IBM education Assistant (IEA) for z/OS V2R3

RACF - Multi-Factor Authentication (MFA)

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

- Multi-Factor Authentication support is now available to raise the level of assurance of z/OS systems and hosting environments.
  - MFA Overview
  - RACF and IBM Multi-Factor Authentication for z/OS
  - User provisioning
  - User experience
  - Architectural overview
  - Supported factor types
  - Options

Overview

- **Problem Statement / Need Addressed:**
  - Authentication with passwords has flaws:
    - 1,429 Incidents in 2015 with confirmed data disclosure as a result of stolen credentials
    - 63% of breaches are due to weak, default or stolen passwords
    - $4 Million – Average total cost of a data breach
  - Problems with passwords:
    - Common / weak passwords
    - Password reuse
    - Write down passwords
    - Malware and Key loggers
    - Password cracking
- **Solution**
  - Multi-Factor Authentication: Authenticate users with multiple factors
- **Benefit / Value**
  - Reduce the attack surface of your z/OS systems

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.

Multi-Factor Authentication

- 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 & RACFsadf
  - 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

MFA 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

RACF MFA 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 use
  - **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)
```

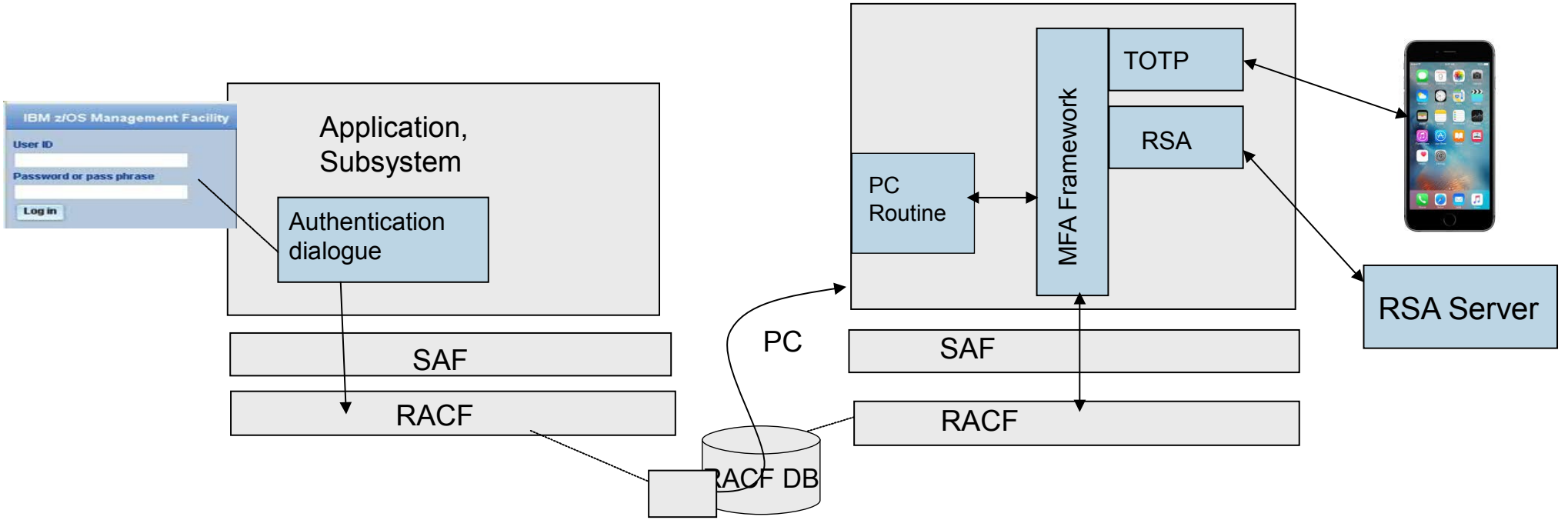
  - Adds factor to the user
  - Activates the factor – JOEUSER is now required to authenticate to RACF with MFA credentials
  - Adds a factor specific tag – SIDUSERID – Associates RSA SecurID user ID with z/OS user ID
  - Password fallback – When MFA is unavailable, the user can logon with their password / phrase

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

RSA 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

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

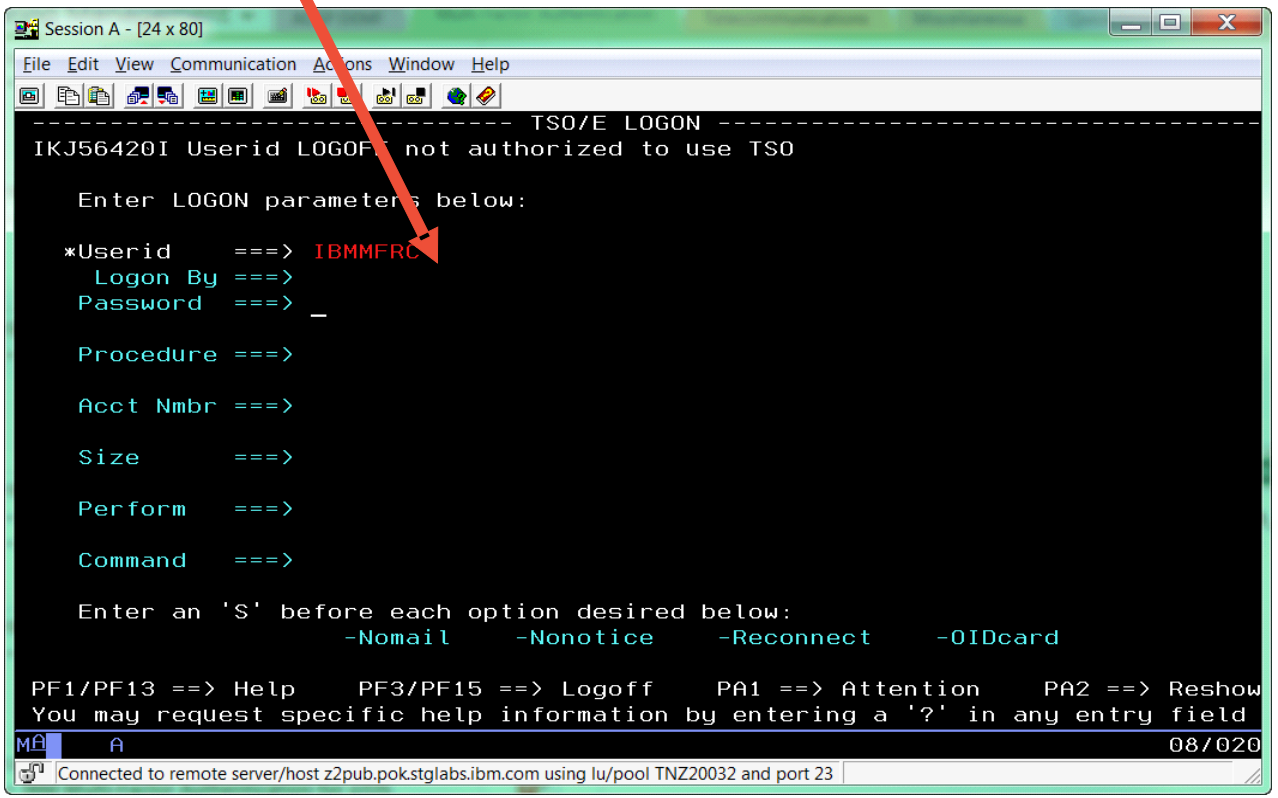
Using Soft RSA SecurID Tokens

- 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

Using Hard RSA SecurID Tokens

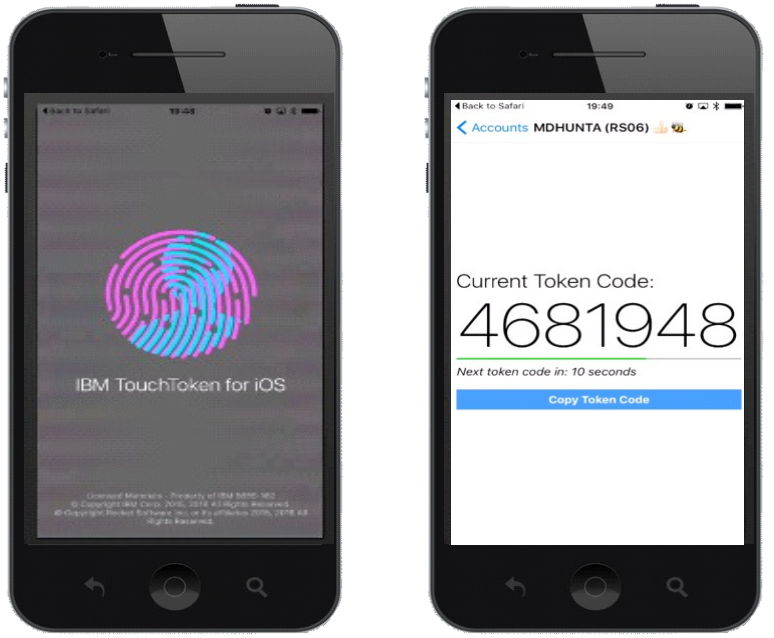
- PIN Code: 1234

123159759

