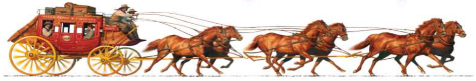
## Experiences with Two Factor authentication on z/OS

### New York RACF User Group

### 19 October 2016

Simon Dodge

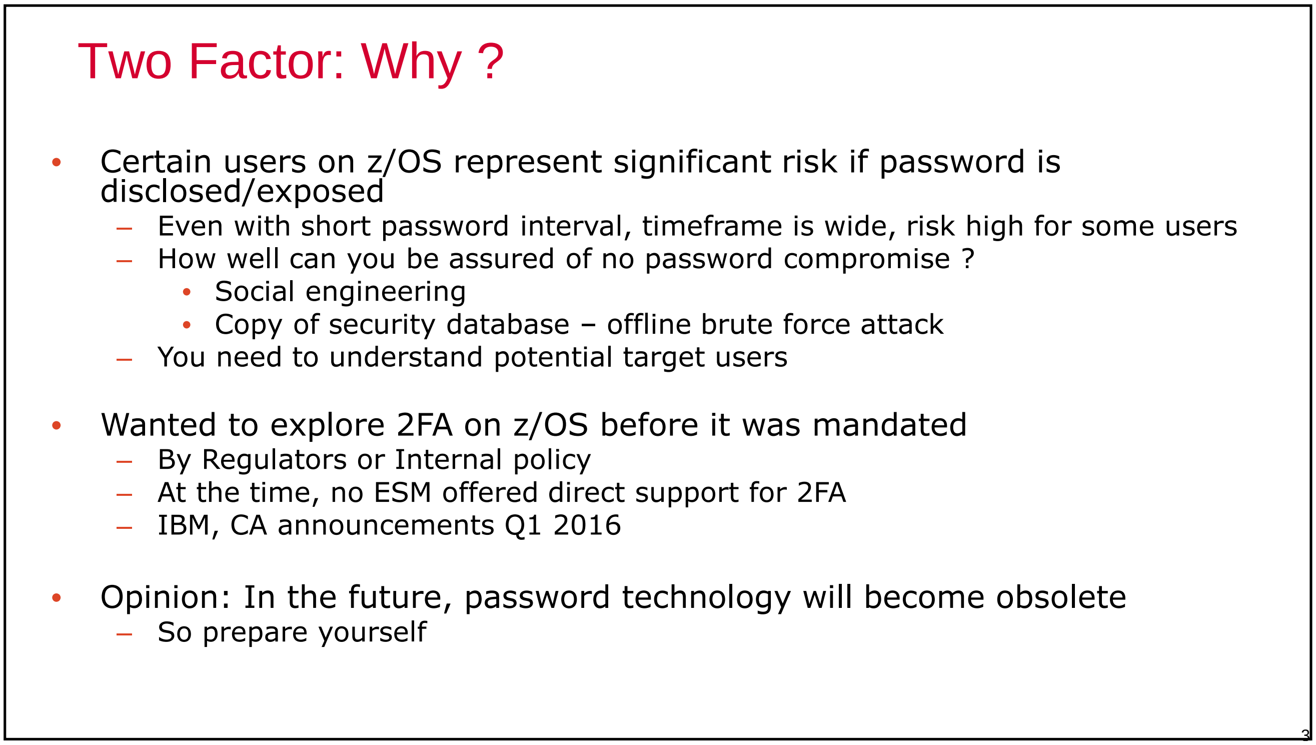
Principal Engineer,
zSeries Security Engineering



Together we'll go far

## Session agenda

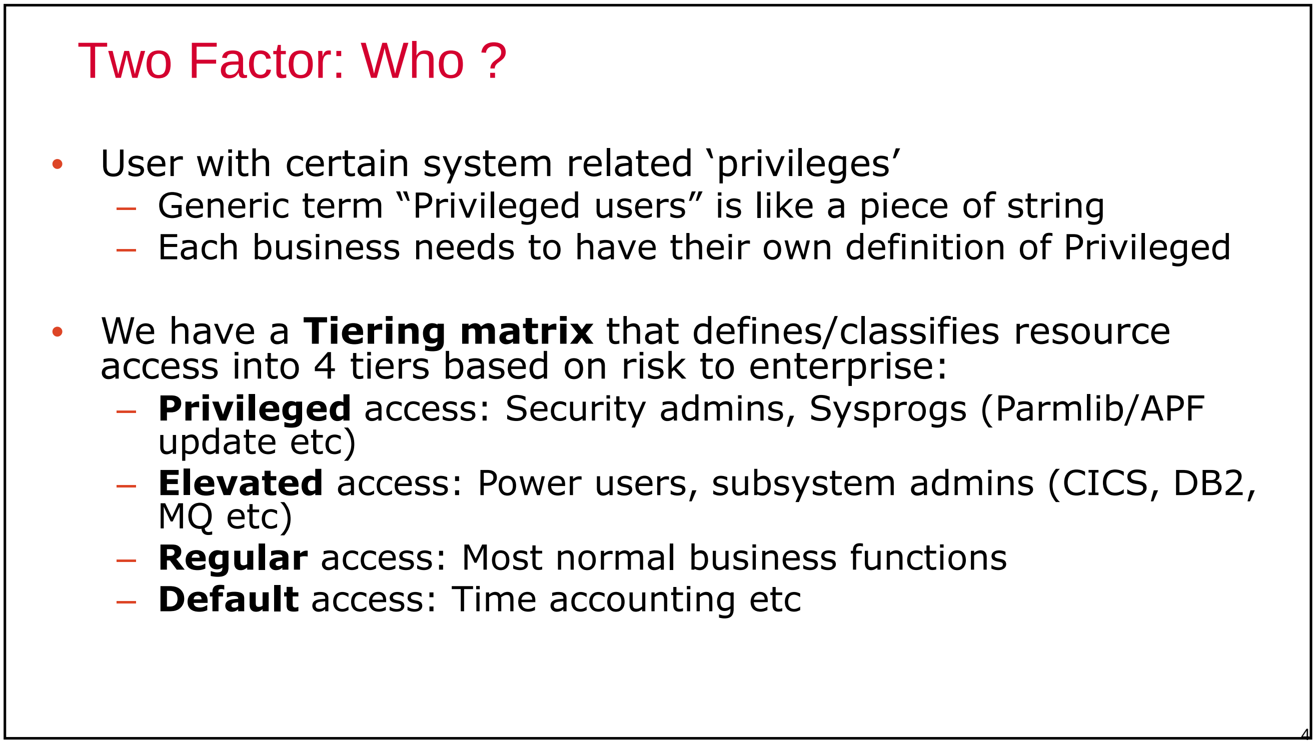
- Scope of testing effort: **Why ? Who ?**
- **Configuration**
  - What we tested: Add on product with TopSecret Q4 2015
    - Many similarities with IBM, CA ESM announcements Q1 2016
- Understand '**lessons learned**'
  - Exactly who are *your* Privileged users ?
  - Consider PassPhrases to allow PIN+token entry
  - Session Managers
  - Applications using PassTickets



