New York RACF Users Group / Tampa RACF Users Group

RACF Update: Multi-Factor Authentication Update

Ross Cooper, CISSP ®
z/OS Security Server Design and Development
IBM Corporation

rdc@us.ibm.com

October 18th, 2016

Multi-Factor Authentication

- **Raise the assurance level of z/OS:**
  - How confident are you that the users of your system are who they claim to be?
- **The problem with passwords:**
  - Common passwords, Reuse passwords
  - Write down passwords
  - Unintentionally install malware and key log
  - Password cracking

Multi-Factor Authentication

- **Multi-Factor Authentication provides a way to raise the assurance level of OS and applications / hosting environments by authenticating users with multiple factor types.**

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

- **Multi-Factor Authentication:**
  - By requiring multiple authentication factors, a user's account can not be compromised even if one of their factors is discovered.
  - 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

Multi-Factor Authentication

- **RACF updated to add new MFA fields and MFA logon processing**
- **IBM Multi-Factor Authentication for z/OS (IBM MFA) – New Product**

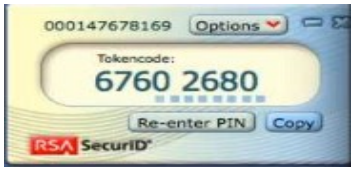
- **Tightly integrated with RACF with RACF extensions to support IBM MFA**
  - User related commands that RACF administrators know and love ❤
  - Definition of acceptable authentication token types in RACF
  - Allow the provisioning and definition of the MFA token types per user
  - Deep RACF integration for configuration and provisioning data stored in RACF database allowing seamless back-up and recovery
  - Auditing extensions leveraging existing SMF infrastructure
    - Tracks that MFA was used during the authentication process for a given user for ease in compliance reporting
  - IBM MFA Infrastructure provides architecture that can easily add new authentication methods

Multi-Factor Authentication

- **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 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
  - Direction to support PIV/CAC Smart Cards
    - Commonly used to authenticate in the Public Sector enterprises

- **Client Use Cases:**
  - Enable higher-security logins for users with administrator privileges or access to critical data and processes
  - Enable strong authentication for employees that carry iOS devices or RSA SecurID tokens



Multi-Factor Authentication

- **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
    - Definition of authentication token types
  - **Extensions to authentication processing**
    - Allows supported tokens to be specified during user authentication requests
  - **Auditing extensions**
    - Tracks MFA used during the authentication process for a given user
  - **Utilities**
    - RACF Database unloads 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

- **IBM MFA started task**
  - IBM MFA address space which tracks state for user authentication events
  - Provides an anchor for communications for factors such as RSA SecurID

User Provisioning for MFA

- MFA user provisioning is performed on a user by user basis with the **ALTUSER** command.