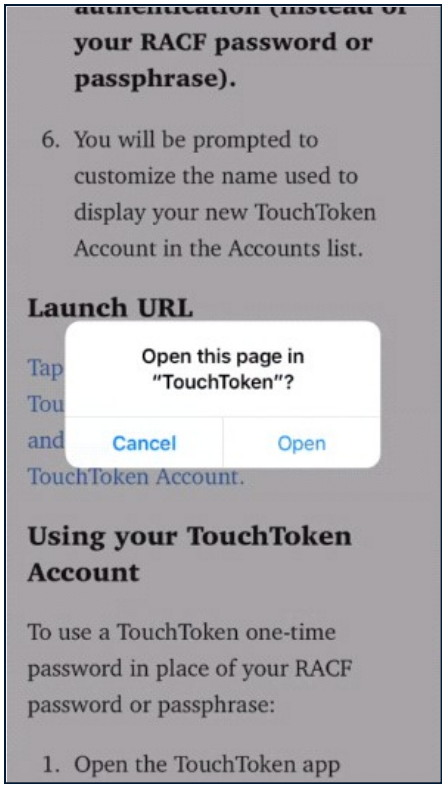


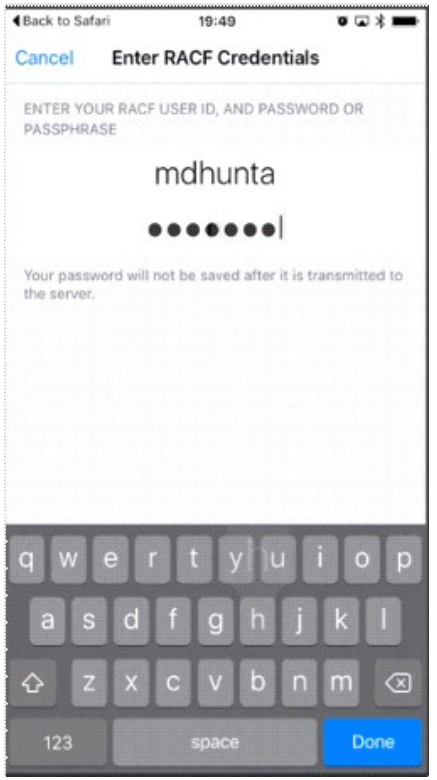
IBM TouchToken – Timed One Time Use Password Generator

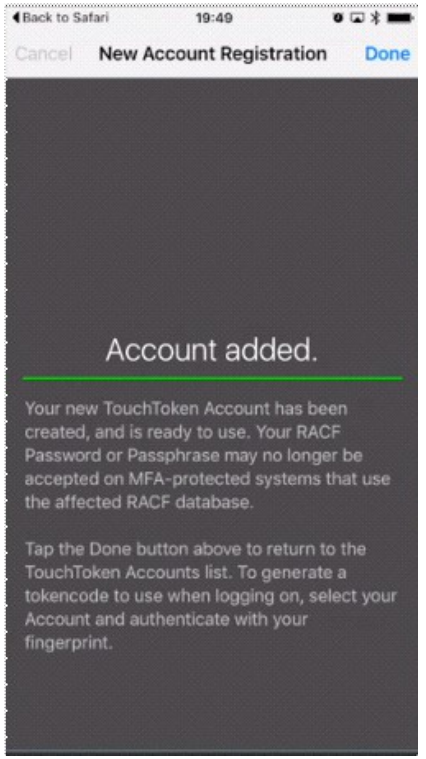
- Authentication factor that can be directly evaluated on z/OS to ensure that there is always a means of enforcing 2 factor authentication for users
- Provisioned with a shared secret key into the iOS key chain
- Does not rely on an external server, eliminates an external point of failure



Using IBM TouchToken for iOS – Registration





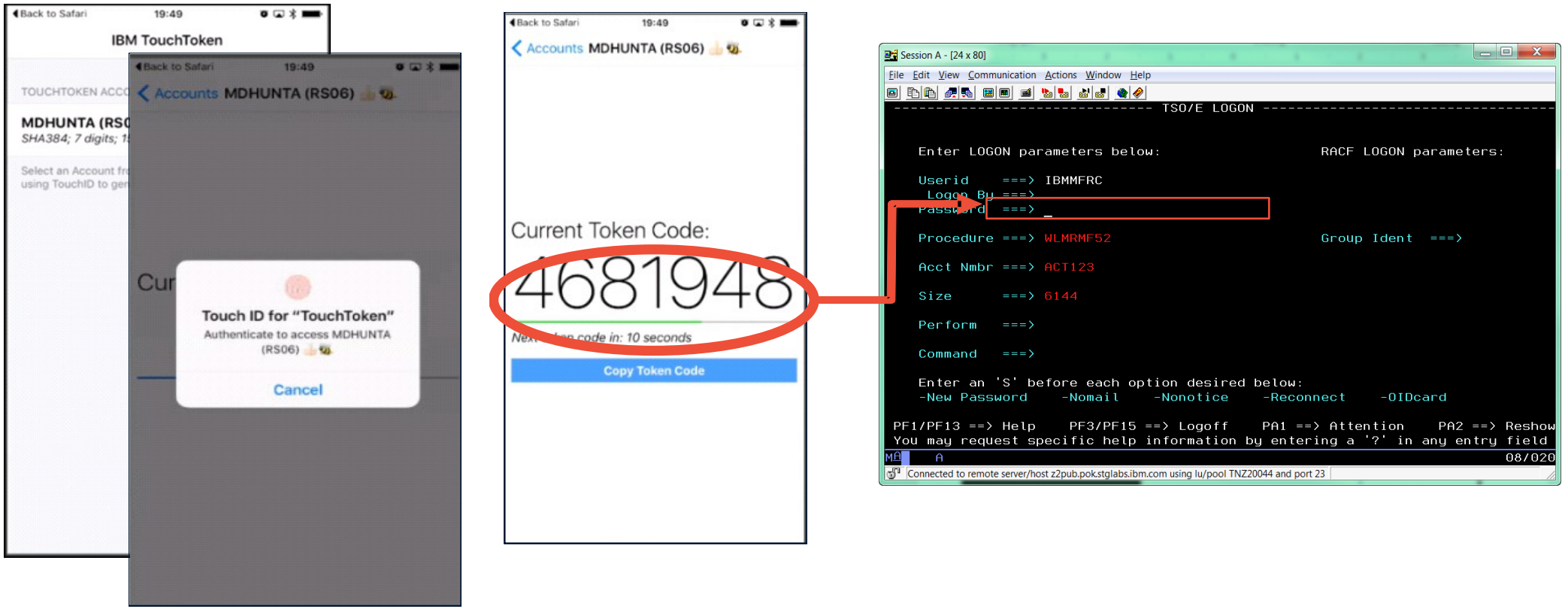


1) RACF admin sends registration email to user

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



1) User selects the account that a IBM TouchToken will be used for Authentication

2) Authenticates with Touch ID

3) IBM TouchToken app access the iOS key chain to generate a TouchToken code

4) User enter TSO user ID and current token

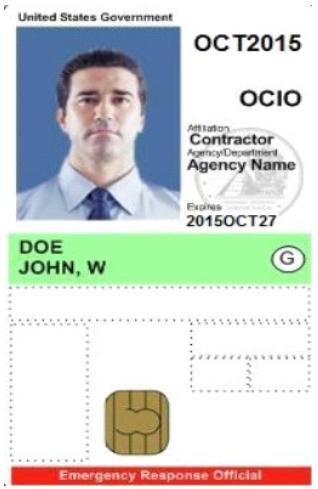
MFA Out-of-Band Support

- **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**

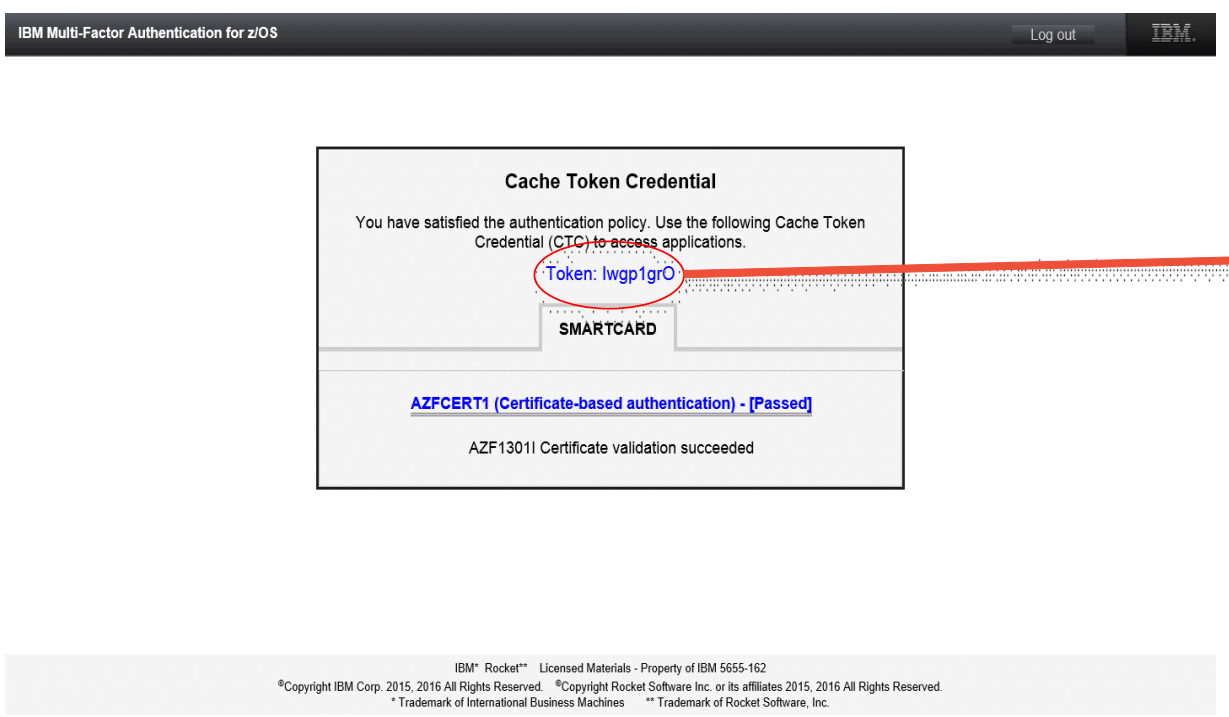
- **Out-of-band authentication allows for a number of improvements to IBM MFA & RACF**