## 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
- 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
  - IBM, CA announcements Q1 2016
- Opinion: In the future, password technology will become obsolete
  - So prepare yourself

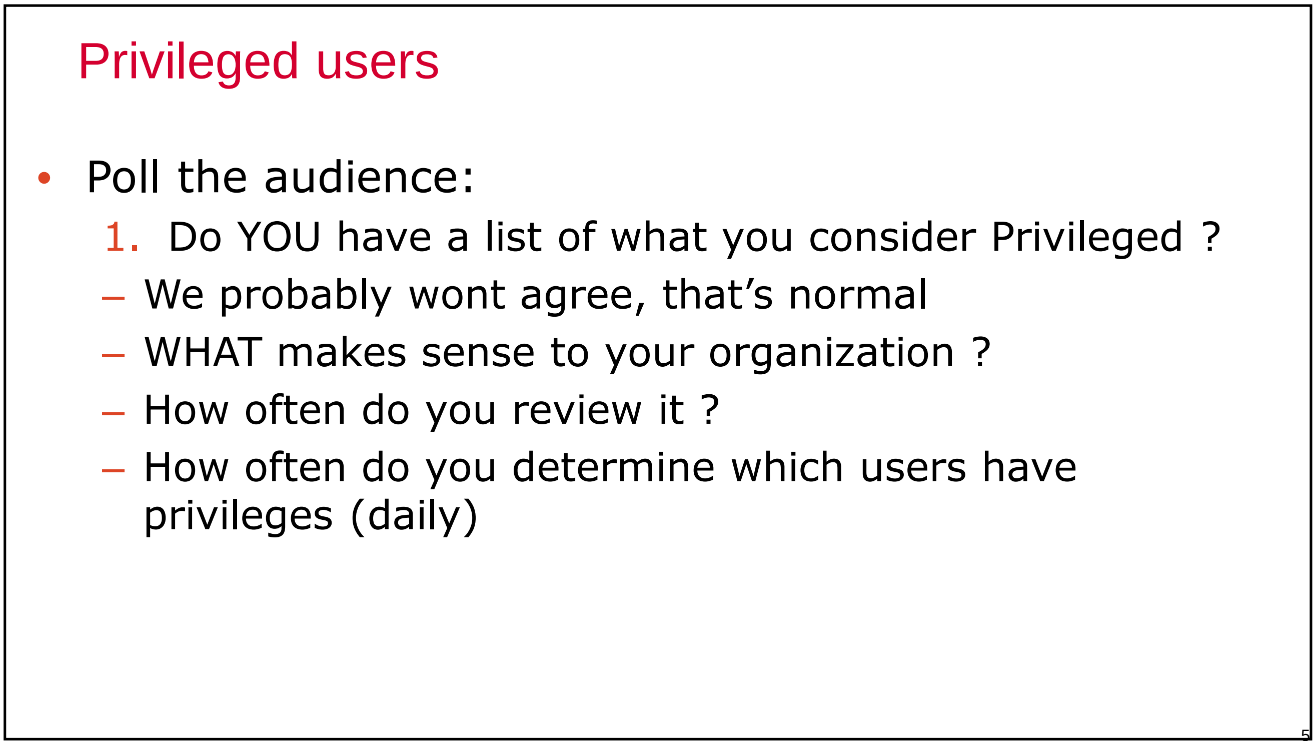
3



## Two Factor: Who ?

- 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

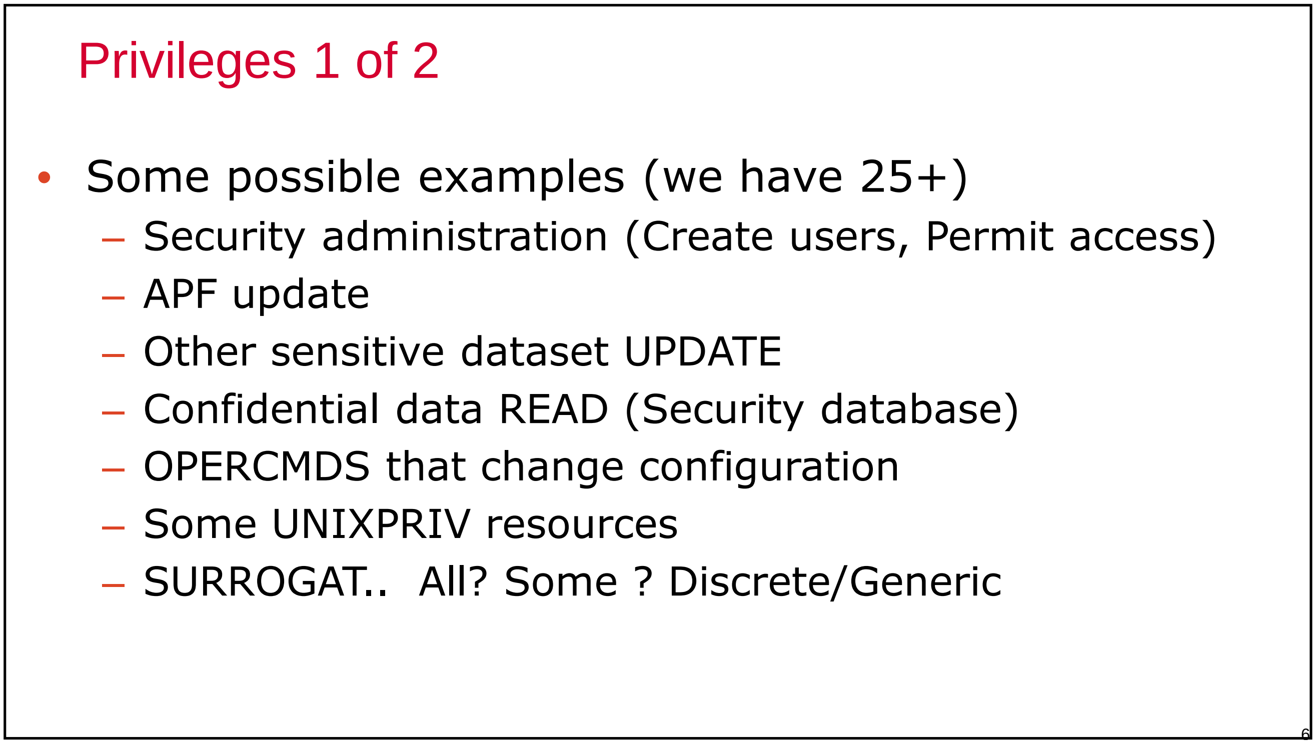
4



## 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)

5



## 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

6

