



MULTI-FACTOR AUTHENTICATION for z/OS and CICS – WHAT, WHY AND HOW

Part of your GDPR compliance strategy

September 2018

This session

Keith Banham

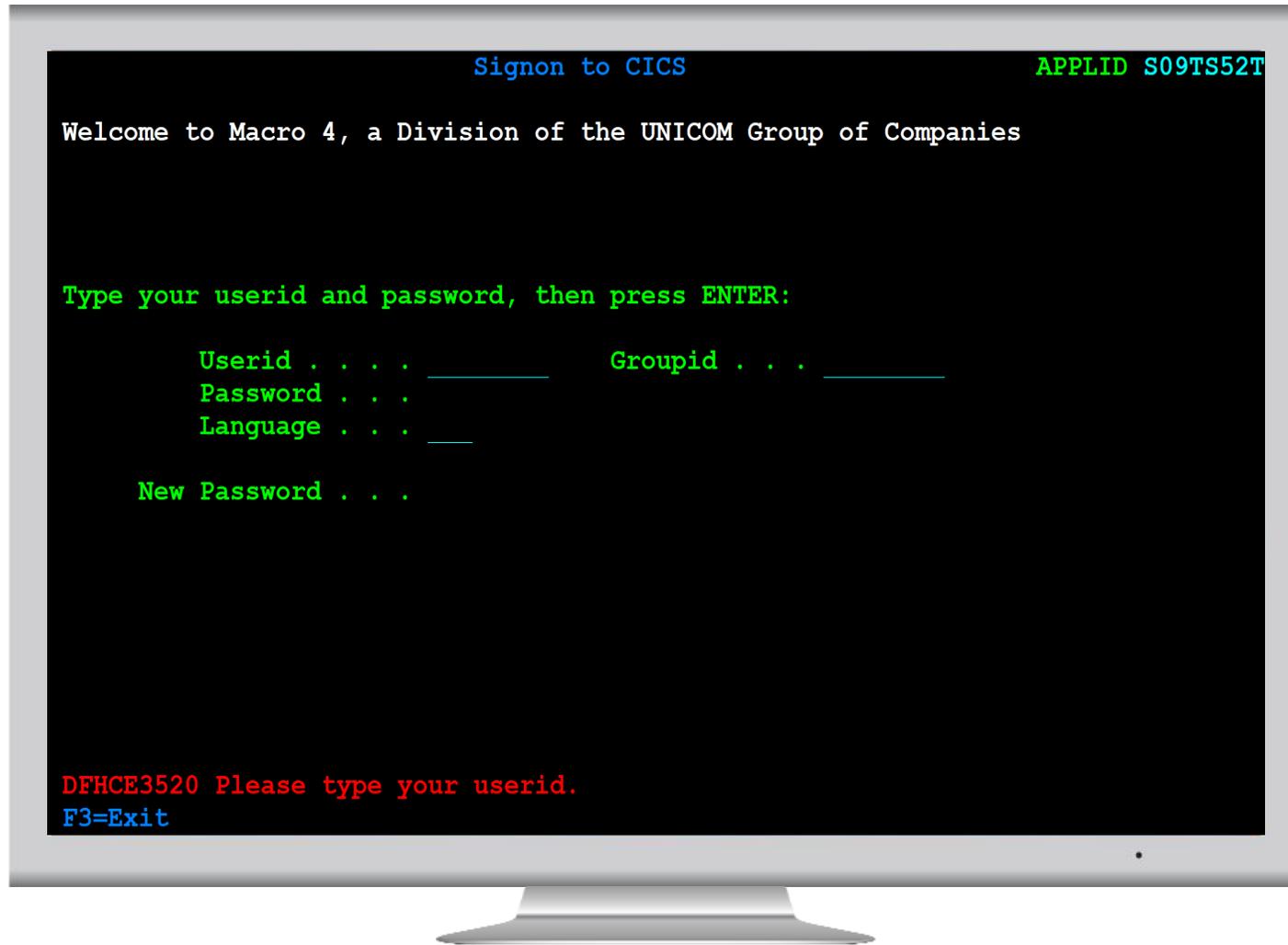
R&D Manager – Macro 4

Security is a key feature of z/OS and CICS but the weakest link is the use of user-IDs and passwords, making the system vulnerable to hacking and misuse. MFA is not a new technology but is now available on z/OS and CICS. This session will explain what MFA is, why it is an important consideration and options on how best to implement it. With GDPR coming into force in May 2018, using MFA can also help you demonstrate compliance with the stricter data protection obligations required by the new directive.

