IBM Multi-Factor Authentication for z/OS
A Product Review and Update

Julie Bergh jbergh@us.ibm.com
Ross Cooper

August 2016

A new z/OS product has become available…

- The new IBM Multi-Factor Authentication for z/OS has become generally available
  - Announced Feb 16th, 2016
  - General Availability March 25th, 2016
  - 5655-162 - IBM Multi-Factor Authentication for z/OS
  - 5655-163 - IBM Multi-Factor Authentication for z/OS S&S

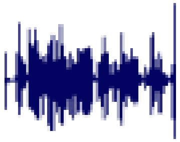
    Requires:
    - z/OS 2.1 or later
    - RSA Authentication Manager 8.1 or later for RSA ® SecurID® exploitation

- Now can enter Requests For Enhancements (RFE)
  - Strongly recommend that clients identify their requirements for IBM MFA through this channel, in addition to the discussions at this council.
    - In particular, please open RFEs for additional authentication tokens that are in use in your shop that would provide value if supported by IBM MFA for z/OS.

Multi-factor Authentication

- Multi-factor Authentication for z/OS provides a way to raise the assurance level of OS and applications / hosting environments by extending RACF to authenticate users with multiple authentication factors.

- Authentication Factors:
  - Something you know
    - A password / PIN Code
  - Something you have
    - ID badge or a cryptographic key
  - Something you are
    - Fingerprint or other biometric data



- Today on z/OS, users can authentication with:
  - Passwords, Password phrases, PassTickets, Digital Certificates, or via Kerberos

- Today's problem:
  - 2014 Verizon Data Breach Investigations Report said 2 out of 3 breaches involved attackers using stolen or misused credentials.
  - In the case of an attempted breach using comprised credentials, the extra protection that MFA provides can make the difference between having a secured vs. compromised system.
  - Breaches impact clients financially, their customers, and their reputations

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 OS and applications / hosting environments by extending RACF to authenticate individual users:
- Support for third-party authentication systems
  - RSA® Ready supporting RSA SecurID® Tokens (hardware & software based)
  - Direction to support the IBM TouchToken – Timed One time use Password (TOTP) generator token
  - Direction to support PIV/CAC cards - Commonly used to authenticate in the Public Sector enterprises
- Tightly integrated with SAF & RACF
  - RACF provides the configuration point to describe multi-factor authentication requirements down to a per User ID basis
  - Deep RACF integration for configuration and provisioning data stored in RACF database allowing seamless back-up and recovery

Typical Client Use Cases:

- **Enable higher- assurance user authentication** on IBM z/OS systems that use RACF for security
- Enable strong authentication for employees that carry **iOS devices** or **RSA SecurID** tokens

TECHNOLOGY RSA READY PARTNER

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

Achieve regulatory compliance, reduce risk to critical applications and data

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

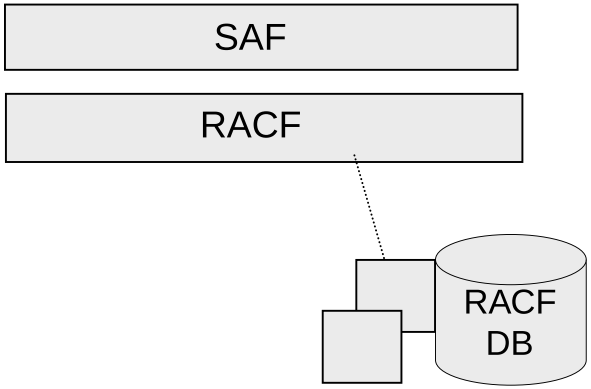
RACF & MFA Services and Related Support – Overview

- RACF 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
    - ISPF panels extended to support command extensions for MFA
  - Extensions to SAF programming interfaces
    - Provides a new SAF service for z/OS MFA Services allowing the access to MFA data stored in the RACF database
  - Auditing extensions
    - Tracks which factors 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
      - Related to the tokens used on a specific authentication event
- z/OS MFA Services started task
  - z/OS MFA address space which tracks state for user authentication events
  - Provides an anchor for communications for factors such as RSA SecurID
  - Extensible architecture to enable support for additional authentication factors