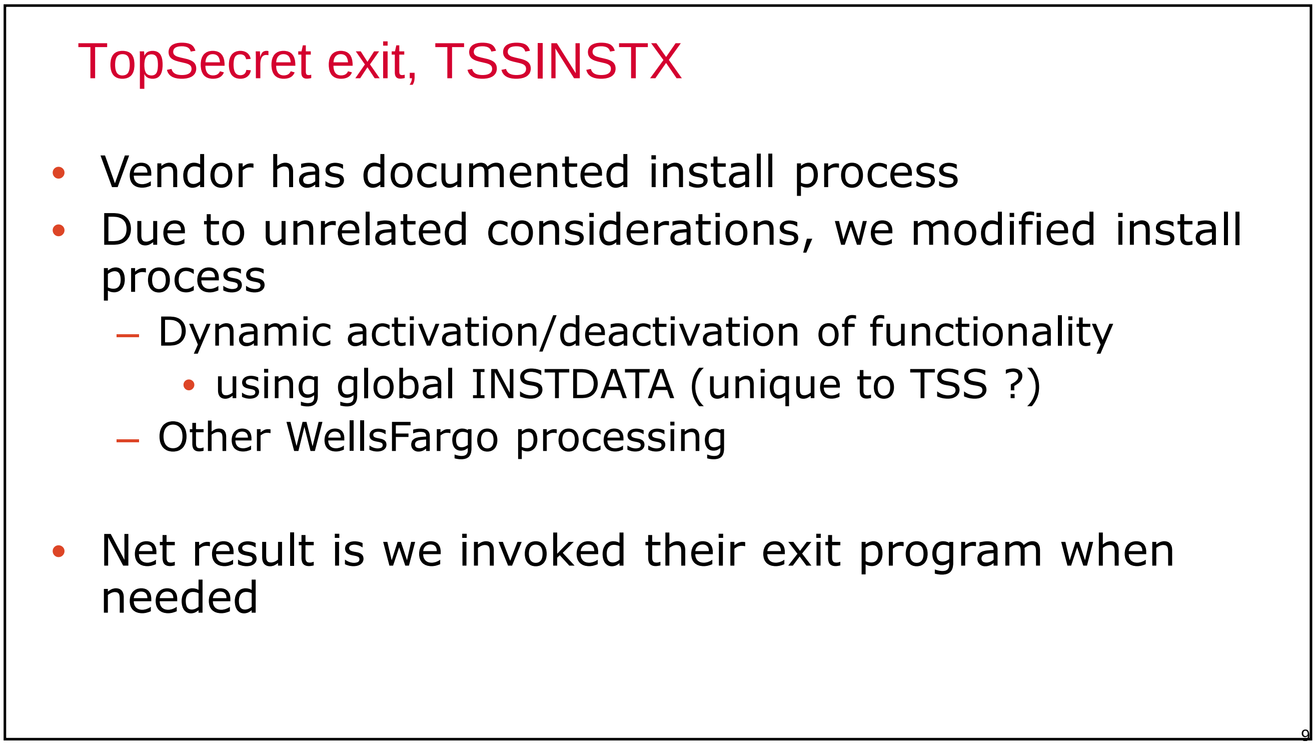
## Privileges 2 of 2

- 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

## Relatively easy install

- Installed 3rd party add-on product
- RACROUTE VERIFY calls are intercepted via ESM exit
- Separate STC determines if *this user* requires
  - 2FA authentication, or
  - Normal Password/PassTicket authentication

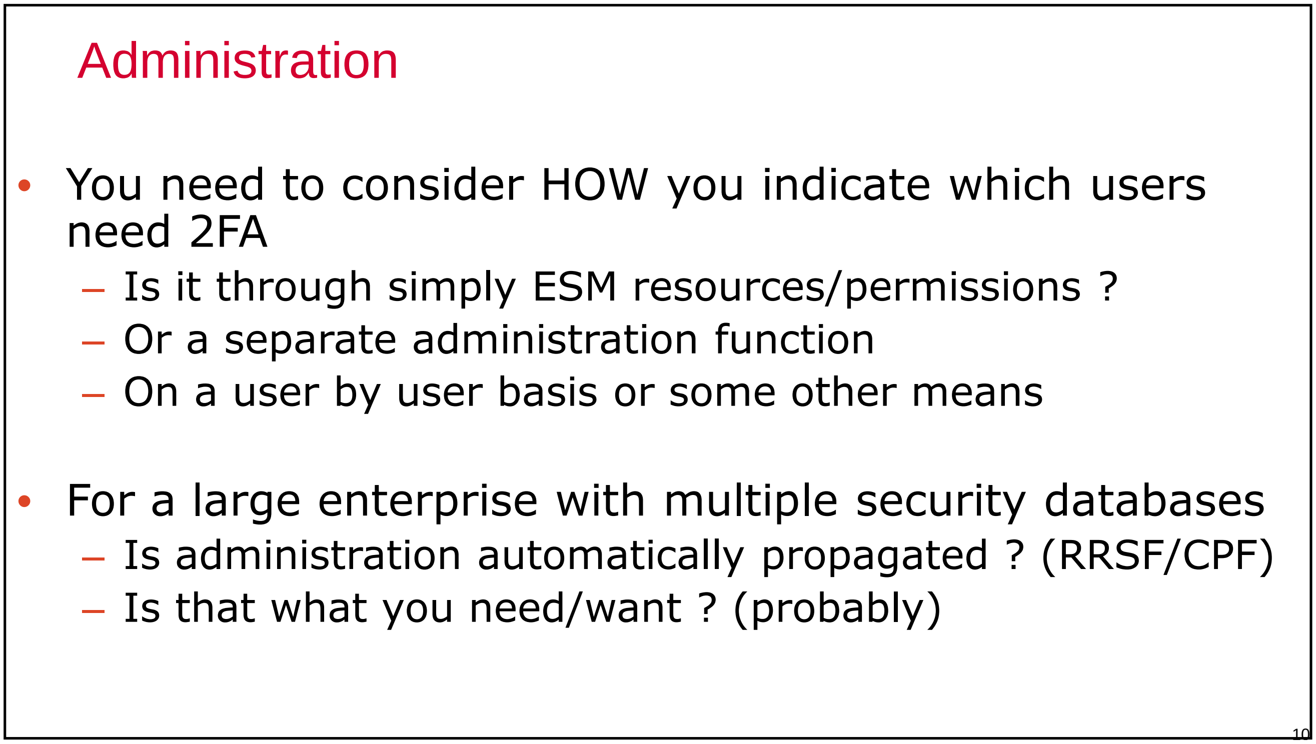
- **No software changes needed to RACROUTE caller**
  - Caller is unaware that user keyed in token value vs password