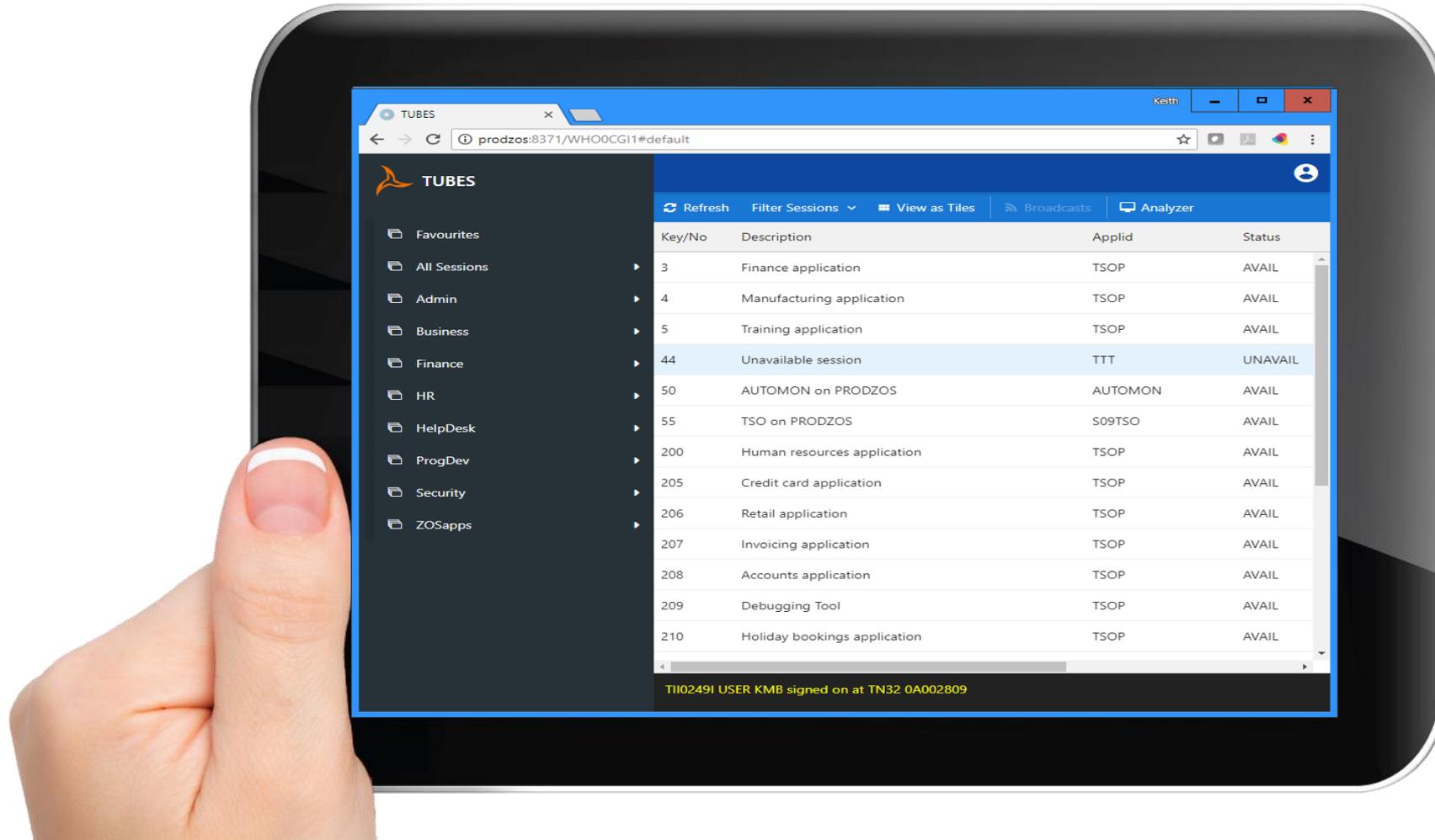
Agenda

- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- MFA – Why?
- MFA – How?
- Summary and Q&A

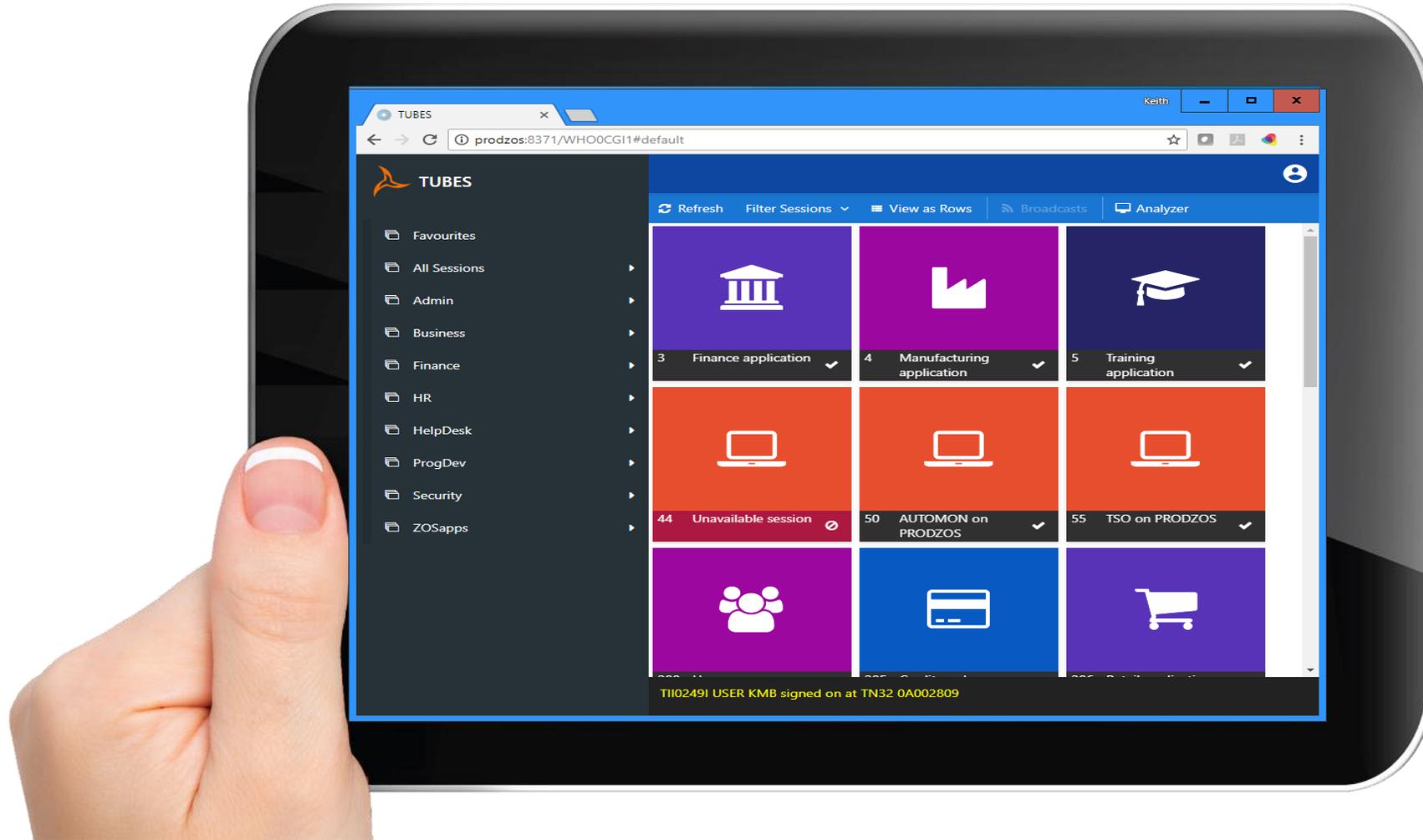
Standard Mainframe security



Accessing the mainframe on the move



Non-IT user accessing on the move



Accessing sensitive data





GDPR COMPLIANCE

Effective information governance

What is GDPR compliance?

- General Data Protection Regulation
- May 2018
- Protect personal data
- Not just EU companies affected
- Accountability & Governance
- Informed consent
- Increased rights
 - Access, corrections, deletion
 - Free of charge
- Tougher fines
- Need to control access!
 - Needs Multi-Factor Authentication

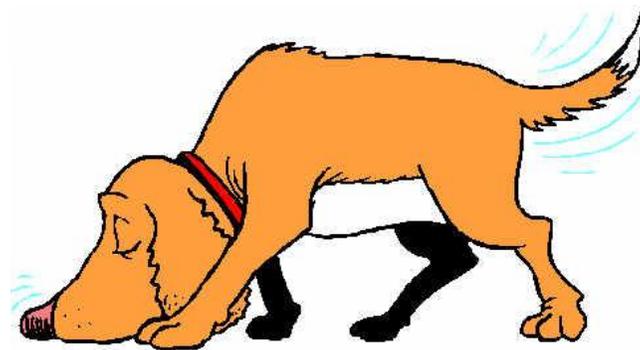
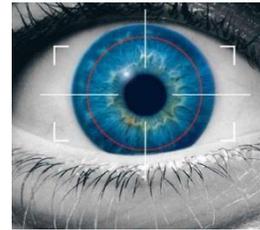


Agenda

- Single Factor Authentication (SFA) - what is the problem?
- **MFA – What?**
- MFA – Why?
- MFA – How?
- Summary and Q&A

It's not biometrics

- Finger print?
- Eye scanner?
- Static data!
- Can be line sniffed, traced and reused



Enhanced Mainframe Security - MFA

- IBM Multi-Factor Authentication for z/OS
 - Integrated with RACF
- OTP – one time password generator
 - Valid for a short period – 60 seconds?
 - Additional hardware and software
- Various options.....