Base RACF Support for MFA Services

- RACF Database extensions
  - Store MFA information in RACF:
    - New MFA fields in the User profile
    - New MFA segment and General Resource profile class
- RACF Commands
  - Administration of MFA information in RACF
    - ALTUSER & RDEFINE / RALTER & RLIST
- RACF Logon processing
  - New MFA processing:
    - RACINIT SVC -- Calls MFA Manger during authentication processing to evaluate authentication factors
    - VLF Updates – Use MFA data in VLF object for fast ACEE access for MFA users
    - INIT_ACEE – Update ACEE cache

- SAF/RACF Database API
  Programmatic Access to RACF MFA data from the MFA Services started task:
  R_FACTOR – Access & update MFA data in RACF profiles
- Utilities
  - Support for new MFA segment data:
    - DBUNLOAD -- Report on MFA data
    - IRRADU00 – RACF SMF Unload

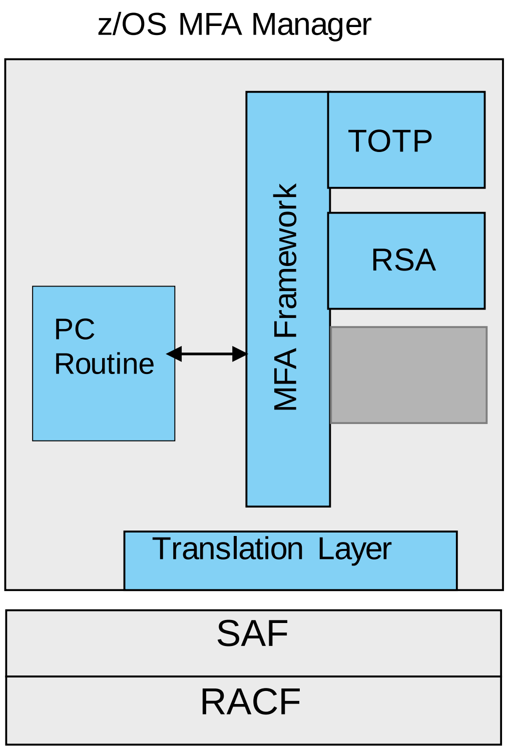


z/OS MFA Services Manager -- Components

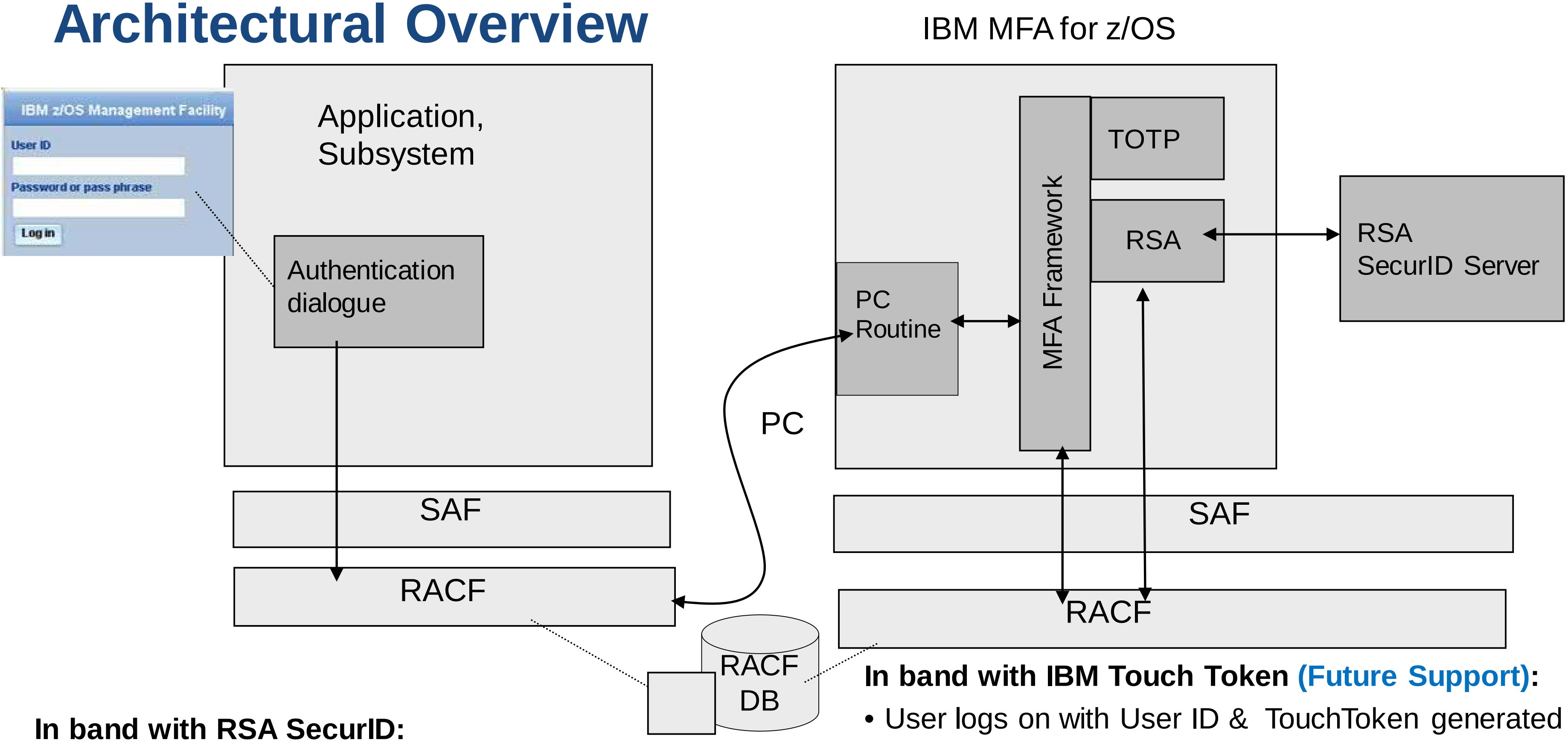
- MFA ISPF panels for management of authentication tokens

