-Band policies associated with the user.
- **PWFALLBACK | NOPWFALLBACK**
 - Allows a user to authenticate with their RACF password / phrase when IBM MFA is unavailable or can not evaluate a credential.

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

RACF User Provisioning for MFA

- **Remove a Factor:**

```
ALTUSER JOEUSER MFA (DELFAC (AZFSIDP1))
```

- **Remove all MFA data:**

```
ALTUSER JOEUSER NOMFA
```

- **Add MFA tags:**

```
ALTUSER JOEUSER MFA (FACTOR (AZFSIDP1) TAGS (TAG1:Value1 TAG2:Value2))
```

- **Replace an existing tag:**

```
ALTUSER JOEUSER MFA (FACTOR (AZFSIDP1) TAGS (TAG1:Value1A))
```

- **Delete a tag:**

```
ALTUSER JOEUSER MFA (FACTOR (AZFSIDP1) DELTAGS (TAG1))
```

Listing User MFA Information

```
LISTUSER JOEUSER MFA
...
THERE IS NO MULTIFACTOR AUTHENTICATION
DATA.
```

```
LISTUSER JOEUSER
...
MULTIFACTOR AUTHENTICATION DATA EXISTS.
USE THE MFA KEYWORD TO DISPLAY IT.
```

```
LISTUSER JOEUSER MFA
...
MULTIFACTOR AUTHENTICATION INFORMATION:
-----

PASSWORD FALLBACK IS NOT ALLOWED
AUTHENTICATION POLICIES:
    USERPOL1
    FACTOR = FACTORA
    STATUS = ACTIVE
    FACTOR TAGS =
        TAGONE:ABC
        TAGTWO:1234
    FACTOR = FACTOR2
    STATUS = INACTIVE
    FACTOR TAGS =
        TAG1:Value1
        TAG2:Value2
```

ALTUSER MFA TAG Validation

- **TAG Validation:**

- The TAGS names and values are validated by IBM MFA.
- The ALTUSER command calls the IBM MFA PC interface passing in the TAGs names and values.
- IBM MFA may reject the command if the tag name or value is not valid.
- **ICH21051I IBM MFA detected an error in the name-or-value of tag tag-name with the following message: MFA-msg**
- The IBM MFA started task must be running in order for TAG validation to occur.
- **ICH21052I Unable to contact IBM MFA to validate tag data. No MFA data is updated.**

- **TAG Deletion notification:**

- DELUSER / ALTUSER will call IBM MFA to notify it when TAGS will be deleted.
- IBM MFA uses this information to potentially clean up associated resources, such as an ICSF key label for Touch Token.

MFA RACF ALTUSER Command Messages

- **ICH21046I MFA cannot be specified for PROTECTED user user-ID.**
 - All MFA Users must also have a password and/or phrase.
- **ICH21047I The FACTOR keyword must be specified when specifying other factor related keywords. No MFA data is updated.**
 - The FACTOR keyword indicates which FACTOR the other keywords modify. ACTIVE, NOACTIVE, TAGS, DELTAGS and NOTAGS are all factor specific.
 - PWFALLBACK is not factor specific.
- **ICH21048I Factor name factor-name cannot be added until the profile-name profile is created in the MFADEF class.**
 - The MFADEF FACTOR.factor-name profile must be created before adding the factor to the user.

RACINIT MFA Support

- **RACROUTE REQUEST=VERIFY** can call IBM MFA during user authentication to handle MFA processing.
- **PASSCHK=NOMFA** option:
 - Allows an application to use VERIFY to check a RACF password for an MFA ACTIVE user.
- **RACINIT Messages:**
- **ICH70008I IBM MFA Message:**
mfa-message
 - IBM MFA can return a message to RACINIT which will either display the message or send it back in a buffer to it's caller.
 - Uses existing RACINIT message return capability.
- **ICH408I LOGON/JOB INITIATION - MULTIFACTOR AUTHENTICATION FAILURE**
 - A user with active multifactor authentication factors attempted to log on with invalid credentials as determined by IBM Multi-Factor Authentication for z/OS.
- **ICH408I LOGON/JOB INITIATION - MULTIFACTOR AUTHENTICATION UNAVAILABLE**
 - A user with active multifactor authentication factors attempted to log on but either IBM Multi-Factor Authentication for z/OS was unavailable to verify them, or RACF was unable to contact IBM MFA. The user is not allowed to fall back to the use of a password or password phrase. The SMF record contains additional information regarding the unavailability of IBM MFA.