Mainframe MFA via RSA

- RSA SecurID
- RSA Authentication Manager
- “Something you have”
 - Hardware or software RSA SecurID token
- “Two things you know”
 - An RSA SecurID PIN
 - Something you know



Mainframe MFA via Apple device

- IBM TouchToken for z/OS
- IBM TouchToken App on iOS device
- “Something you have”
 - iOS device and App
- “Something you are”
 - Your fingerprint



MFA – “In-band”

- RSA SecurID
- RSA Authentication Manager
- IBM TouchToken for z/OS
- IBM TouchToken App on iOS device
- Single token!

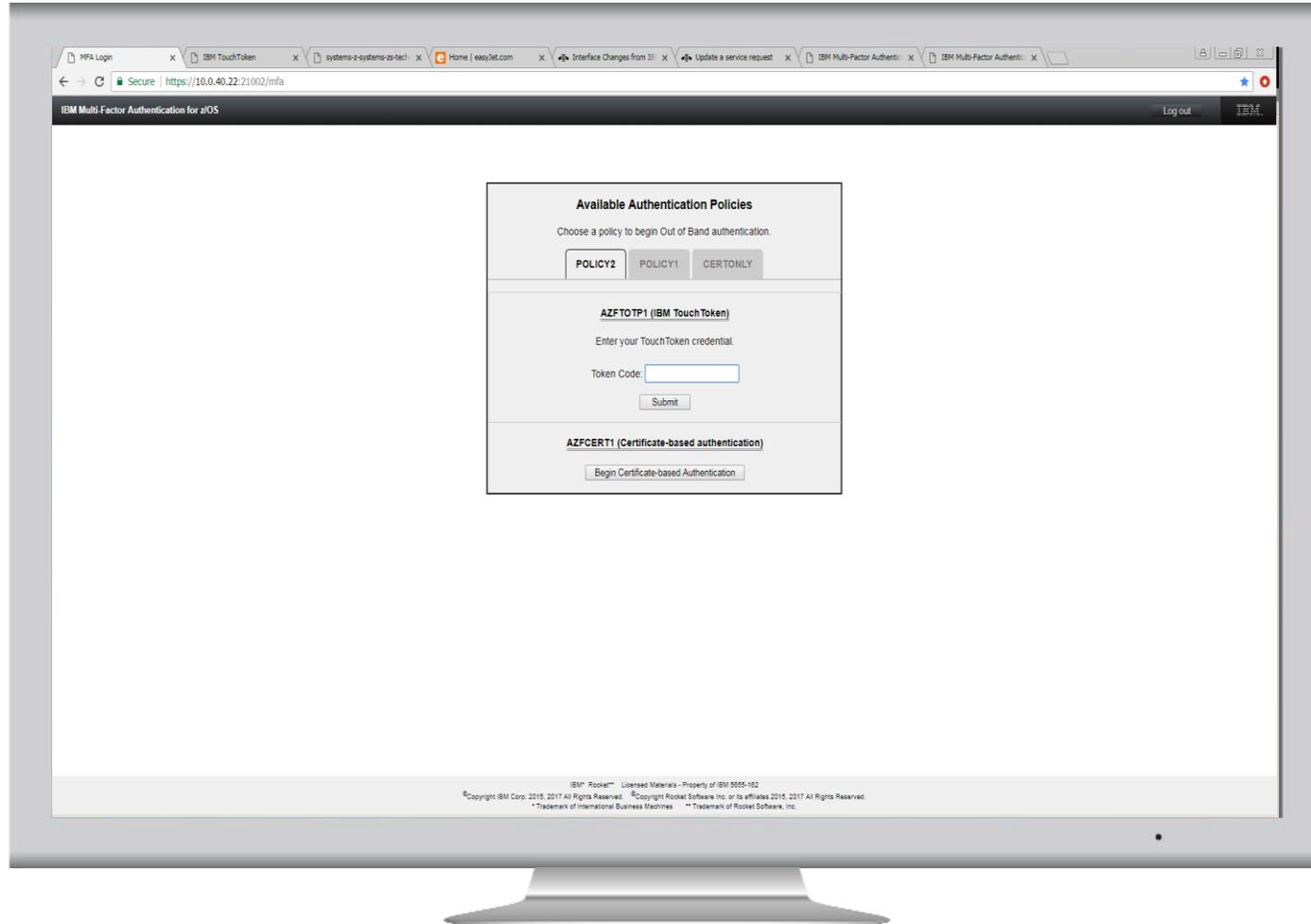


MFA – “Out-of-band”

- IBM Multi-Factor Authentication for z/OS
 - Web page
 - Enter RACF credentials
- User’s MFA policy
 - RSA SecurID
 - IBM TouchToken for z/OS
 - Plus others
- Single token!



MFA “Out-of-Band” multi-factor security



Mainframe MFA via CAC

- IBM MFA Certificate Authentication
- Common Access Card (CAC)
- Personal Identification Verification (PIV)
- Use in “Out-of-Band” only

- “Something you have”
 - The approved certificate from the card
- “Something you know”
 - PIN



True MFA has arrived

- IBM Multi-Factor Authentication for z/OS v1.3 announcement

http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/6/877/ENUSZP17-0546/index.html&lang=en&request_locale=en

- Release date - November 2017
- Additional factors
 - RADIUS support
 - Remote Authentication Dial-in User Service
 - Generic, SafeNet, RSA SecurID
 - Generic TOTP
 - Time-based One Time Password
 - Android and Microsoft™ Windows™ support
 - Compound Authentication for “In-Band”
 - Via PassPhrase field

Further reading

- IBM Redbook – IBM MFA V1R1 TouchToken, PassTicket, and Application Bypass Support
 - [REDP-5386-00](#)
- IBM Multi-Factor Authentication for z/OS User's Guide
 - [SC27-8448-03](#)
- IBM Multi-Factor Authentication for z/OS Installation and Customization
 - [SC27-8447-03](#)

Agenda

- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- **MFA – Why?**
- MFA – How?
- Summary and Q&A