- Allows greater control over the user authentication experience
  - e.g.: Via webpage, mobile smartphone app, or other future supported token types
- Supports factor types which are not well suited to text entry
  - 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

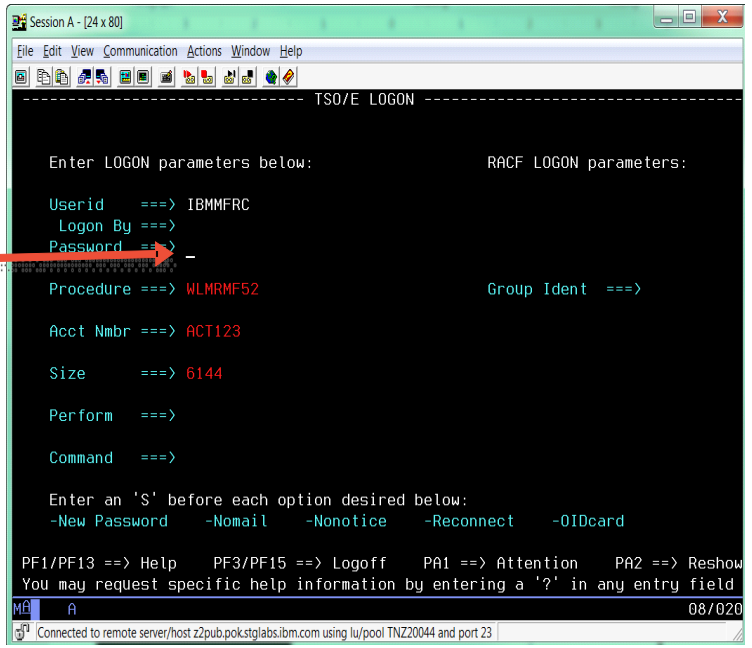
IBM MFA PIV / CAC / Smart Card Support

- 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



Using Smart Card 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.
  - Session Manager Applications
- 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**
  - 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.

IBM MFA Product Details

- IBM Multi-Factor Authentication for z/OS (5655-162)
- IBM Multi-Factor Authentication for z/OS S&S (5655-163)
- **2016:**
  - **March 25** - IBM MFA V1.1 General Availability
  - **June** - Functional Enhancements for IBM TouchToken and Application Bypass
  - **November 18** - IBM MFA V1.2 General Availability

Computer Associates Support

- **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.

- Message to Clients:
  - Check with CA Technologies support for the most current information.