RACINIT MFA SMF Records

- **New event code qualifiers are added for the Type 80 event code 1 (RACINIT) record:**
 - **40(28)** – SUCCESSM - Successful Multifactor authentication
 - **41(29)** – INVMFA - Failed Multifactor authentication
 - **42(2A)** – MFAUNAVL - Failed authentication because no multifactor decision could be made for a MFA user who has the NOPWFALLBACK option
 - **43(2B)** – MFAPSUCC - IBM MFA partial success: credentials were not incorrect, but a re-authentication is required.
- **New Authenticator Bits – Indicates how the user was authenticated:**
 - Password / Phrase / PassTicket / MFA
- **Also indicate other Authentication information:**
 - ACEE from VLF / User has MFA factors / Password Fallback Setting / IBM MFA authentication decision

MFA RACF Callable Service Updates

- **R_Admin (IRRSEQ00) – RACF Administration API:**
 - The update-user function and extract-user functions are updated to support the new MFA fields in the BASE segment.
 - All the fields that can be set via the commands can be set programmatically via R_Admin.
- **R_Factor (IRRSFA64) – MFA Service:**
 - Mainly for the IBM MFA product to get and set MFA information from the RACF database programmatically.
 - Authorized by profiles in the FACILITY class.
 1. **Get general factor data** – Retrieve factor wide data from the FACTOR.factor-name profile in the MFADEF class.
 2. **Set general factor data** – Set factor wide data
 3. **Get user factor data** – Retrieve user specific MFA data
 4. **Set user factor data** – Set user specific MFA data
 5. **Get general policy data** – Retrieve policy data from the POLICY.policy-name profile in the MFADEF class.
- **R_GenSec (IRRS GS00 or IRRSGS64) – Generic security API:**
 - **R_TicketServ (IRRSPK00) – Parse or extract:**
 - R_GenSec and R_TicketServ are updated to add a new PassTicket Subfunction code value:
 - 3 – Evaluate PassTicket Extended
 - Same as “Evaluate passticket” function, but the failure reason code is more informative.

Selective MFA Application Exclusion

- The RACF and IBM Multi-Factor Authentication support allows users to authenticate to z/OS applications with multiple authentication factors.
- By default Multi-factor authentication is enforced for all applications for MFA provisioned users.
- **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:**
 - Allow 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 RACF PassTicket

MFA Bypass Examples: Inclusion or Exclusion of Applications

- The MFA bypass policy can be configured to require MFA by default or bypass MFA by default depending on the access level given to a generic MFABYPASS profile.
- Policy to require MFA by default: The following example configuration requires MFA authentication for MFA users to all applications, except the applications identified with a discrete MFABYPASS profile with READ access:

```
MFABYPASS.APPL.*    UACC (NONE)
MFABYPASS.USERID.*  UACC (NONE)
MFABYPASS.DEFAULT   UACC (NONE)
```

```
MFABYPASS.APPL.APP123  UACC (READ)
```

→ MFA excluded for the "APP123" application

Policy to bypass MFA by default: The following configuration bypasses MFA for all applications, except those identified with a discrete MFABYPASS profile with NONE access:

```
MFABYPASS.APPL.*    UACC (READ)
MFABYPASS.USERID.*  UACC (READ)
MFABYPASS.DEFAULT   UACC (READ)
```

```
MFABYPASS.APPL.MYAPP  UACC (NONE)
```

→ MFA included for the "MYAPP" application.

Note: The inclusion/exclusion policy can be customized for different sets of users by granting a different level of access to the generic profiles.