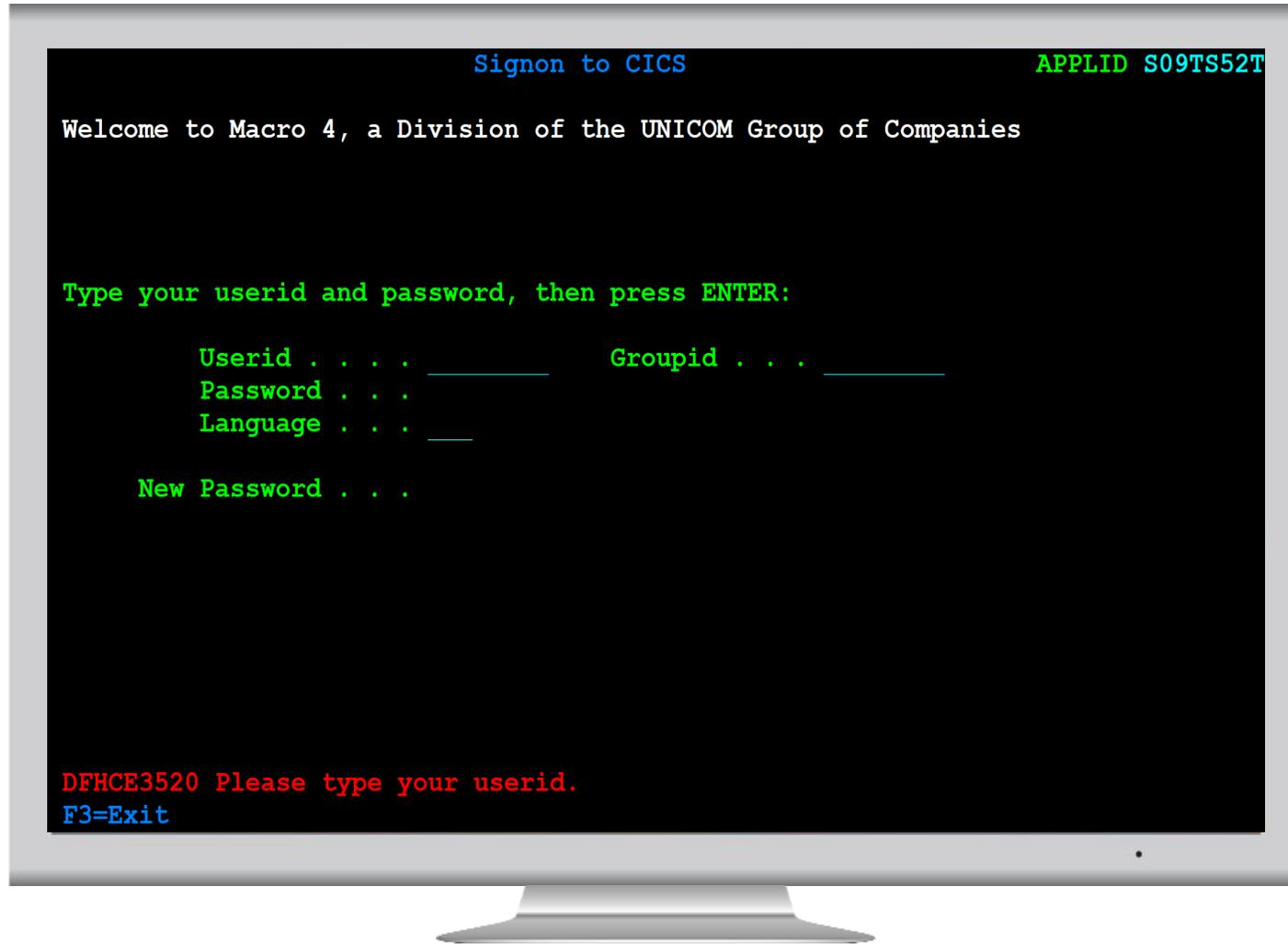
Why do you need MFA?



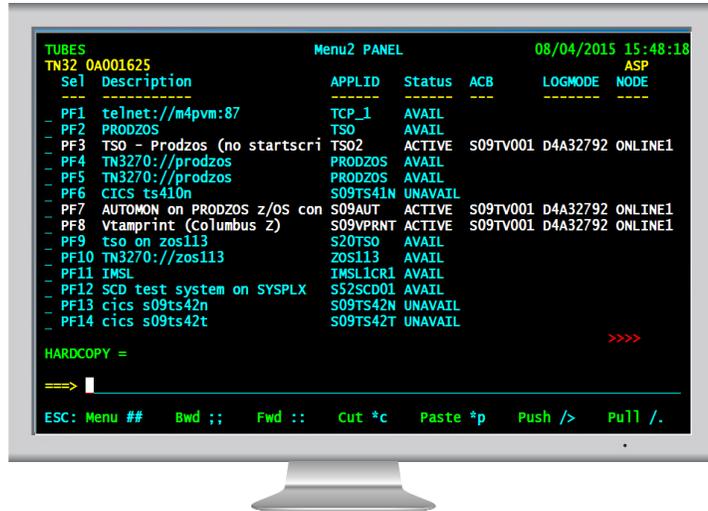
Agenda

- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- MFA – Why?
- **MFA – How?**
- Summary and Q&A