Interactions & Dependencies

- **Software Dependencies**
  - RSA Authentication Manager 8.1 or later for RSA® SecurID® exploitation
- **Hardware Dependencies**
  - None
- **Exploiters**
  - In general, applications which authenticate users with RACROUTE do not need to be updated to use MFA.

Migration & Coexistence Considerations

- When a user is provisioned for MFA authentication and the RACF DB is shared with a system that does not have the MFA support installed or configured that user can continue to authenticate with their RACF password / phrase on that system.

Installation

- **RACF APARs**
  - **MFA V1.1 - RSA:** OA48359, OA48650
  - **TouchToken Support & Application Bypass & Passticket:** OA50016
  - **Out of Band & Smart-Card:** OA50930, OA50931

- **IBM MFA Product**
  - IBM Multi-Factor Authentication for z/OS Installation and Customization
    - Contains full description of the installation and customization steps.
    - **Example Steps:**
      - Sysprog Steps:
        - Copy and customize jobs
        - Authorize Load Library
        - Update SCHEDxx PARMLIB program properties
      - RACF Admin Steps:
        - Define user for AZF started tasks
        - Define profile in STARTED class
        - RACLIST and ACTIVATE MFADEF class
        - Define and authorize factor profiles
      - Configure IBM MFA STC
        - ICSF Setup: Configure a PKCS#11 Token
        - Configure AT-TLS profile
        - Configure MFA STC Panel
      - Start the IBM MFA started task
      - … And More...

Session Summary

- IBM Multi-Factor Authentication is now available!
- z/OS V2.1 and up
- RSA SecurID, TouchToken and PIV / CAC / Smart Card Logon
- Taking requirements for additional MFA Authentication Mechanisms

Appendix

- **Introduction to IBM MFA:**
  - http://www.ibm.com/support/knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.azfu100/azf_server.htm
- **IBM MFA Solution Brief:**
  - http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSS03139USEN
- **IBM Multi-Factor Authentication for z/OS V1.2 Announcement Letter:**
  - http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSS03139USEN
- **IBM MFA Publications:**
  - http://www-03.ibm.com/systems/z/os/zos/library/bkserv/v2r2pdf/#AZF