RACF Command extensions for MFA Out-of-Band Support...

- The MFPOLICY contains multi-factor authentication policy information in a MFADEF POLICY.<policyName> profile:

```
[ MFPOLICY (
  [ FACTORS(factor-name ...)
    | ADDFACTORS(factor-name ...)
    | DELFACTORS(factor-name ...)
    | NOFACTORS ]
  [ TOKENTIMEOUT(timeout-seconds) ]
  [ REUSE(YES | NO) ]
)
NOMFPOLICY]
```

- **FACTORS(*factor-name1* ...) | ADDFACTORS() | DELFACTORS() | NOFACTORS**
 - Modifies the list of factors names that are required in order to satisfy this authentication policy.
- **TOKENTIMEOUT(*timeout-seconds*)**
 - Specifies the number of seconds for which out-of-band authentication with the policy is valid.
 - When a out-of-band authentication record times out, a user must authenticate out-of-band again to the MFA Server in order to logon.
 - The value of timeout-seconds can be between 1 and 86,400 (the number of seconds in a day) with a default of 300 seconds (5 min).
- **REUSE(YES | NO)**
 - REUSE (YES) specifies whether this out-of-band authentication policy allows multiple z/OS logons using the out-of-band token within the TOKENTIMEOUT setting.
 - When REUSE(NO) is specified the user must authenticate out-of-band with the policy prior to every z/OS logon.

MFA Out-of-Band Policy Example

- **Add factor definition:**

```
RDEFINE MFADEF FACTOR.FACTOR01  
RDEFINE MFADEF FACTOR.FACTOR02
```

- **Define the MFA authentication policy:**

```
RDEFINE MFADEF POLICY.POL01 MFPOLICY (FACTORS (FACTOR01 FACTOR02) TOKENTIMEOUT (60)  
REUSE (YES) )
```

- **Add the factors and policy to the user:**

```
ALTUSER USER01 MFA (FACTOR (FACTOR01) ACTIVE)  
ALTUSER USER01 MFA (FACTOR (FACTOR02) ACTIVE)  
ALTUSER USER01 MFA (ADDPOLICY (POL01) )
```

- **User is provisioned:**

- USER01 can now authenticate to out-of-band to IBM MFA with FACTOR01 and FACTOR02 to obtain a logon token code. The token code can then be used instead of a password to logon to z/OS applications.

IBM Multi-Factor Authentication for z/OS

Part III - Technical Information for IBM MFA

IBM MFA Services Started Task

- The IBM MFA services started task supports authentication of users and validation of tags specified in the RACF ALTUSER command at runtime.
- This started task must run in every z/OS instance sharing the RACF database where users will log on.
- The MFA Services address space:
 - Provides MFA main logic
 - Accesses MFA Data via SAF/RACF
 - Validates a user provided factor against RACF stored MFA Data
 - Validates user provided credentials using RACF MFA data and external MFA sources
 - Validates MFA data during administrator initiated provisioning
 - Provides an anchor for communications for factors
 - Tracks states for user authentication events
 - Provides cache of token credentials generated during Out-of-Band authentication

IBM MFA Web Services Started Task

- Required for:
 - IBM TouchToken registration
 - PIV/CAC - Certificate authentication
 - Out -of-Band authentication
 - For applications that replay credentials like sessions managers and DB2 Connect
- Not required for RSA SecurID
 - Unless you have applications that are replaying passwords (example: session managers / DB2 connect)
- Must run on only one LPAR in the SYSPLEX

Configuring IBM MFA Services started task

- Via Configuration Attributes Panel
- Execute AZFEXEC and enter STC

```
IBM Multi-Factor Authentication for z/OS
Started Task and Factor Administration

Command ==> STC

Configure Started Task
STC Started Task

Configure Factors
C  AZFCERT1 Factor
PT AZFPTKT1 Factor
S  AZFSIDP1 Factor
T  AZFTOTP1 Factor
```

- *Continued....*

Configuring IBM MFA Services started task

```
IBM Multi-Factor Authentication for z/OS
STC Configuration Attributes

Command ==> _____

MFA Services Started Task

Initial Trace Level . . . . . 2
Cache Token Sharing . . . . . C
Cache Name . . . . . RSPLEX05
Cache Entries . . . . . 1024
Server Port Number . . . . . 6790
```

Initial Trace Level

- 0 through 3 - higher number increases the level of verbosity.
- The default is 0 however, 2 is recommended during start up.