- **ALTUSER Syntax:**

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

     )
| NOMFA ]
```

- **Note:** RACF will call the MFA product 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

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:**

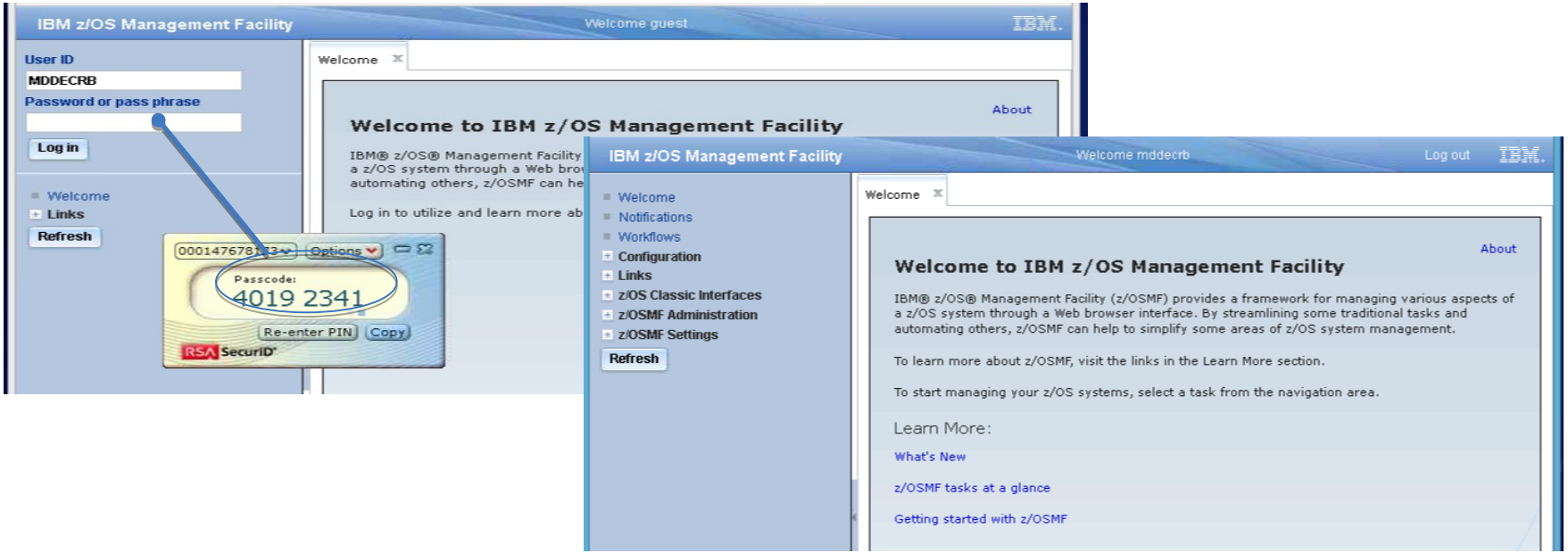
```
ALU JOEUSER MFA(FACTOR(AZFSIDP1) ACTIVE TAGS(SIDUSERID:JOE1) PWFALLBACK)
```

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

- **User is provisioned:**
  - JOEUSER can now authenticate to RACF with a RSA SecurID token.

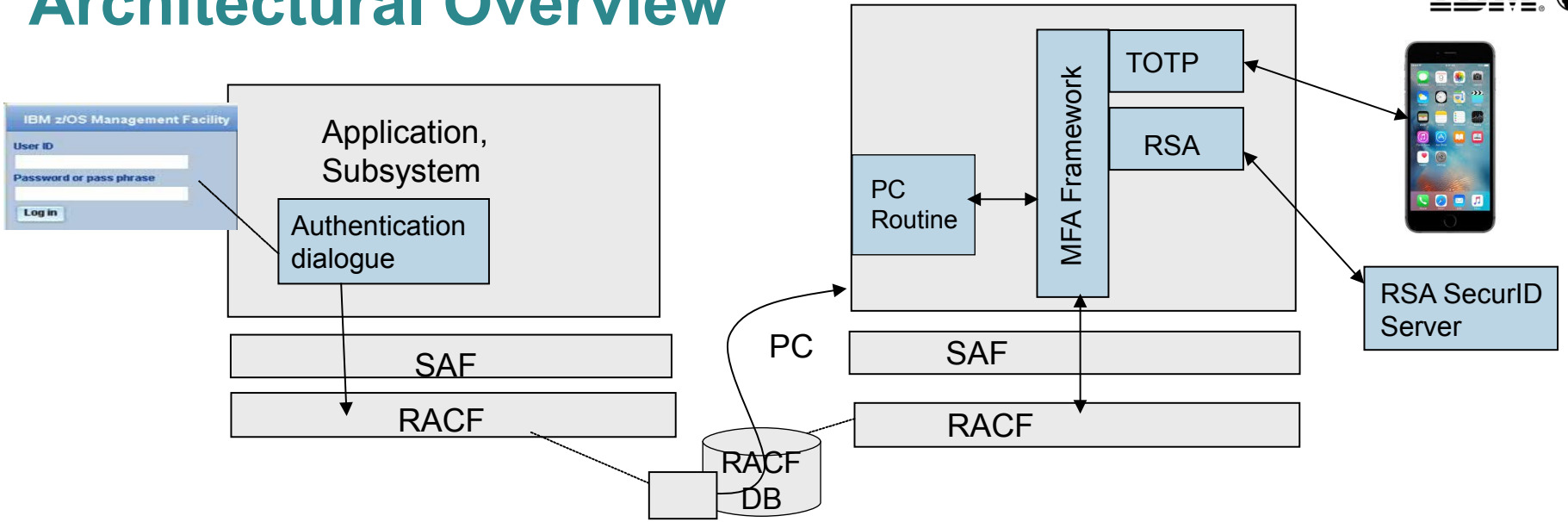
Sample Logon Interaction with z/OSMF

- **Using Soft RSA SecurID Tokens:**
- User enters their User ID and token generated code in the password field
  - User's pin entered on token generator, not during logon processing



9

Architectural Overview



Logon with RSA SecurID:

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

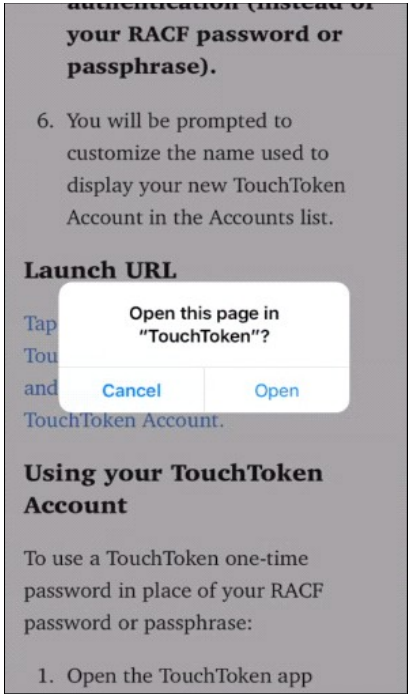
Initial MFA Authentication Factors

- **RSA SecurID Tokens**
  - Requires RSA SecurID server configured to the MFA Server
  - RSA SecurID requires an external configured server