## TopSecret exit, TSSINSTX

- Vendor has documented install process
- Due to unrelated considerations, we modified install process
  - Dynamic activation/deactivation of functionality
    - using global INSTDATA (unique to TSS ?)
  - Other WellsFargo processing
- Net result is we invoked their exit program when needed

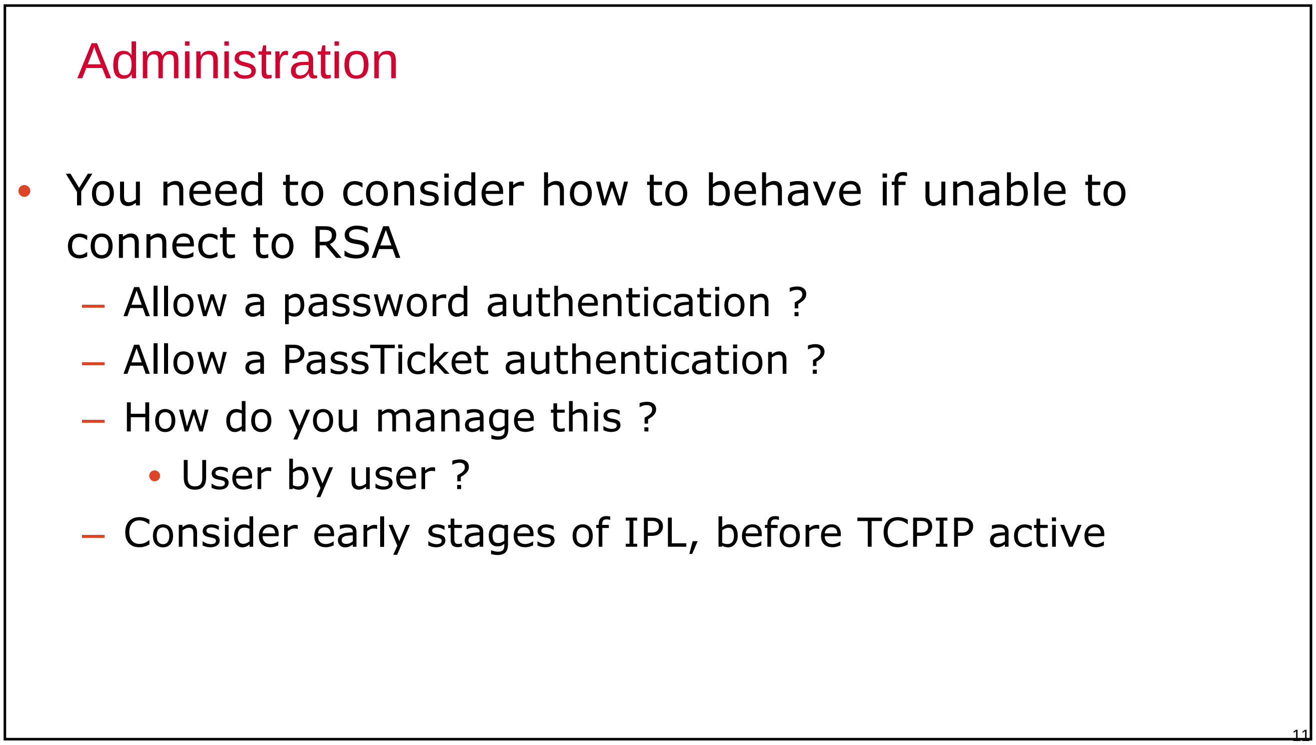
9



## Administration

- You need to consider HOW you indicate which users need 2FA
  - Is it through simply ESM resources/permissions ?
  - Or a separate administration function
  - On a user by user basis or some other means
- For a large enterprise with multiple security databases
  - Is administration automatically propagated ? (RRSF/CPF)
  - Is that what you need/want ? (probably)

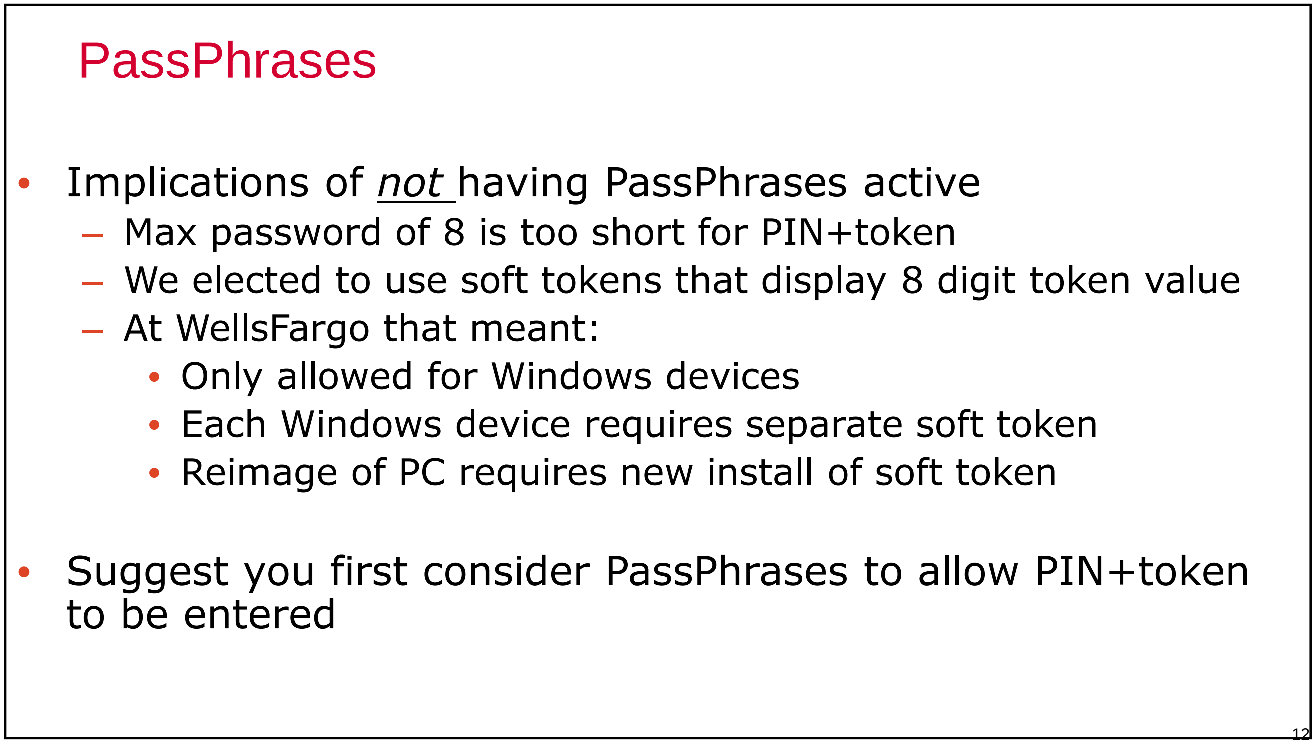
10



## Administration

- You need to consider how to behave if unable to connect to RSA
  - Allow a password authentication ?
  - Allow a PassTicket authentication ?
  - How do you manage this ?
    - User by user ?
  - Consider early stages of IPL, before TCPIP active