Cache Token Sharing

- This determines whether Cache Token Credentials (CTC) can be used on LPARs other than the one the Web Services started task is running on. Values are 'C' (Use Coupling Facility Notepad), 'N' (Not shared), & 'X' (Use XCF services. Recommended value in a plex if you have a coupling facility is to use 'C'.

Cache Name

- Must be always specified.

Cache Entries

- Must always be specified.
- An entry is stored for every CTC created until it is used (Reuse No) or the first sweep after it has been created.

Sever Port Number

- A listener port that facilitates internal communication between the IBM MFA web services task and the IBM MFA services started task.
- Choose a valid port.
- You can use the NETSTAT PORTLIST command to see which ports are currently in use.

Start the IBM MFA services started task using: **S AZF#IN00**

Configuring IBM MFA Web Services started task

- Via Configuration Attributes Panel
- Execute AZFEXEC and enter STC

```
IBM Multi-Factor Authentication for z/OS
Started Task and Factor Administration

Command ==> STC

Configure Started Task

STC Started Task

Configure Factors

C  AZFCERT1 Factor
PT AZFPTKT1 Factor
S  AZFSIDP1 Factor
T  AZFTOTP1 Factor
```

- *Continued....*

Configuring IBM MFA Web Services started task

MFA Web Services Started Task

```
Server Authentication Port. . . . 6789
Mutual Authentication Port. . . . 7890
Host Name . . . . . rs06.rocketsoftware.com
Document Root . . . . . /u/tskxb/usr/lpp/IBM/azfv1r2/htd
PKCS#11 Token Name . . . . . AZFTOTP.TOKEN
Enable Out of Band Services . . . Y
Enable TOTP Registration Services Y
Enable Certificate Authentication Y
Initial Trace Level . . . . . 3
```

Server Authentication Port – Listener

- For TouchToken and Out of Band.
- Enter the port number on which the IBM MFA web server is listening.
- The port must be configured for AT-TLS.

Mutual Authentication Port

- Required only if "Enable certificate authentication" is set to Y.
- Certificate authentication requires that AT-TLS be configured for client (mutual) authentication on a dedicated port.
- The port must be configured for AT-TLS using mutual authentication

Host Name

- Hostname of your web server.
- Must match the fully-qualified hostname of the system the IBM MFA web services started task is going to run and the ISPF session is running.

Document Root

- Identifies the directory from which MFA web services serves files.
- Enter the default of /usr/lpp/IBM/azfv1r2/htdocs, or your chosen value.

PKCS#11 token name

- Token to be used for cryptographic operations.
- Required for all web services.

• *Continued....*

Configuring IBM MFA Web Services started task

MFA Web Services Started Task

```
Server Authentication Port. . . . 6789
Mutual Authentication Port. . . . 7890
Host Name . . . . . rs06.rocketsoftware.com
Document Root . . . . . /u/tskxb/usr/lpp/IBM/azfv1r2/htd
PKCS#11 Token Name . . . . . AZFTOTP.TOKEN
Enable Out of Band Services . . . Y
Enable TOTP Registration Services Y
Enable Certificate Authentication Y
Initial Trace Level . . . . . 3
```

Enable Out of Band Services

- Set Y if you plan to use Out of Band.
- The default is N.

Enable TOTP Registration Services

- Set Y if you plan to use IBM TouchToken.
- The default is N.

