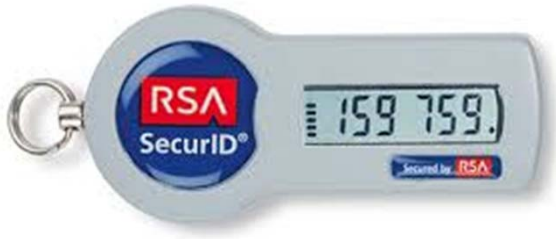
# Experiences with Two Factor authentication on z/OS

WELLS FARGO

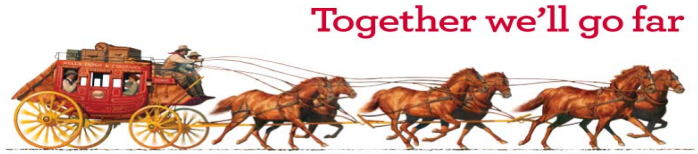
## Georgia RACF Users Group




## 11 May 2017

Simon Dodge

Principal Engineer,
zSeries Security Engineering



# Session agenda

- **Why** would you want this ?
- **Which** users should be 2FA ?
- **Configuration**
  - Initial POC with AddOn product for TopSecret Q4 2015
  - IBM, CA announced MFA support Q1 2016
  - 2nd testing with native TopSecret support Q4 2016
  - Many similarities with RACF
- **Lessons learned**:
  - Exactly who do you want to target for 2FA (Privileged users ?)
  - Need to support PassPhrases to allow PIN+token  entry
  - Session Managers need to use PassTickets
  - Some PTFs still “in the works”

# Session agenda

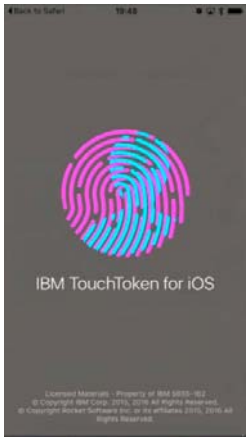
- **Why** would you want this ?
- **Which** users should be 2FA ?
- **Configuration**
  - Initial POC with AddOn product for TopSecret Q4 2015
  - IBM, CA announced MFA support Q1 2016
  - 2nd testing with native TopSecret support Q4 2016
  - Many similarities with RACF
- **Lessons learned**:
  - Exactly who do you want to target for 2FA (Privileged users ?)
  - Need to support PassPhrases to allow PIN+token  entry
  - Session Managers need to use PassTickets
  - Some PTFs still “in the works”

# Multi-Factor Authentication - MFA

Multi-Factor Authentication provides a way to raise the assurance level by authenticating users with multiple factors


Authentication Factor 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


From: RACF Update: MFA 18Oct2016 Ross Cooper, IBM

# Two Factor: Why ?

- Certain users on z/OS represent *significant* risk if password is disclosed/exposed
  - Even with short password interval, timeframe is wide, risk high for some users
  - How well can you be assured of no password compromise ?
    - Social engineering
    - Copy of security database – offline brute force attack
  - You need to understand potential target users
- We wanted to explore 2FA on z/OS before it was mandated
  - By Regulators or Internal policy
  - At the time, no ESM offered direct support for 2FA (2015)
  - IBM, CA announcements Q1 2016
- Opinion: In the future, password technology will become obsolete
  - So prepare yourself

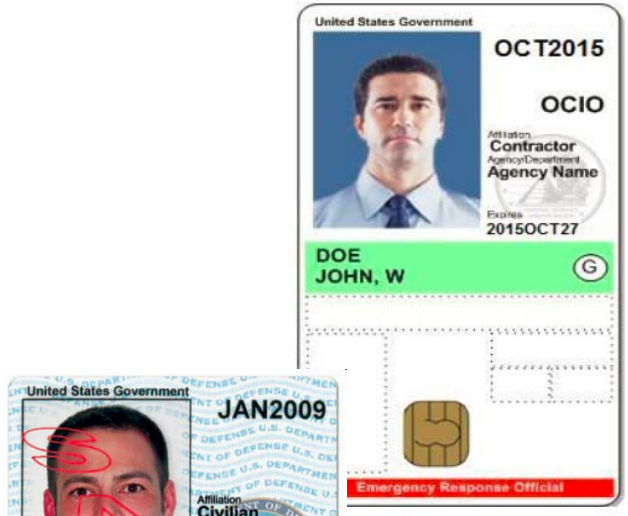
# Multi-Factor Authentication – Future/Soon

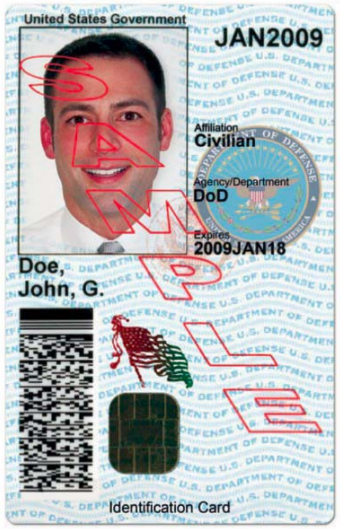
IBM and CA have both announced that they intend to support **SmartCards**: PIV/CAC format

- Personal identity verification (**PIV**)
- Common Access Card (**CAC**)

are both for United States Federal Government smart cards.