- 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 Data base access APIs



Architectural Overview



In band with RSA SecurID:

- User logs on with User ID & RSA SecurID Token and PIN
- RACF determines if the user is an MFA user & calls the MFA Services
- MFA Services calls RACF to retrieve user's MFA factor details
- MFA Server validates the users authentication factors and calls RSA Server
- RACF uses MFA Services status to allow or deny the logon

In band with IBM Touch Token (Future Support):

- User logs on with User ID & TouchToken generated on provisioned iOS device
- RACF Determines if the user is an MFA user & calls MFA Services
- MFA Server calls RACF to retrieve user's MFA factor details
- MFA Server validates the users authentication factors in this case the IBM TouchToken code
- RACF uses MFA Services status to allow or deny the logon

Authentication Factor Data Stored in RACF Profiles

- The RACF database will serve as the data repository for MFA data.

- MFA data will be accessed via RACF commands and via a SAF/RACF callable service.

- MFA User Specific 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 MFA Services
    - New RACF general resource class: **`MFADEF`**
    - Profile naming conventions: **`FACTOR.<factorName>`**

MFA RACF User Profile Management

- MFA Factor fields is stored in the RACF user profile
- Defined by a RACF Administrator via ALTUSER command

- Example ALTUSER Syntax:

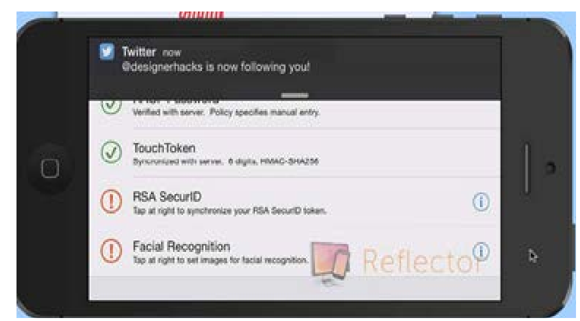
```
[ MFA(
      [ PWFALLBACK | NOPWFALLBACK ]
      [ FACTOR(factor-name) | DELFACTOR(factor-name)
      ]
      [ ACTIVE | NOACTIVE ]
      [ TAGS(tag-name:value …) ]
        | DELTAGS(tag-name … )
        | NOTAGS ]
)
| NOMFA ]
```

- RACF will call the MFA Services Task to validate the factor specific information that is specified on the ALTUSER command TAGS keyword
  - If a syntax error or unknown name value pair is supplied MFA Services will reflect an error to RACF
    - RACF issues a message and a MFA Services provided message which indicates the nature of the syntax error