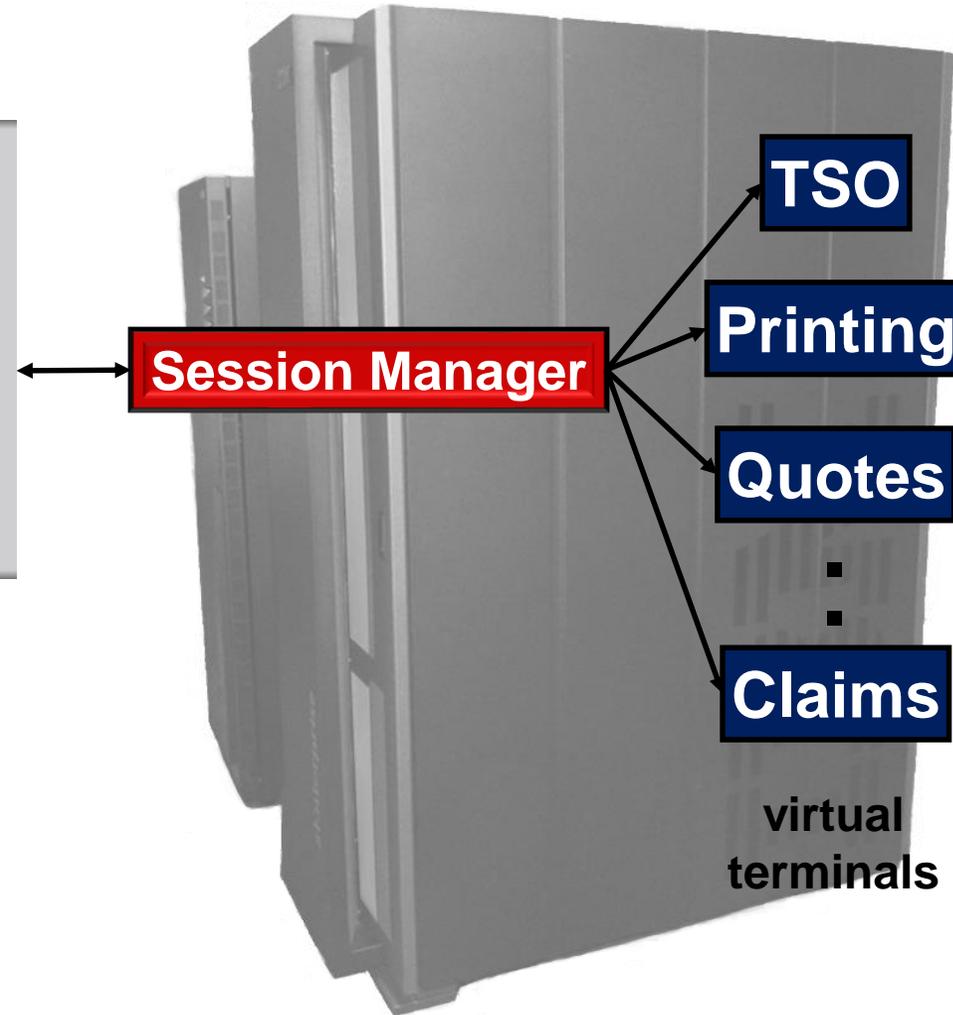
Standard Mainframe security



Mainframe Session Management



Feature rich session management



How do you implement MFA?

- Which option or options to use?
- Not clear what to enter and where!

- Use a modern Session Manager
 - Single logon and control
 - Simplify the process
 - Use PassTickets
 - Customise logon screens?
 - Add instructions?



Acquire local security token



Enter security token, separator and password

```

TIMES LU 0227CP26 11/05/2018 15:42:01 ASP
(C) Copyright 1982-2018 - All Rights Reserved.
Macro 4 started - a Division of UNICOM Global

Please enter your security credentials below:
Required:
Userid ==>
Security token ==>
Separator ==>
Password or phrase ==>

Optional:
New password or phrase ==>
Verify password or phrase ==>

==>

PF1:Help PF2:Transfer PF3:Logoff PF6:Err Mugs PF9:Transfer Override
    
```

External security manager passes security token to MFA server



MFA server passes security token to specific token server



Access security token server



If OK, logon to your Session Manager

MFA result returned to your Session Manager

MFA status returned

Security token status returned

Example In-Band & Compound using RACF* and IBM TouchToken*

```

TIMES TR32 04001682 Menu2 PANEL 03/05/2018 16:20:13 ASP
-----
SK1 Description APPLID Status ACB LOGMODE MODE
-----
PF1 ts1net://tdpvc:07 TSO J1 AVAIL
PF2 PRODZOS TSO AVAIL
PF3 TSO - Prodzos (no startscr) TSO AVAIL