11



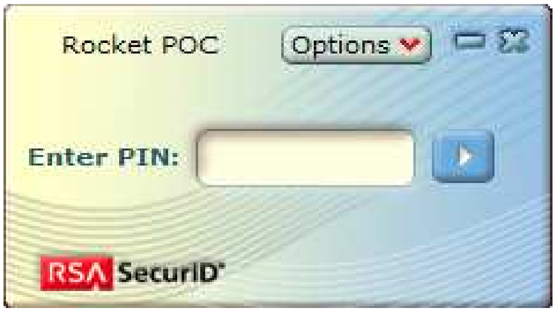
## PassPhrases

- Implications of *not* having PassPhrases active
  - Max password of 8 is too short for PIN+token
  - We elected to use soft tokens that display 8 digit token value
  - At WellsFargo that meant:
    - Only allowed for Windows devices
    - Each Windows device requires separate soft token
    - Reimage of PC requires new install of soft token
- Suggest you first consider PassPhrases to allow PIN+token to be entered

12

## Soft Token

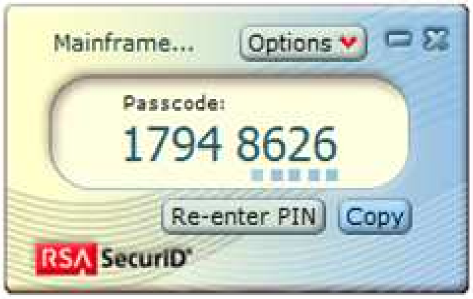
- Installed on Windows device
- Prompt for a PIN when started and after 3 token displays



13

## Soft Token

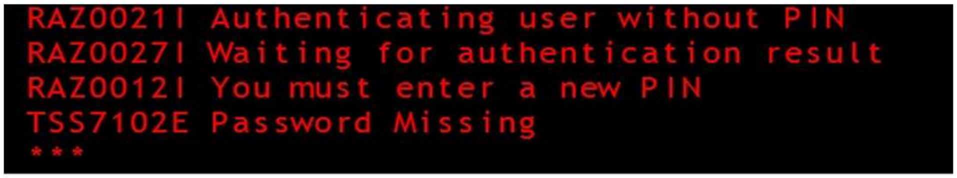
- 8 digit token value displayed after you enter a PIN
  - Will be valid if you entered correct PIN
  - Will not work if you entered wrong PIN
  - IE soft token does not validate PIN


Passcode: 1794 8626

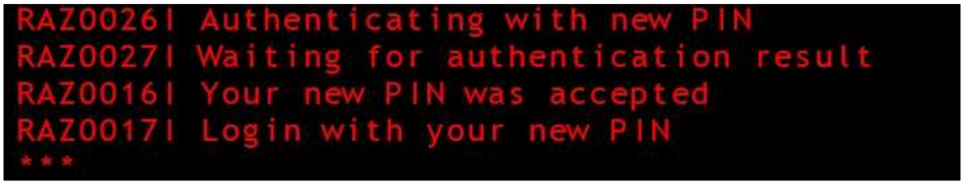
14

## New PIN mode

- Need to consider how you will establish initial PIN
- TSO new password dialog allows user to establish initial PIN
  - We couldn't get this to work in CICS



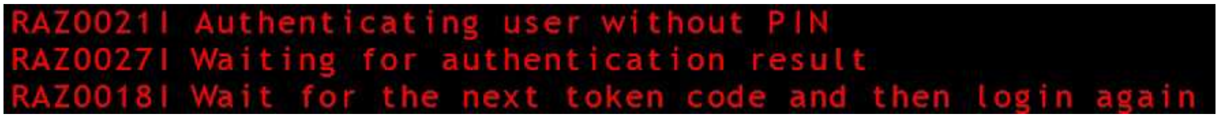
```
RAZ0021I Authenticating user without PIN
RAZ0027I Waiting for authentication result
RAZ0012I You must enter a new PIN
TSS7102E Password Missing
***
```



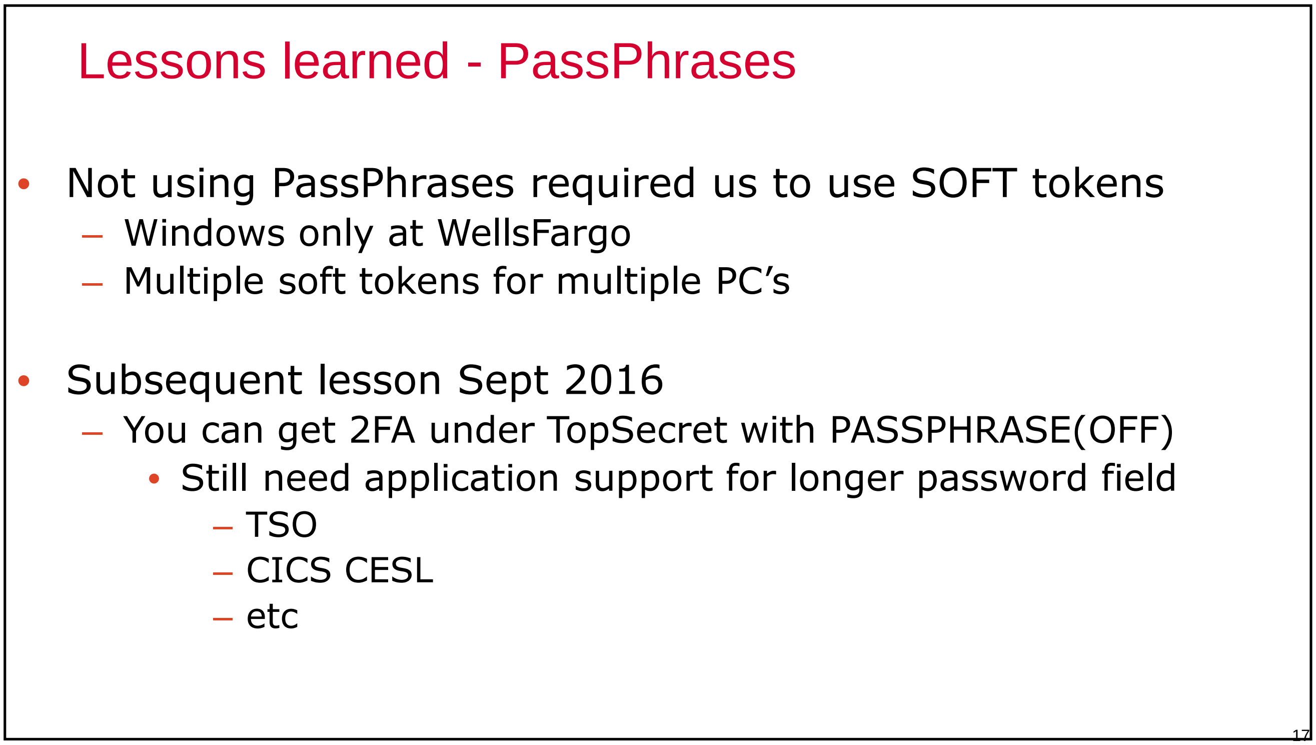
```
RAZ0026I Authenticating with new PIN
RAZ0027I Waiting for authentication result
RAZ0016I Your new PIN was accepted
RAZ0017I Login with your new PIN
***
```