They are standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel




From: RACF Update: MFA 18Oct2016 Ross Cooper, IBM

# Two Factor: Which users ?

- User with certain system related ‘privileges’
  - Generic term “Privileged users” is like a piece of string
  - Each business needs to have their own definition of Privileged

- We have a **Tiering matrix** that defines/classifies resource access into 4 tiers based on risk to enterprise:
  - **Privileged** access: Security admins, Sysprogs (Parmlib/APF update etc)
  - **Elevated** access: Power users, subsystem admins (CICS, DB2, MQ etc)
  - **Regular** access: Most normal business functions
  - **Default** access: Time accounting etc

# Privileged users

- Poll the audience:
  1. Do YOU have a list of what you consider Privileged ?
  - We probably wont agree, that's normal
  - WHAT makes sense to your organization ?
  - How often do you review it ?
  - How often do you determine which users have privileges (daily)

# Privileges 1 of 2

- Some possible examples (we have 25+)
  - Security administration (Create users, Permit access)
  - APF update
  - Other sensitive dataset UPDATE
  - Confidential data READ (Security database)
  - OPERCMDS that change configuration
  - Some UNIXPRIV resources
  - SURROGAT.. All? Some ? Discrete/Generic

# Privileges 2 of 2

- Sub system admin
  - DB2 – SYSADM, SYSOPER etc
  - CICS – CEDA/CEDB,  CMD/SPI CREATE/DISCARD
  - CICS – Update to DFHRPL datasets
    - Do you even monitor what they are ?
  - etc

# MFA - Relatively easy install

- Configure ESM to communicate to RSA server
- Define MFA ‘factors’ and associate users
- **No software changes needed to RACROUTE caller**
  - Caller is unaware that user keyed in token value vs passphrase
- Consider enabling *applications* for PassPhrase support
  - TSO
  - CICS
  - TPX (Session manager)
  - etc

# PassPhrases

- Applications need to be “PassPhrase ready”
  - TSO
  - CICS  (CESL vs CESN)
  - TPX

- Implications of *not* having PassPhrases active
  - Max password of 8 is too short for PIN+token
  - You can use soft tokens that display 8 digit token value

# MFA - BCP

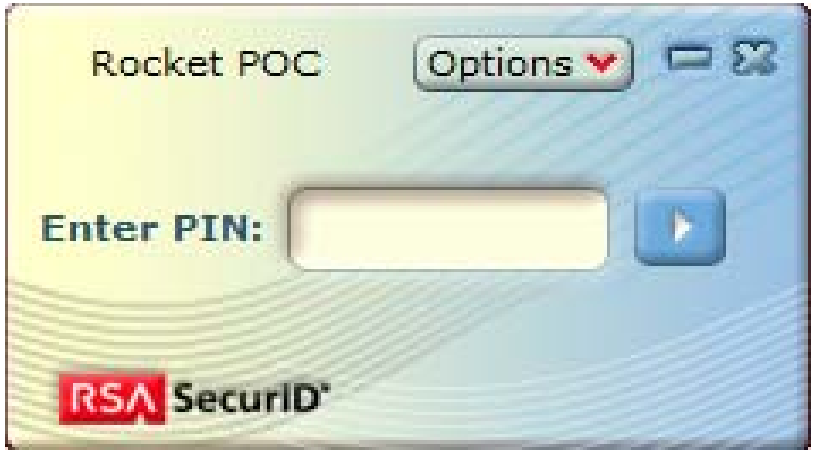
- Your z/OS BCP now needs to require RSA authentication server
  - Available and connected

# Authentication server unavailable

- You need to consider how to behave if unable to connect to RSA
  - Allow a password authentication ? (fallback)
  - Consider early stages of IPL, before TCPIP active
  - Consider tool to generate PassTicket
  - Even with fallback, may not remember password