PF4 TR3270://prodzos PRODZOS AVAIL
PF5 ts1net://20022 20022 AVAIL
PF6 CICS S09TS52T (DEV52T) S09TS52T UNAVAIL
PF7 AUTOMON on PRODZOS z/OS con S09AUT AVAIL
PF8 Vtainerpt (Columbus 2) S09VPRINT AVAIL
PF9 user defined key USER UNAVAIL
PF10 CICS S09TS52T (DEV520T) S09TS52T AVAIL
PF11 JNCR JNCR UNAVAIL
PF12 user defined key USER UNAVAIL
PF13 cics s09cp53e for multi von S09CP53E UNAVAIL
-----
HARDCOPY =
TT140121 Signon complete for ASP
-----
ESC: Menu ## End ;; Fwd ;; Cut *c Paste *p Push /> Pull /,
    
```

Request Passticket

Passticket gives access to all applications with a single, secure logon

```

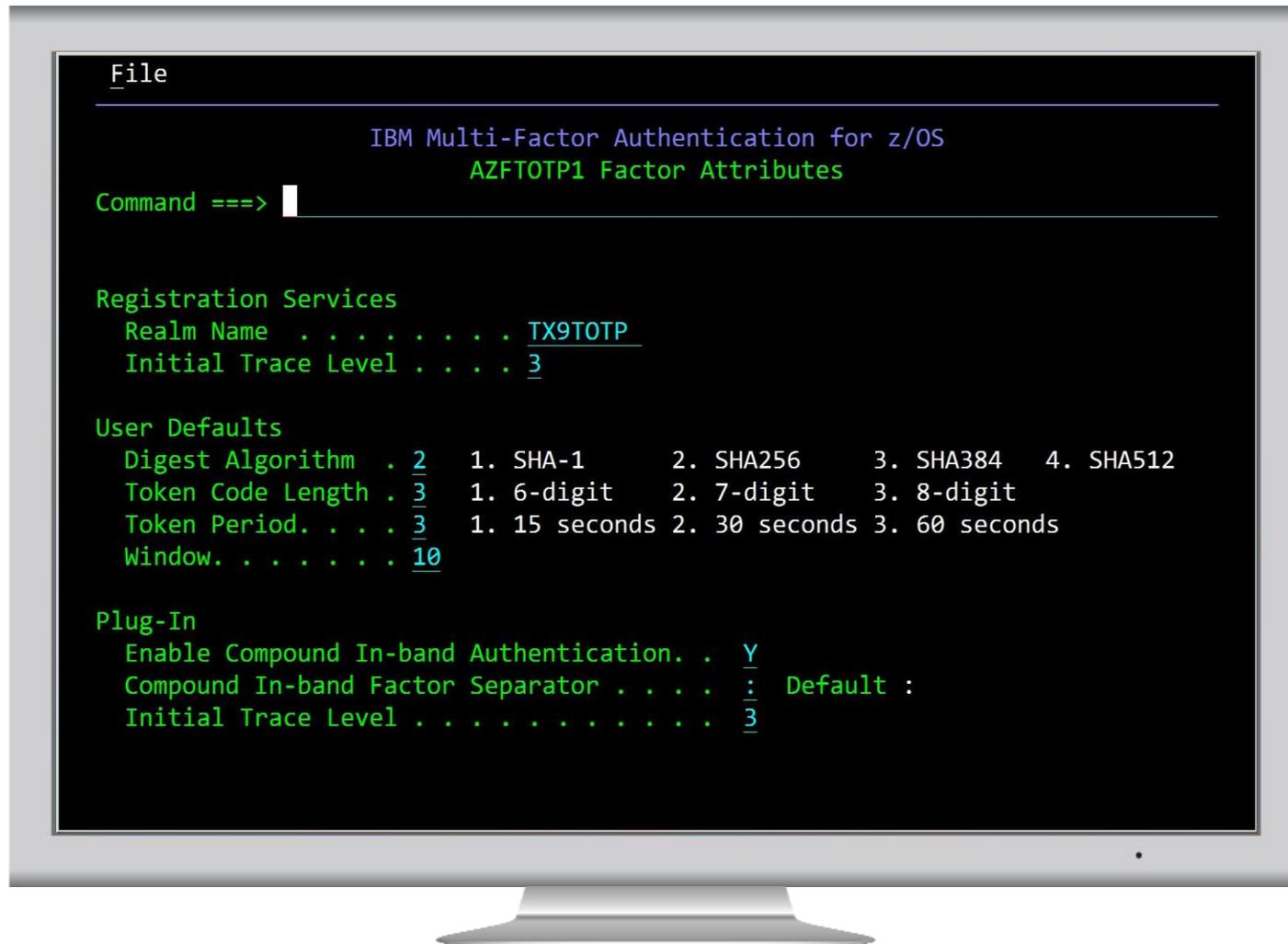
TIMES TR32 04001682 Menu2 PANEL 03/05/2018 16:29:57 ASP
-----
SK1 Description APPLID Status ACB LOGMODE MODE
-----
PF1 ts1net://tdpvc:07 TSO J1 AVAIL
PF2 PRODZOS TSO ACTIVE S09SM036 D4A32792 VSWITCH1
PF3 TSO - Prodzos (no startscr) TSO AVAIL
PF4 TR3270://prodzos PRODZOS AVAIL
PF5 ts1net://20022 20022 AVAIL
PF6 CICS S09TS52T (DEV52T) S09TS52T UNAVAIL
PF7 AUTOMON on PRODZOS z/OS con S09AUT ACTIVE S09TV001 D4A32792 VSWITCH1
PF8 Vtainerpt (Columbus 2) S09VPRINT AVAIL
PF9 user defined key USER UNAVAIL
PF10 CICS S09TS52T (DEV520T) S09TS52T ACTIVE S09TV001 D4A32792 VSWITCH1
PF11 JNCR JNCR UNAVAIL
PF12 user defined key USER UNAVAIL
PF13 cics s09cp53e for multi von S09CP53E UNAVAIL
-----
HARDCOPY =
TT103831 Escaped from session 10 - S09TS52T
-----
ESC: Menu ## End ;; Fwd ;; Cut *c Paste *p Push /> Pull /,
    
```