  - Supports both hard and soft RSA SecurID tokens

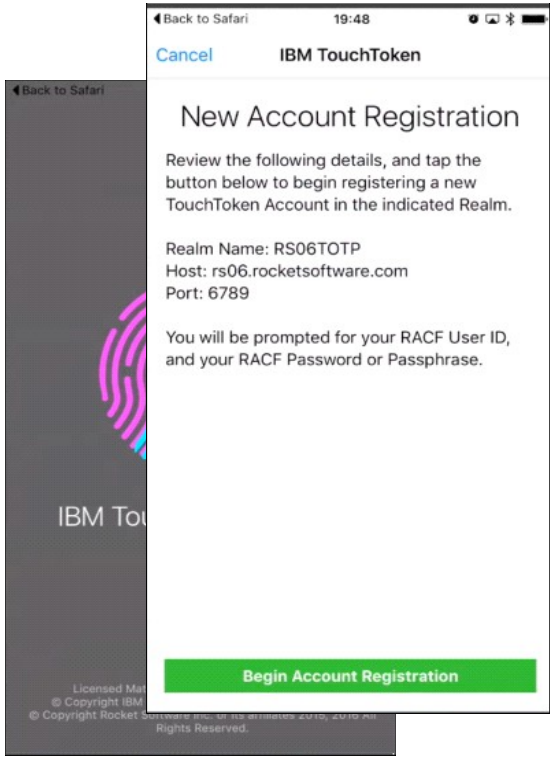
- **IBM TouchToken – Timed One time use Password generator token - *NEW***
  - Authentication factor that can be directly evaluated on z/OS
    - Helps to ensure that there is always a means of enforcing two factor authentication for users
  - Provisioned with a shared secret key into the iOS key ring from z/OS

IBM TouchToken – User Registration

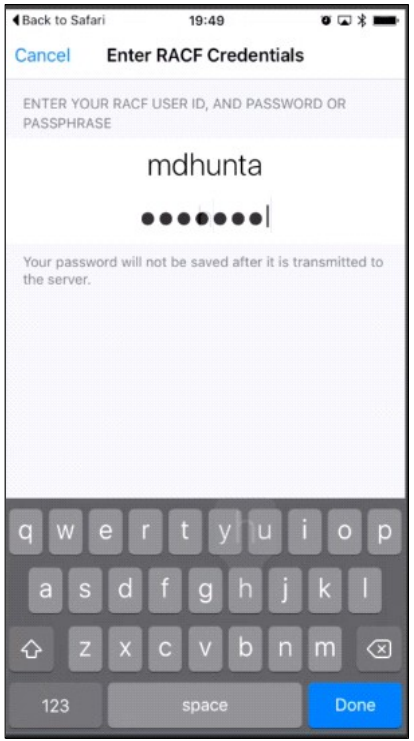
IBM MFA Admin sends user an enrollment email



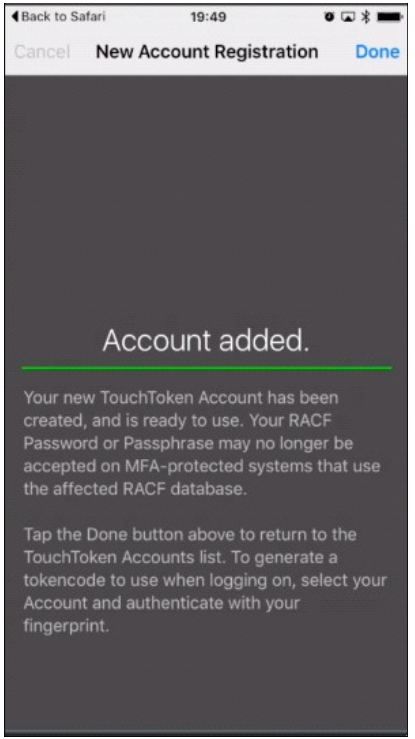
Link opens in the TouchToken iOS App



User authenticates with RACF credentials

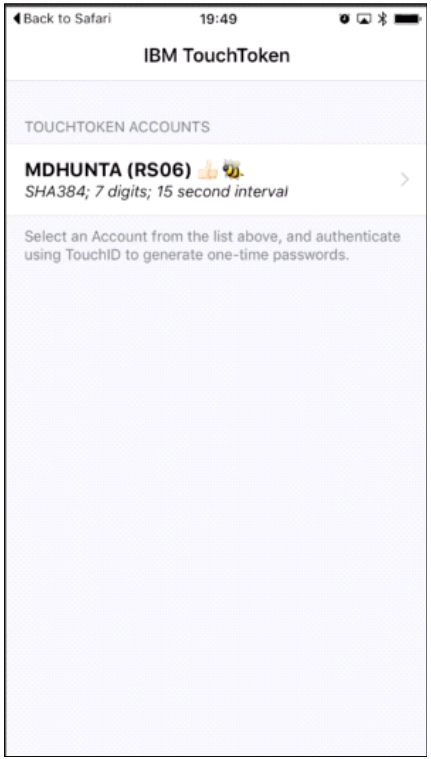


Registration Complete

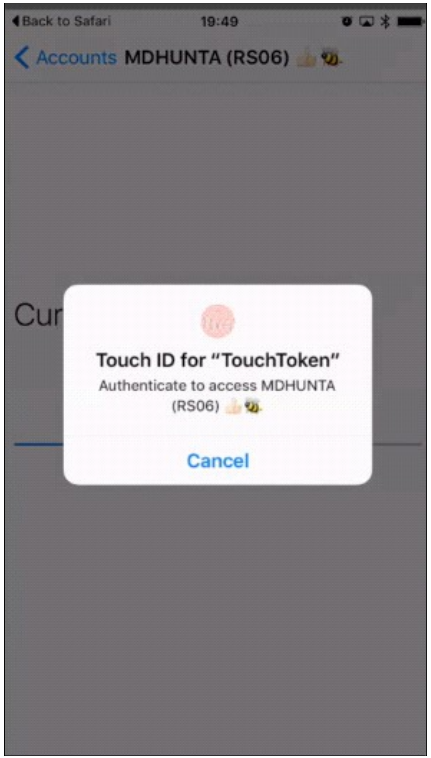


IBM TouchToken – Token Generation

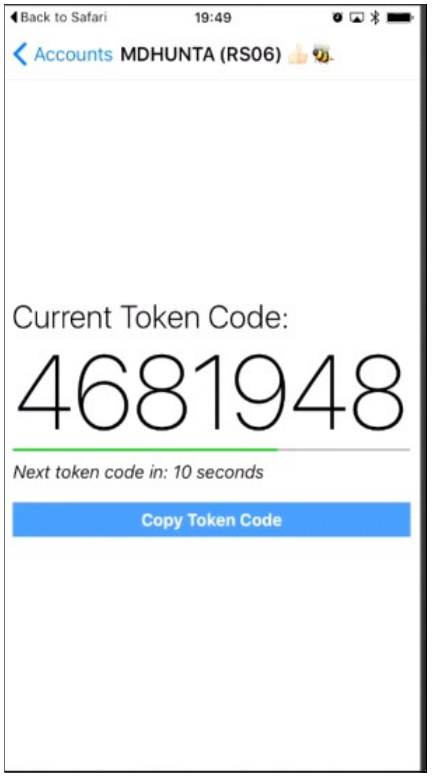
List of TouchToken Acounts



User selects an account and authenticates with Touch ID

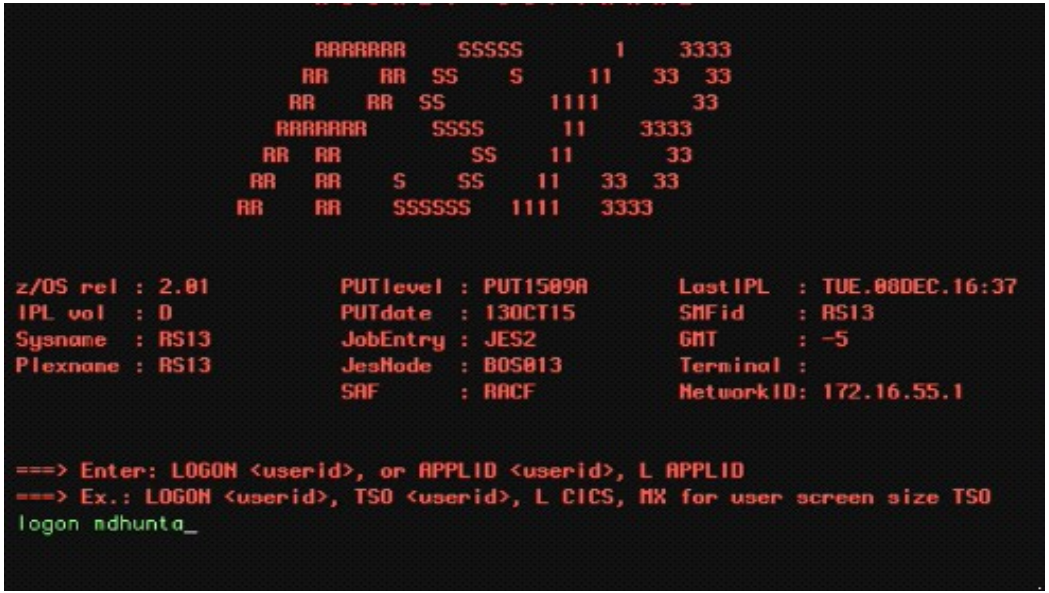


TouchToken Token Code

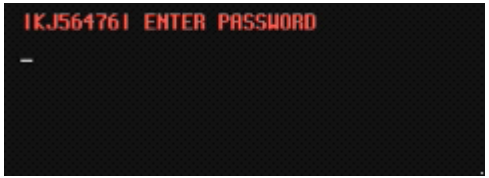


IBM TouchToken – User Logon

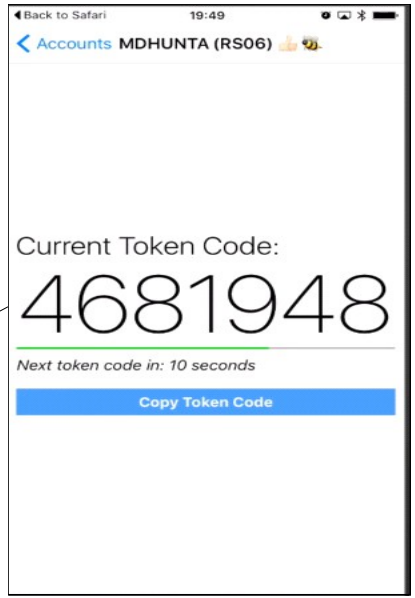