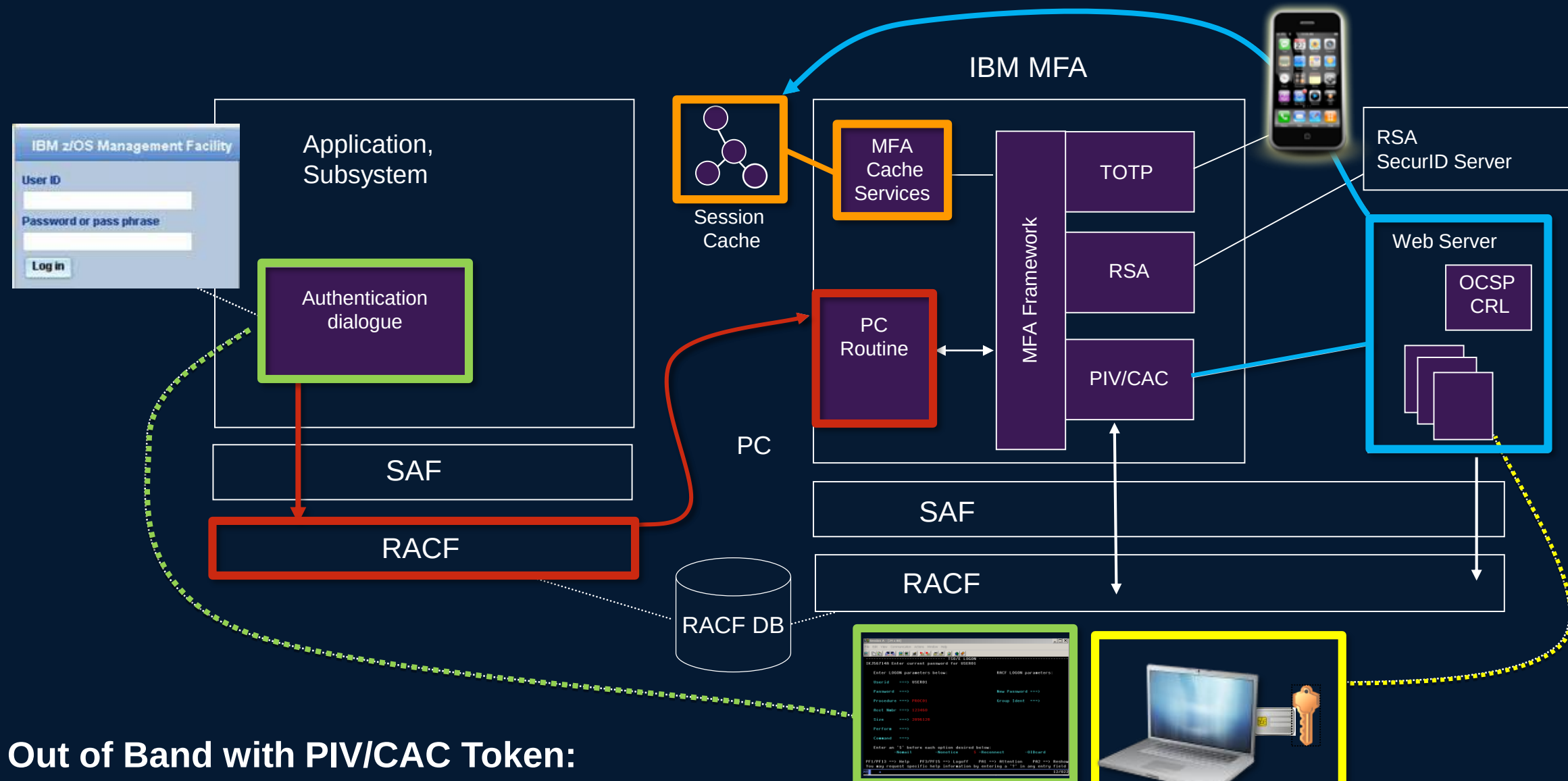
Enable Certificate Authentication

- Set Y if you plan to use PIV/CAC.
- Requires that out-of-band services also be enabled.
- The default is N.

Initial Trace Level

- 0 through 3 - higher number increases the level of verbosity.
- The default is 0 however, 2 is recommended during start up.

Start the IBM MFA web services started task using: **S AZF#IN01**



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

Thank you