## Next token mode

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



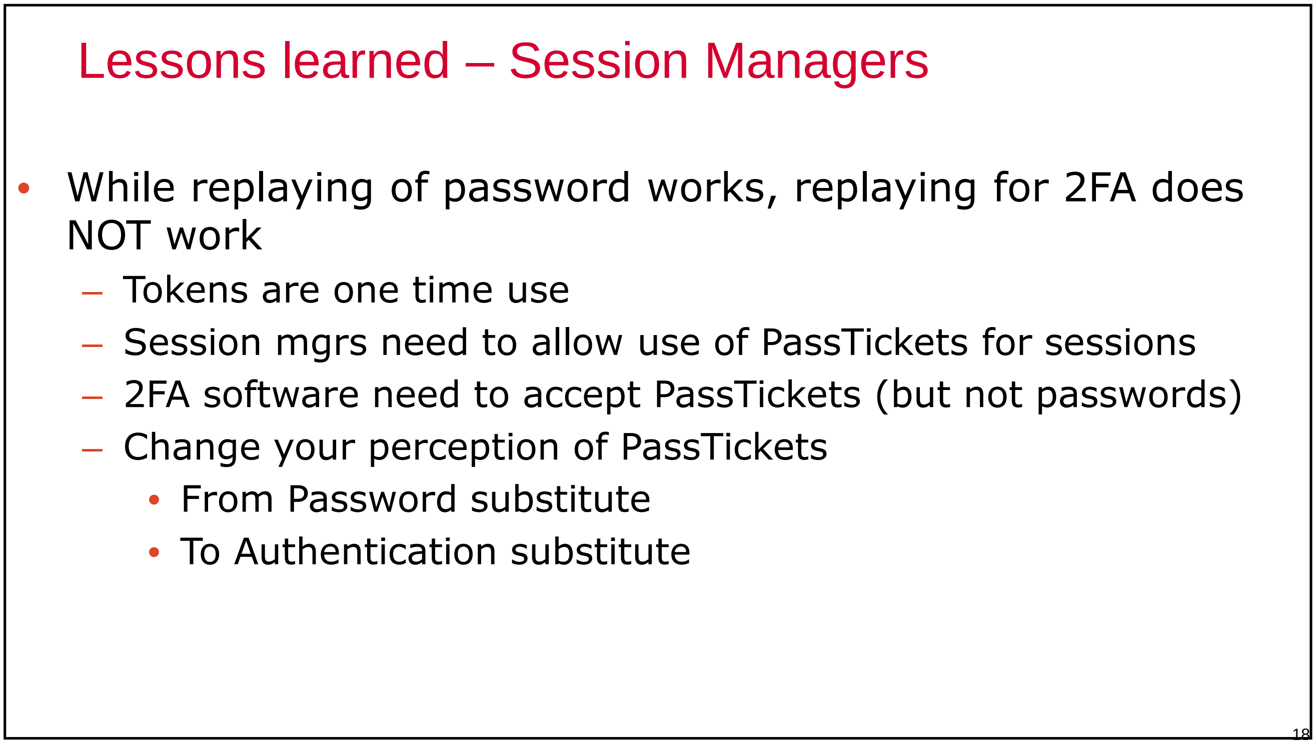
```
RAZ0021I Authenticating user without PIN
RAZ0027I Waiting for authentication result
RAZ0018I Wait for the next token code and then login again
```



## Lessons learned - PassPhrases

- Not using PassPhrases required us to use SOFT tokens
  - Windows only at WellsFargo
  - Multiple soft tokens for multiple PC’s
- Subsequent lesson Sept 2016
  - You can get 2FA under TopSecret with PASSPHRASE(OFF)
    - Still need application support for longer password field
      - TSO
      - CICS CESL
      - etc