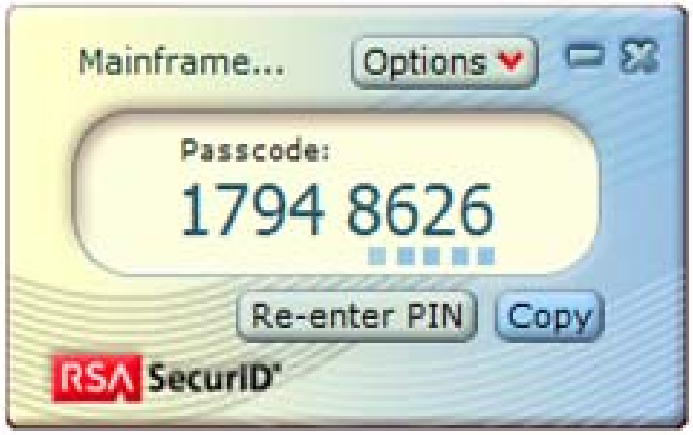
# Soft Token

- Installed on Windows device
- Prompt for a PIN when started and after 3 token displays



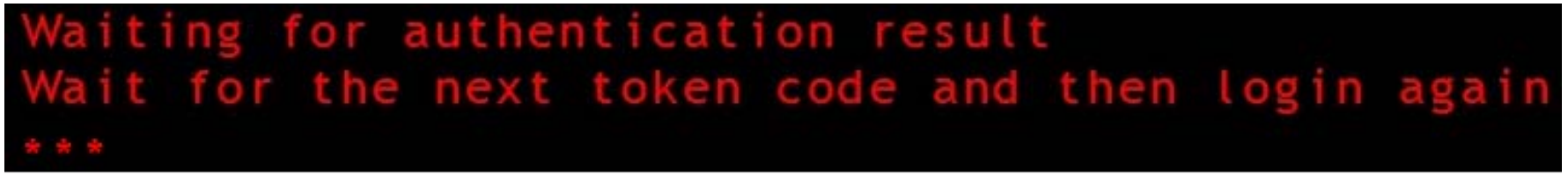
# Soft Token

- 8 digit token value displayed after you enter a PIN
  - Will be valid if you entered correct PIN
  - Will not work if you entered wrong PIN
  - IE soft token does not validate PIN



# “Next token” mode

- Sometimes happens after nn bad attempts
- RSA isn’t simple 3 strikes, you get extra chance to try again



# Configuring MFA on RACF

- SETR CLASSACT(MFADEF)
- RDEFINE MFADEF FACTOR.AZFSIDP1 for RSA

```
ALU SIMON MFA(FACTOR(AZFSIDP1)
              ACTIVE
              TAGS(SIDUSERID:SDODGE)
              PWFALLBACK))
```

From: RACF Update: MFA 18Oct2016 Ross Cooper, IBM

# Configuring MFA on RACF

- `RDEFINE MFADEF FACTOR.AZFPTKT1 for PassTickets`

`ALU SIMON MFA(FACTOR(AZFPTKT1) ACTIVE )`

From: RACF Update: MFA 18Oct2016 Ross Cooper, IBM

# Configuring MFA on RACF - future

- `RDEFINE MFADEF FACTOR.xxxxx  for Next factor`

```
ALU SIMON MFA(FACTOR(XXXXX) ACTIVE )
```

# ALTUSER syntax

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

  | NOMFA ]
```

From: RACF Update: MFA 18Oct2016 Ross Cooper, IBM

# SMF 80 update – new section 443

- Event code 1 (authentication) has new relocate *section* 443 that will show type of authentication
  - Password
  - PassPhrase
  - MFA
  - PAssTicket

From: RACF Update: MFA 18Oct2016 Ross Cooper, IBM

# Lessons learned - PassPhrases

- *Without* PassPhrase support
  - Must use soft token to generate 8 digit value for password field
  - Windows ap (multiple PC's = multiple soft tokens)
  - iPhone ap
- *With* PassPhrase support
  - Can also use handheld tokens: PIN + token value

# Lessons learned – PassTickets

- If a user uses an application that employs PassTickets, they didn't work
  - *Until* 2FA software allowed PassTickets
  - CA Chorus – some components
  - CICS explorer
  - RD/z ?
- Get fresh maintenance for your ESM

# Lessons learned – Session Managers

- While replaying of password works, replaying for 2FA does NOT work
  - Tokens are one time use
  - You must configure your session manager to use PassTickets
  - Change your perception of PassTickets
    - From Password substitute
    - To Authentication substitute

# Lessons learned – Session Manager TPX

- TPX already has configurable option to allow use of PassTickets instead of password replay
- You should get fresh maintenance from CA for LOCK screen updates
  - Redrive authentication with ESM
  - Longer passcode field

# Lessons learned – EXEC CICS VERIFY PASSWORD

- Aps using VERIFY PASSWORD must be upgraded to use VERIFY PHRASE
  - Which is smart enough to handle both
- Be sure you are up to date on CICS maintenance

# Lessons learned – Future

- Smartcard support
- PIV / CAC support ids being worked on \
- Both IBM + CA will deliver smartcard support soon

# Questions ?

# Q & A

Simon.dodge@wellsfargo.com

404 327 8781