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

Part of your GDPR compliance strategy

September 2018

MACRO 4
A Division of UNICOM Global

This session

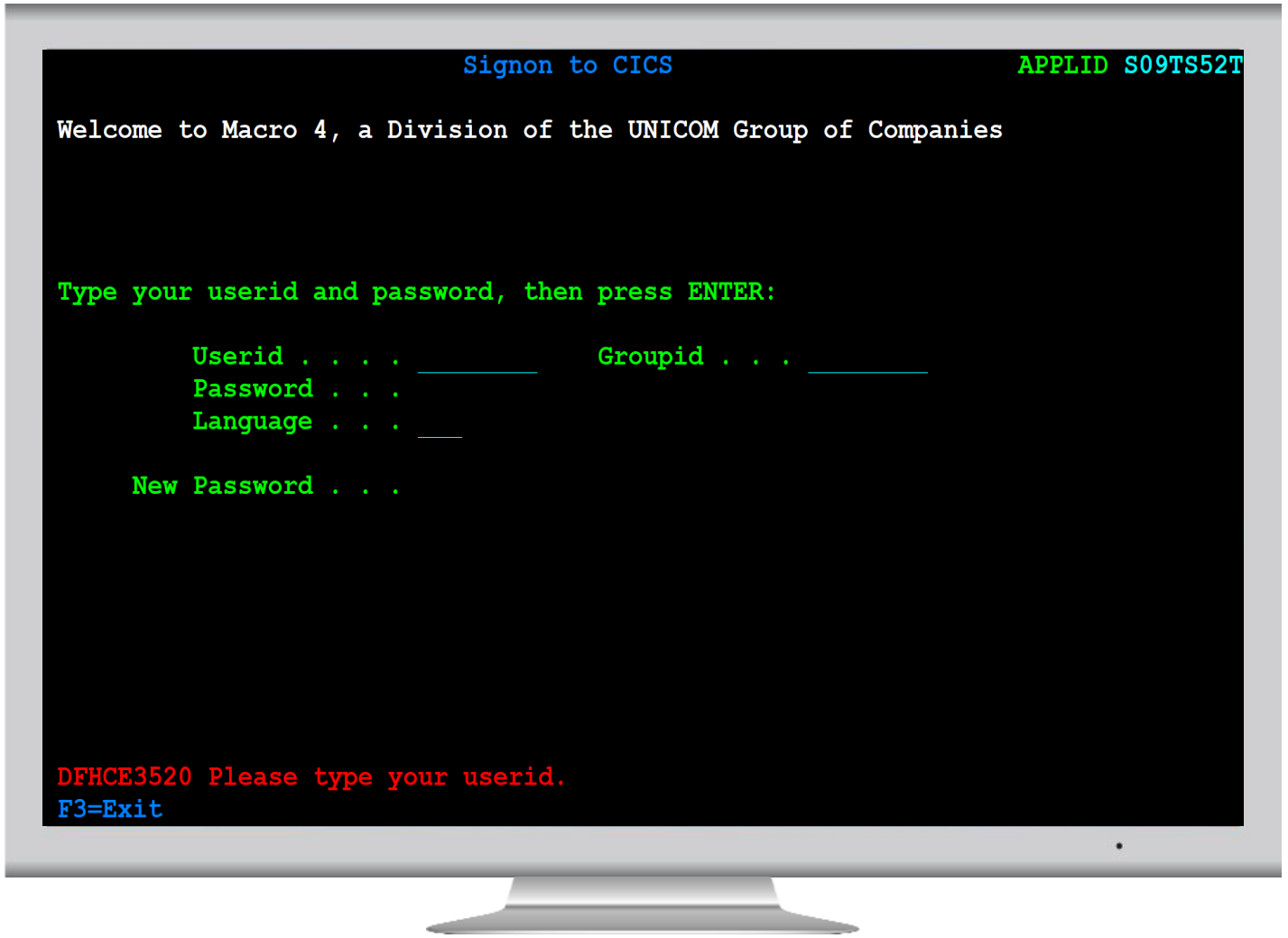
Keith Banham
R&D Manager – Macro 4

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.