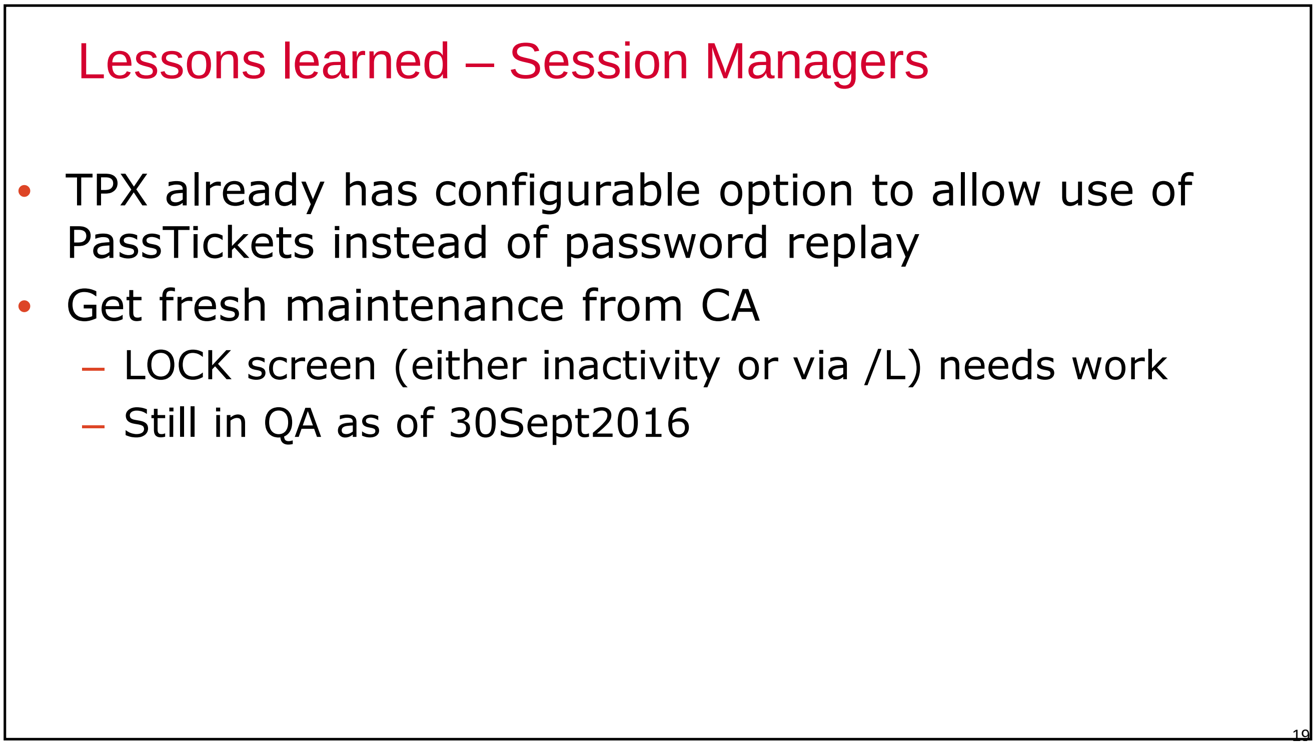
17



## Lessons learned – Session Managers

- While replaying of password works, replaying for 2FA does NOT work
  - Tokens are one time use
  - Session mgrs need to allow use of PassTickets for sessions
  - 2FA software need to accept PassTickets (but not passwords)
  - Change your perception of PassTickets
    - From Password substitute
    - To Authentication substitute

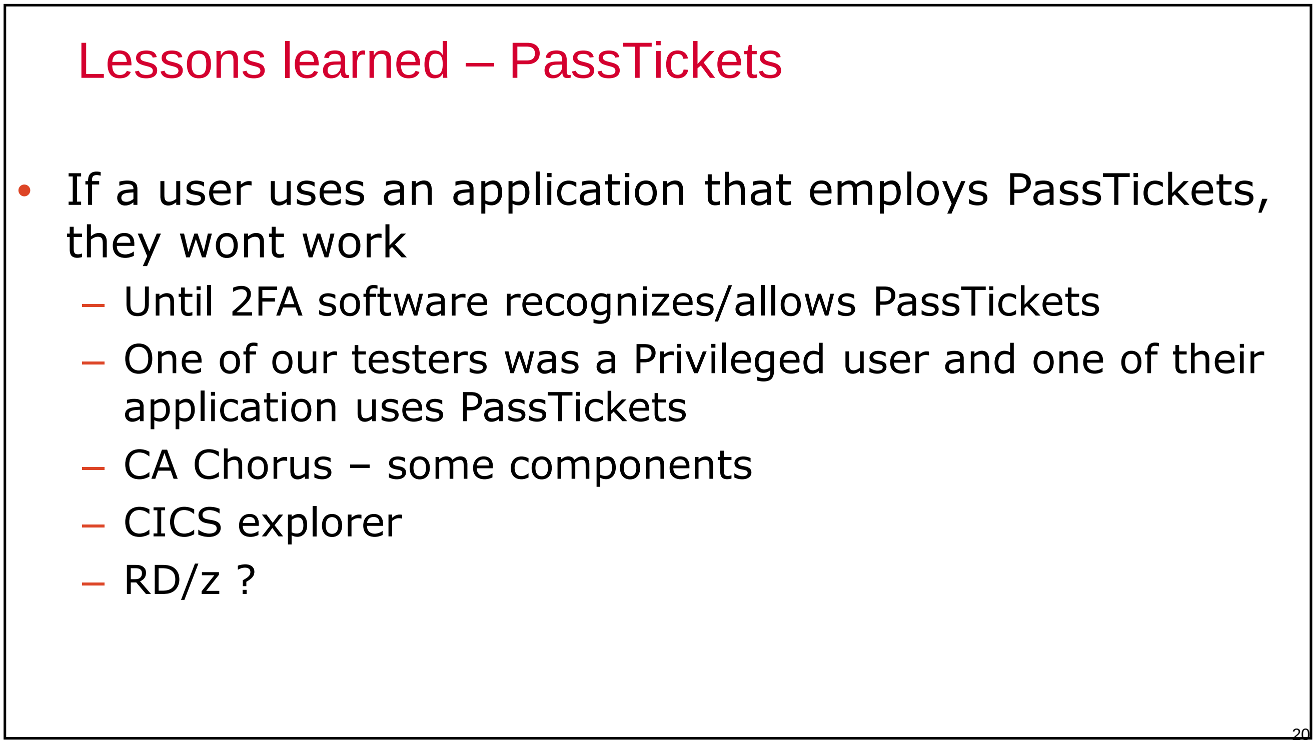
18



## Lessons learned – Session Managers

- TPX already has configurable option to allow use of PassTickets instead of password replay
- Get fresh maintenance from CA
  - LOCK screen (either inactivity or via /L) needs work
  - Still in QA as of 30Sept2016

19



## Lessons learned – PassTickets

- If a user uses an application that employs PassTickets, they wont work
  - Until 2FA software recognizes/allows PassTickets
  - One of our testers was a Privileged user and one of their application uses PassTickets
  - CA Chorus – some components
  - CICS explorer
  - RD/z ?