* Other ESMs and MFA solutions are available

MFA options – AZFEXEC command



AZFTOTP1 option

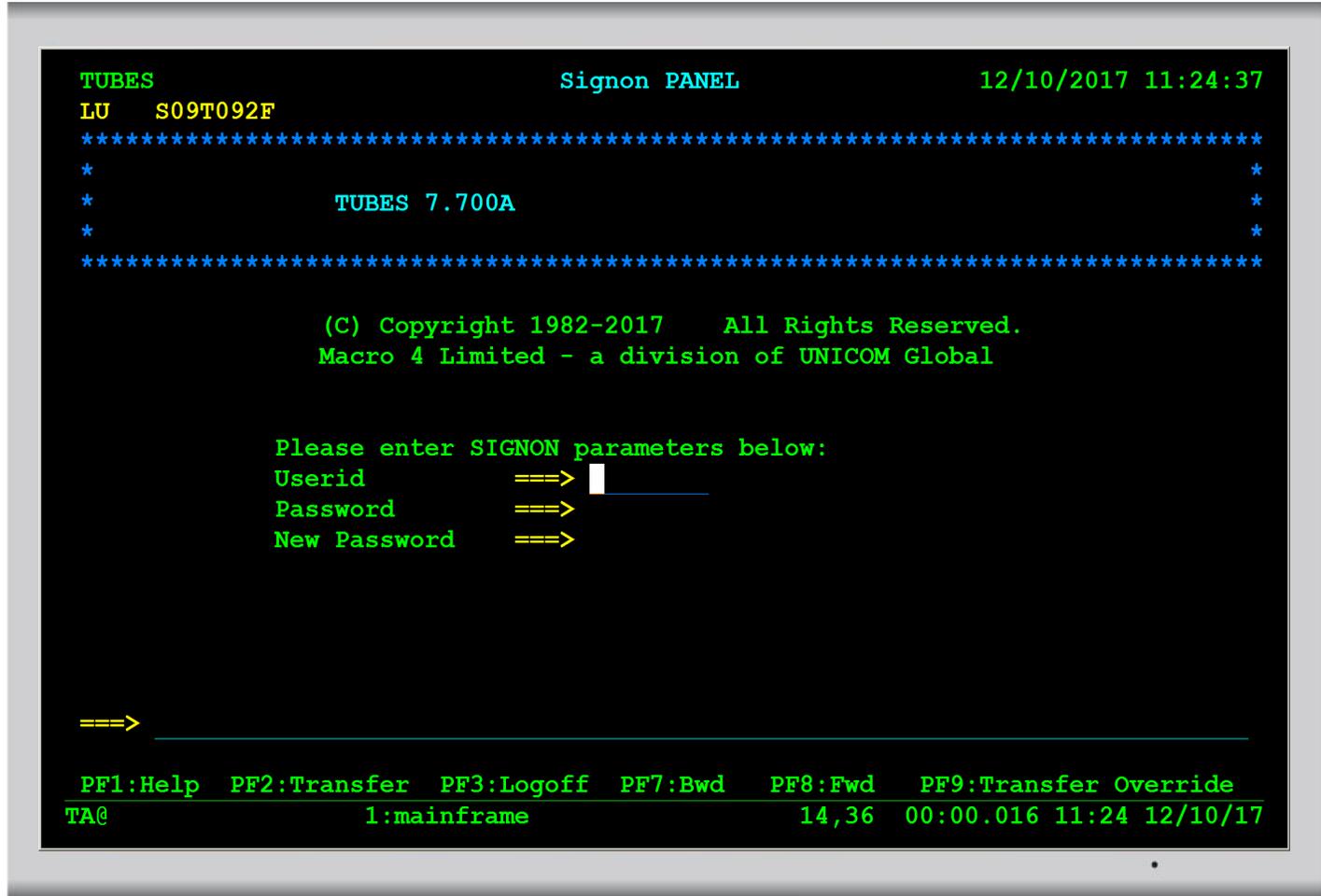


LISTUSER command

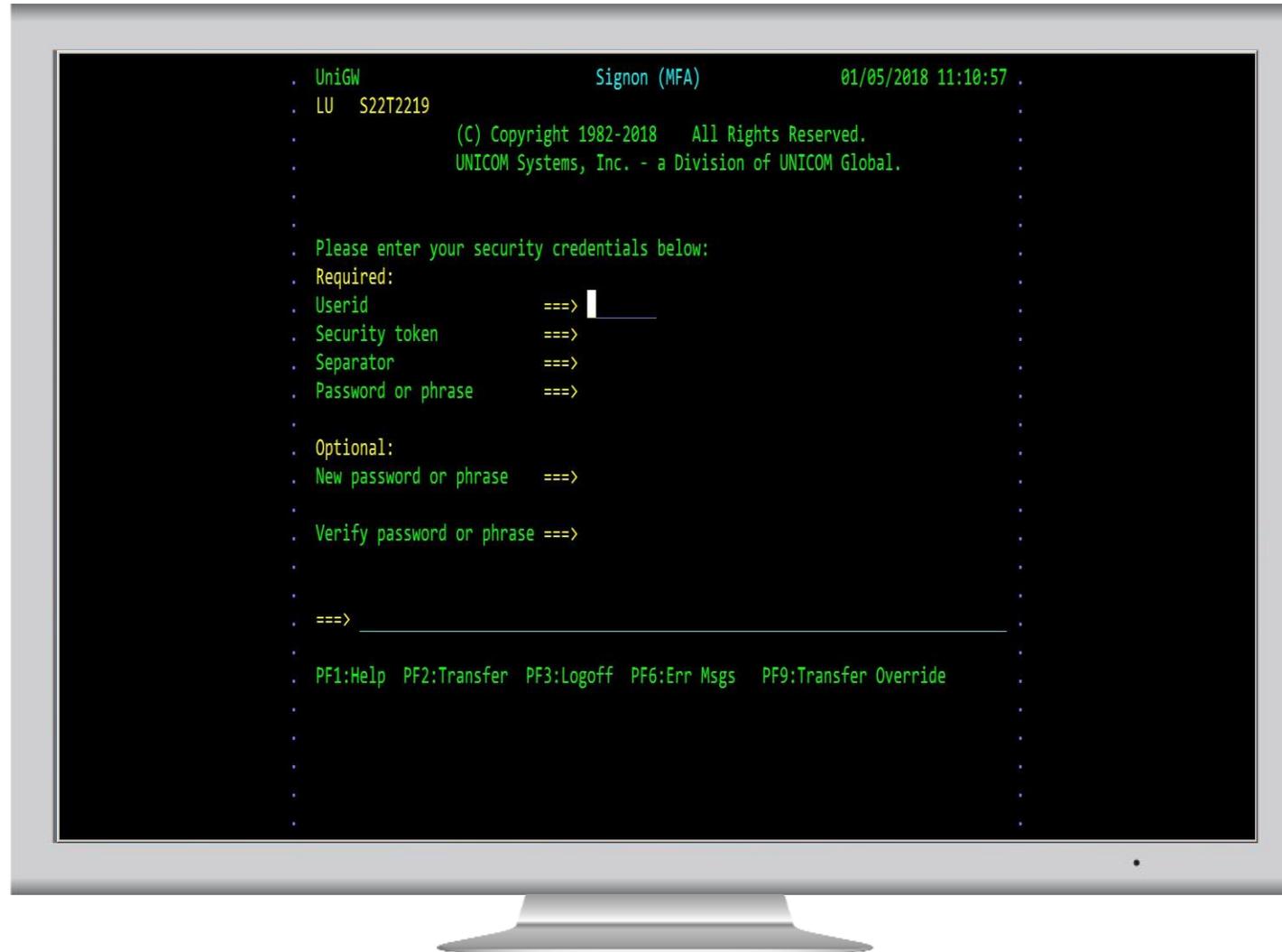
```
USER=MFA22 NAME=MFA22 OWNER=MUSER CREATED=18.085
DEFAULT-GROUP=MUSER PASSDATE=18.120 PASS-INTERVAL=180 PHRASEDATE=18.120
ATTRIBUTES=PASSPHRASE
REVOKE DATE=NONE RESUME DATE=NONE
LAST-ACCESS=18.121/11:12:10
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME

MULTIFACTOR AUTHENTICATION INFORMATION:
-----
PASSWORD FALLBACK IS ALLOWED
FACTOR = AZFTOTP1
STATUS = ACTIVE
FACTOR TAGS =
REGSTATE:PROVISIONED
KEYLABEL:AZF.MFA22.D4161BDA8FBF8511
ALG:SHA256
CVALUE:25418183
NUMDIGITS:8
PERIOD:60
WINDOW:10
```