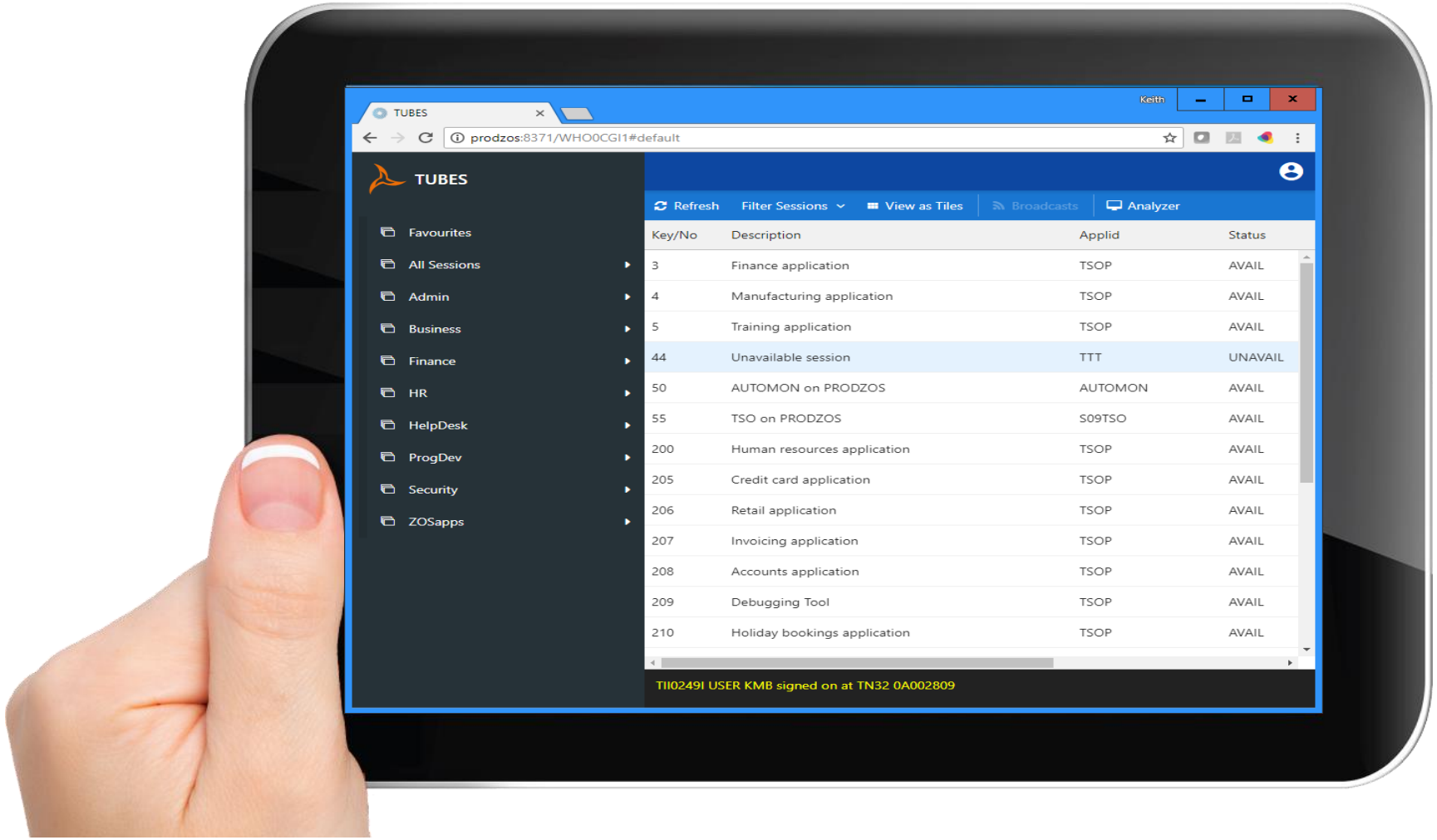
Agenda

- 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



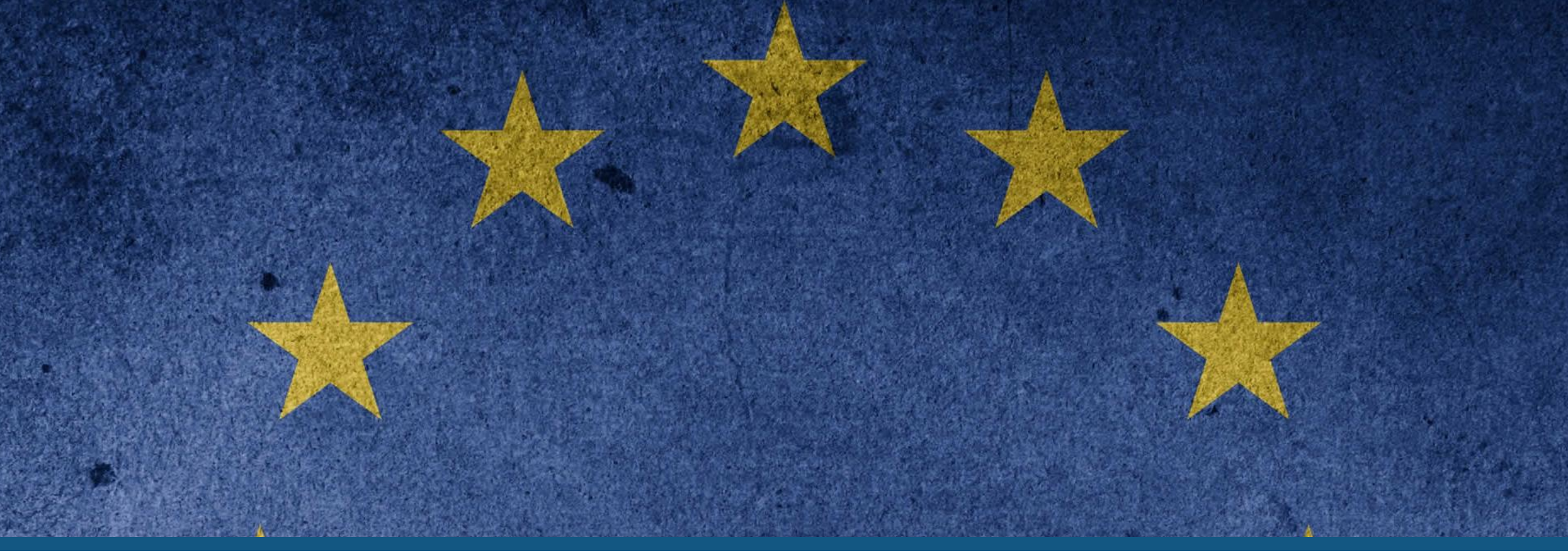
MACRO 4
A Division of UNICOM Global

Non-IT user accessing on the move

MACRO 4
A Division of UNICOM Global

Accessing sensitive data

MACRO 4
A Division of UNICOM Global



GDPR COMPLIANCE

Effective information governance

MACRO|4
A Division of UNICOM Global

What is GDPR compliance?

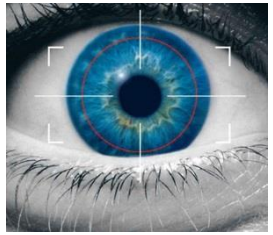
- General Data Protection Regulation
- May 2018
- Protect personal data
- Not just EU companies affected