Initial MFA Authentication Factors

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

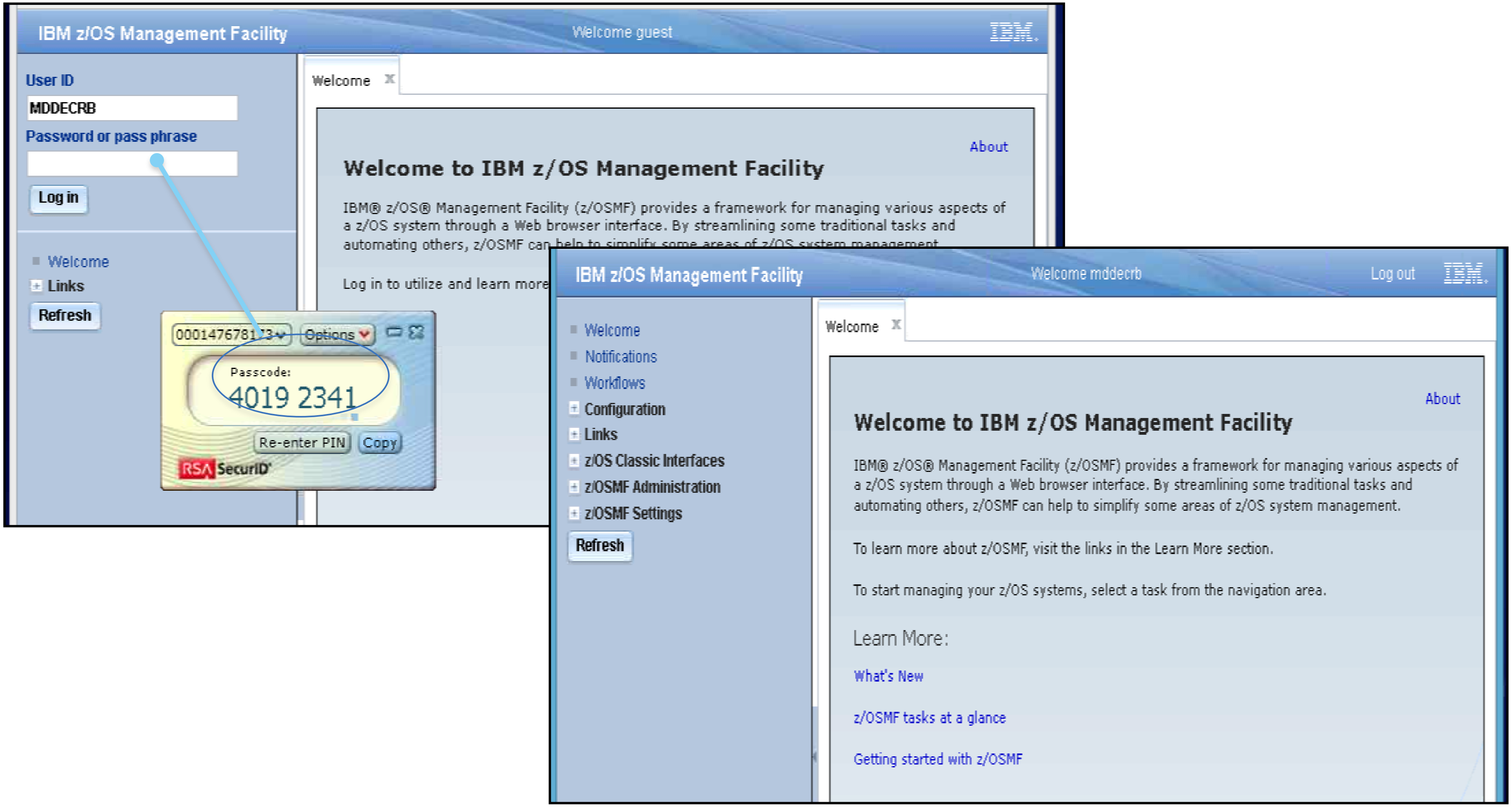
- IBM TouchToken – Timed One time use Password generator token – Post GA Delivery
  - Authentication factor that can be directly evaluated on z/OS to ensure that there is always a means of enforcing 2 factor authentication for users
  - Provisioned with a shared secret key into the iOS key ring
  - Granular – can have different shared secrets for different z/OS applications



Sample Logon Interaction with z/OSMF

Using Soft RSA SecurID Tokens

- User enters their User ID and token generated code in the password field.
  - The User's pin is not entered during logon processing



Statement of Direction for MFA Additional Authentication Factors & Support

PIV/CAC

- 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

zSecure Support

- Support is intended to simplify administration by helping to enforce authentication policy, providing alert notifications, and reporting on authentication audit events and compliance.