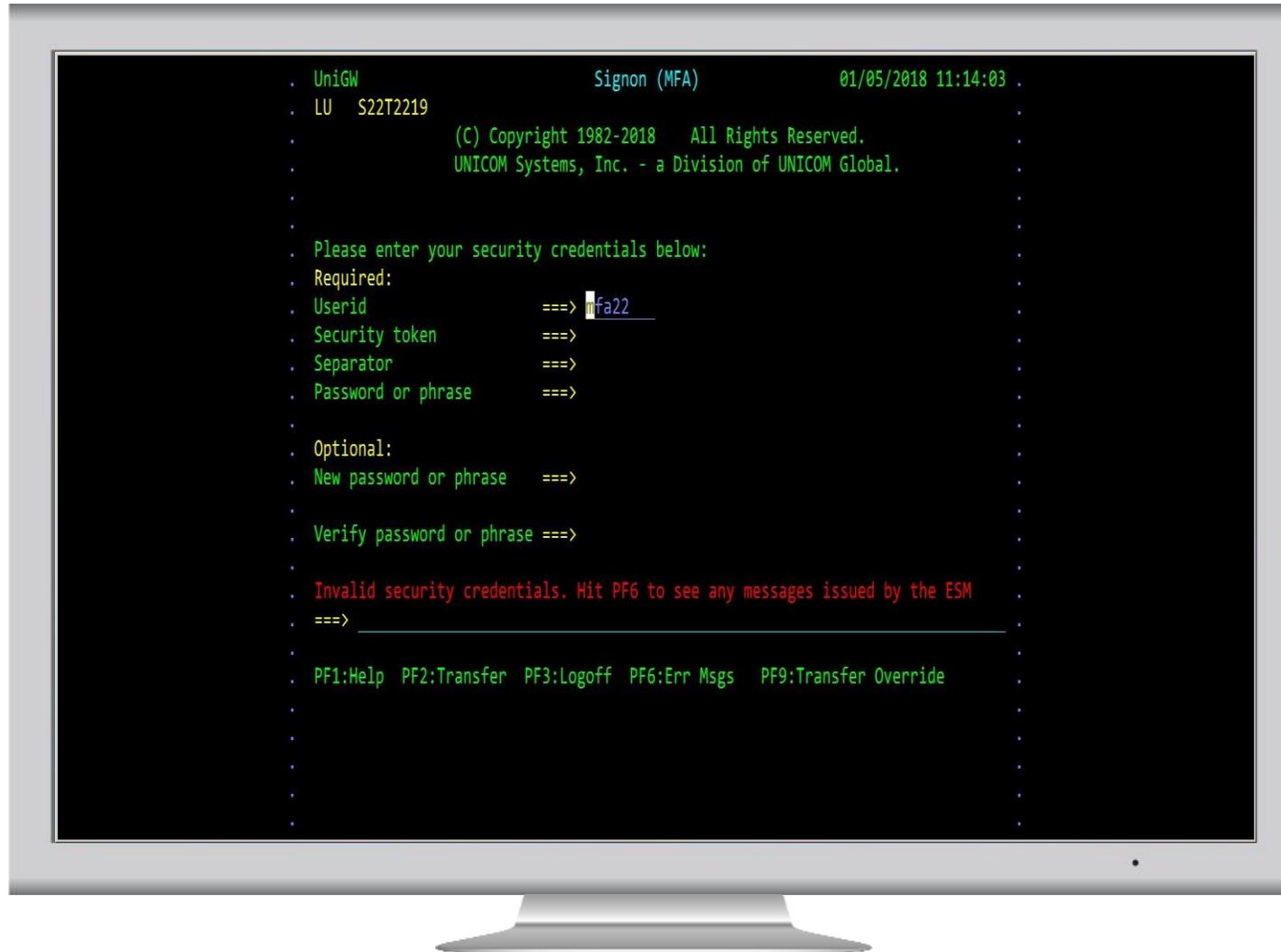
```
***
```



MFA “In-Band” security



Invalid credentials



MFA error messages



Still utilise PassTickets

- Customize Session Manager
- Use to access applications
- Single MFA sign on



There is a fall back option

- PWFALLBACK option
 - Use RACF password if MFA not available
- GDPR auditors
 - Not sure they will like this!
- Just for test environment?

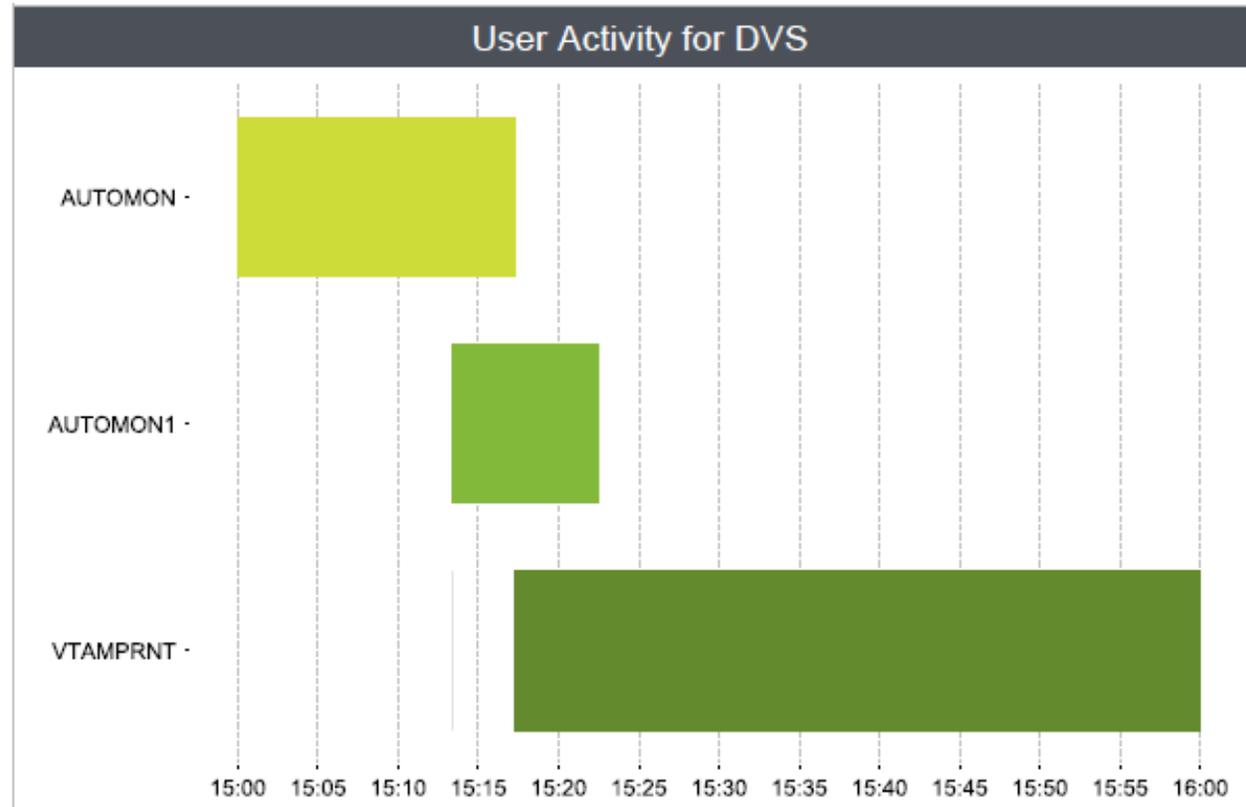


Auditing

- Auditing
 - Part of GDPR strategy
 - Who signed in
 - Who used a specific application
 - When and for how long
 - Push metrics into Business Analytic tools
 - Combine with other metrics

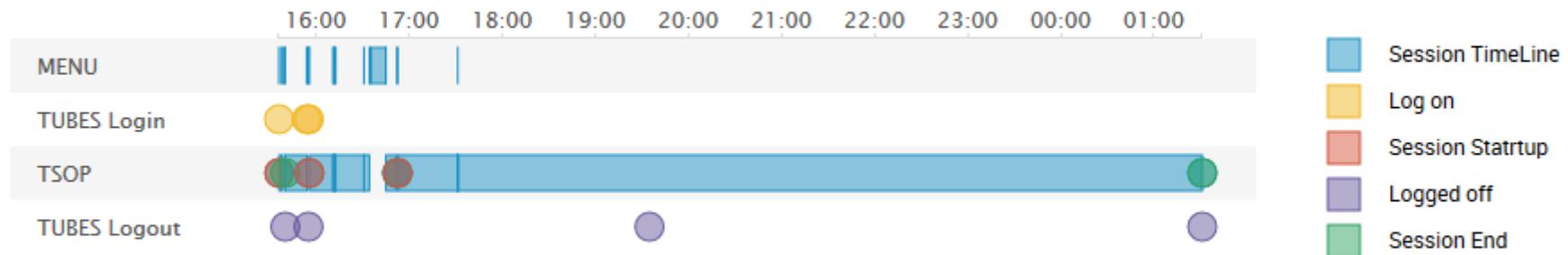


Auditing – Jasper report



Auditing – Splunk interactive report

Application Session Switches in Tubes by RXH



Agenda

- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- MFA – Why?
- MFA – How?
- **Summary and Q&A**

Summary

- Enhance your mainframe security
 - Part of a GDPR strategy
- Enable ease of use
 - Use a modern Session Manager as an enabler
- IBM to add other MFA options?
- Other vendor MFA options?
 - Easier to utilise in one place!





ANY QUESTIONS?

Summary

- Embrace MFA
- Utilise a modern Session Manager
- Reduce business risks





Putting **IT** All Together. SM

THANK YOU

keith.banham@macro4.com