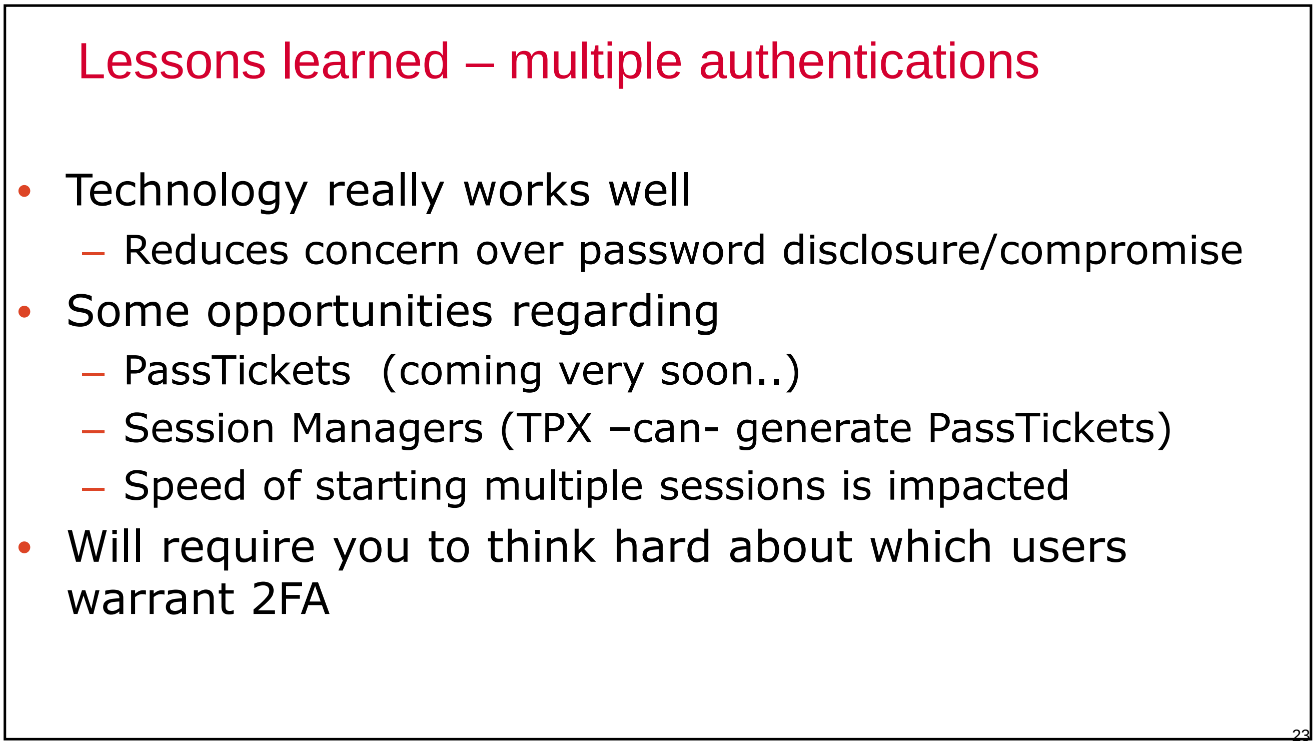
20

## Lessons learned – PassTickets

- Sept 2016: Re testing under TSS R16 indicates TSS will now allow PassTicket for MFA user
- IBM is aware of need for a similar solution for RACF
  - See later session today ?

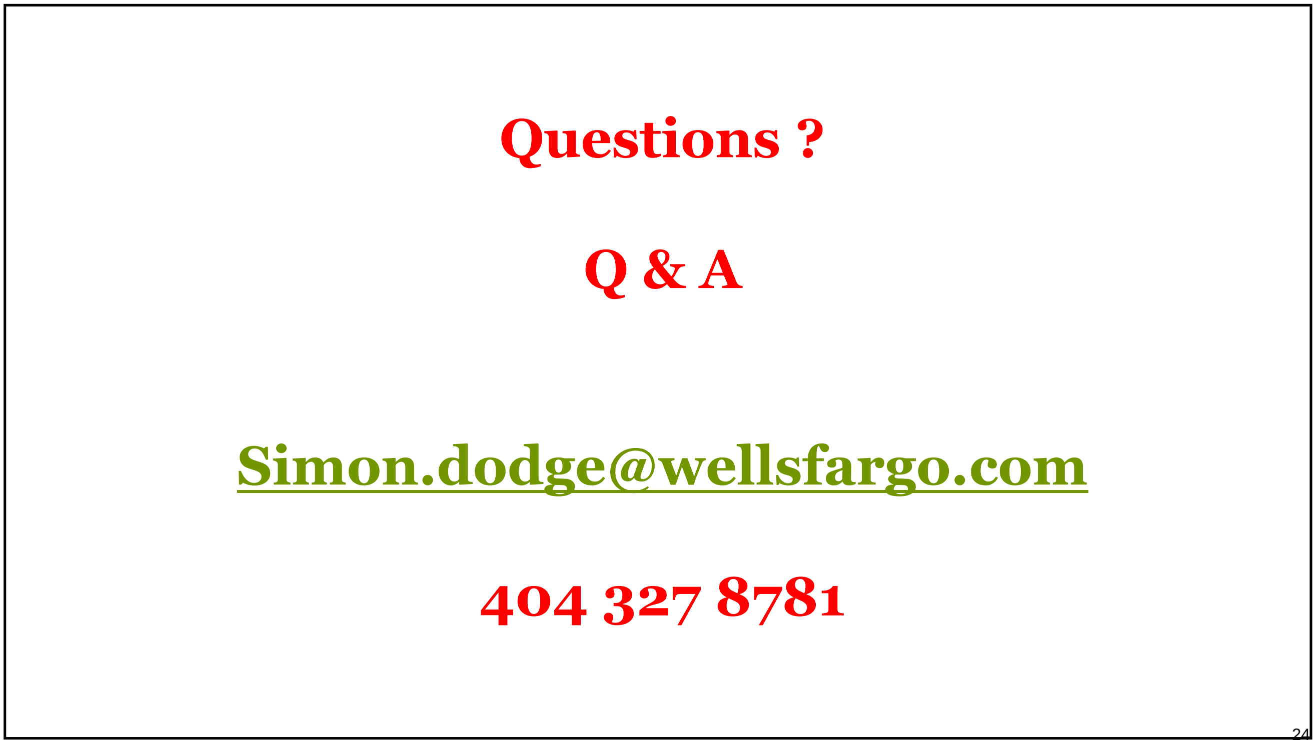
## Lessons learned – multiple authentications

- Speed of starting multiple sessions is impacted
- RSA tokens are one time use, changes every minute
- So only 1 session per minute, no faster
- So 5 sessions now takes 5 minutes, not 5 seconds
- Consider your definition of Privileged users
- Maybe you need multiple userids
  - Regular one not Privileged allowing multiples session
  - Privileged Id that does not need multiple session quickly



## Lessons learned – multiple authentications

- Technology really works well
  - Reduces concern over password disclosure/compromise
- Some opportunities regarding
  - PassTickets (coming very soon..)
  - Session Managers (TPX –can- generate PassTickets)
  - Speed of starting multiple sessions is impacted
- Will require you to think hard about which users warrant 2FA



**Questions ?**

**Q & A**

**Simon.dodge@wellsfargo.com**

**404 327 8781**