- Start the logon process



- TSO Prompts for the password

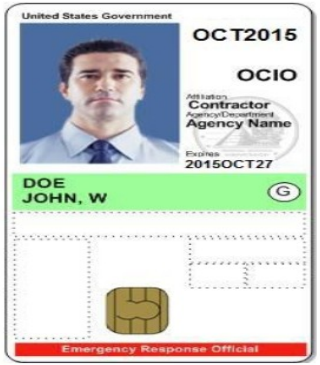


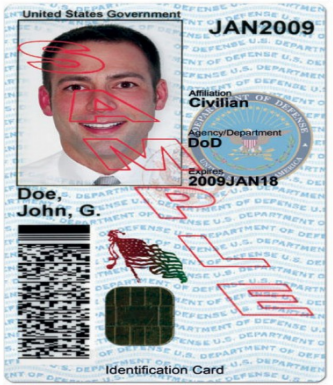
- Use the TouchToken Application to obtain a logon Token Code:



MFA Future Authentication Factors

- **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.
- **Others?**
  - Other MFA systems?





MFA Application Bypass - *NEW*

- The RACF and IBM Multi-Factor Authentication for z/OS support allows users to authenticate to z/OS applications with multiple authentication factors.

- Previously, multi-factor authentication was enforced for all applications for MFA provisioned users.
- Unfortunately some applications have authentication properties which can be problematic for MFA:
  - **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
  - **PassTickets authenticators** – previously not supported by MFA

- 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

MFA Application Bypass - *NEW*

- 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 Authentication Flow:**
  - When a user has an ACTIVE MFA factor