Selective MFA Application Exclusion

- The new RACF and IBM multi-factor authentication support will allow users to authenticate to z/OS applications with multiple authentication factors.

- Presently, 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
  - No password change field – MFA can use the password change field to change a RSA SecurID PIN during logon
  - PassTickets authenticators – presently not supported by MFA
  - 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 PassTicket

Selective MFA Application Exclusion

- Applications can identify themselves with an 'Application Name' (APPLID) parameter to SAF during authentication.
- A new profile will be used to indicate that MFA processing should be bypassed for a named application.
- When the user being authenticated has READ access to a profile containing the application name, MFA processing is bypassed.

```
RDEFINE MFADEF MFABYPASS.APPL.<applName>
```

- New Processing flow:
  - Only when a user has an ACTIVE MFA factor
  - Check if the user being authenticated has **READ** access to the profile name for the input Application.
    - If the user has **READ** access, MFA processing is bypassed.
    - If the user does not have **READ** access, MFA is required.

- MFA processing will be bypassed during authentication for the application for users on the access list with **READ** access. Those users will be able to authenticate with their password, password phrase or PassTicket.

Selective MFA Exclusion when APPLID not supplied

- Not all applications specify the with the APPLID parameter.
  - In this case VERIFY will user the Address space level security context – the ACEE User ID -- to identify the “application”, such as a started task.

- When the user being authenticated has READ access to a profile containing the address space level ACEE USER ID, MFA processing will be bypassed.

```
RDEFINE MFADEF MFABYPASS.USERID.<UserID>
```

- New Processing flow:
  - Only when a user has an ACTIVE MFA factor
  - Check if the user being authenticated has READ access to the profile name for the address space level ACEE User ID.
    - If the user has **READ** access, MFA processing is bypassed.
    - If the user does not have **READ** access, MFA is required.

- MFA processing will be bypassed during authentication for the 'application' for users on the access list with READ access. Those users will be able to authenticate with their password, password phrase or PassTicket.

MFA Policy 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 could be customized for different sets of users by permitting them a different level of access to the generic profiles.

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.

- Goal to allow the Security Administrator 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.PASSTICKET
ALTUSER JOEUSER MFA(FACTOR(PassTicket) ACTIVE)
```

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

Interim Planned Extensions
RACF & IBM Multifactor Authentication for z/OS

- Interim extensions are planned as SPEs for both IBM MFA and RACF

- z/OS MFA Services – Available with PI60774
  - Support for PassTickets as an authentication factor
  - Support MFA Application Exclusion/Inclusion policy
  - Support for IBM TouchToken TOTP authentication factor

- z/OS RACF Base support for MFA – Available with OA50016
  - Support for selective MFA Application Exclusion -- OA50016
    - Additional parameters passed from RACF to MFA services during authentication processing

  - z/OS IHS powered by Apache -- support for MFA – APAR PI62733
    - New MFA mod_saf_mfa module support – shipped by the IBM MFA product
    - Extensions to Apache mod_authnz_saf – shipped by z/OS Apache
    - Dependency on z/OS Unix kernel APAR

Cross Component Service and Updates supporting IBM MFA

Product /Component	APAR / Service level	Comments
SAF	OA48650	SAF enablement for MFA
RACF	OA48359	RACF enablement for MFA
zSecure Admin/Audit	OA50009	
zSecure Command Verifier	OA50011, OA50012	
zSecure RACF-Offline	OA50012	
CL/SuperSession	OA49597	CL/Supersession V2.1
OTELNETD	PI57945	Add support for 16 character long passwords
z/OS ITDS	OA50078	Allow the forward slash (/) in password specification on bind
z/OS UNIX	OA50245	Apache MFA support, when available.
TKE 8.1	With maintenance MCL002 in the P08469 EC. Also provides support for password phrases.	Requires ICSF HCR77B0 or HCR77B1 with APAR OA49811
TKE 8.0	With maintenance MCL005 in the N98850 EC. Also provides support for password phrase.	See Above
IBM HTTP Server on z/OS		Support for IBM MFA mod_saf_mfa module -- prevents MFA credential. Replay. Support for Apache code base V9 & V8.5

Questions?