  - IBM MFA checks if the user being authenticated has **READ** access to the application bypass profile
    - 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 Application Bypass - *NEW*

- Not all applications specify the APPLID parameter during authentication.
- In this case VERIFY will use 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 Authentication flow:**
  - 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 Application Bypass – Examples...

- The MFA bypass profiles can be configured to require MFA by default or bypass MFA by default depending on the access level given to a generic MFABYPASS profile.
- **Profiles 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

- **Profiles 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 permitting them a different level of access to the generic profiles.

MFA PassTicket Support - *NEW*

- 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.

- Allow the Security Administrator indicate that an MFA user can authenticate with a PassTicket in place 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.

MFA Various RACF Updates:

- **New SMF Type 80 event code 1(RACINIT) Relocate 443:**
  Details of authenticator types – User authenticated with Password / Phrase / MFA / PassTicket

- **DBUNLOAD:**
  Unloads the new MFA fields

- **R_Admin:**
  Supports set / extract of the new MFA fields

- **Messages:**
  ICH408I – Indicates Multi-Factor Authentication failure

- **ACEE:**
  New flags to indicate user authenticated with MFA

Requirements?

- **We want to hear from YOU!**
- **You can submit your own requirements via RFE:**
  - https://www.ibm.com/developerworks/rfe
- All requirements are reviewed by the RACF development team.

More Information...

- **z Systems** - http://www-03.ibm.com/systems/z/
- **z13s Announce** - http://www-03.ibm.com/systems/z/hardware/z13s.html
- **IBM MFA** - http://www-03.ibm.com/systems/z/os/zos/multifactor-authentication.html
- **z/OS** - http://www-03.ibm.com/systems/z/os/zos/
- **IBM Enterprise Security** -
  - http://www-03.ibm.com/systems/z/solutions/enterprise-security.html
- **Techdocs -** http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs
  - **Keywords:** Crypto, TKE, ICSF
- **Redbooks** - http://www.redbooks.ibm.com/

Questions?