- Accountability & Governance
- Informed consent
- Increased rights
  - Access, corrections, deletion
  - Free of charge
- Tougher fines
- Need to control access!
  - Needs Multi-Factor Authentication

Agenda

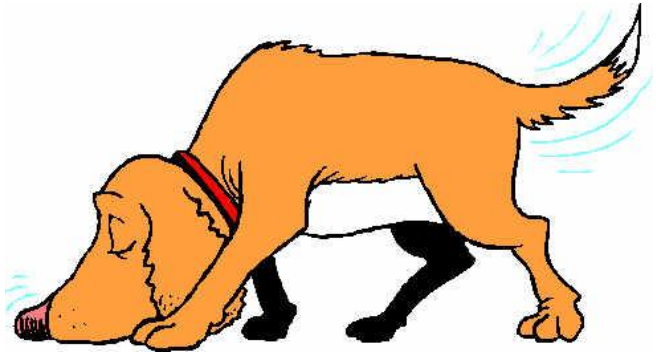
- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- MFA – Why?
- MFA – How?
- Summary and Q&A

It's not biometrics

- Finger print?
- Eye scanner?



- Static data!
- Can be line sniffed, traced and reused



MACRO|4
A Division of UNICOM Global

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!

MACRO 4
A Division of UNICOM Global

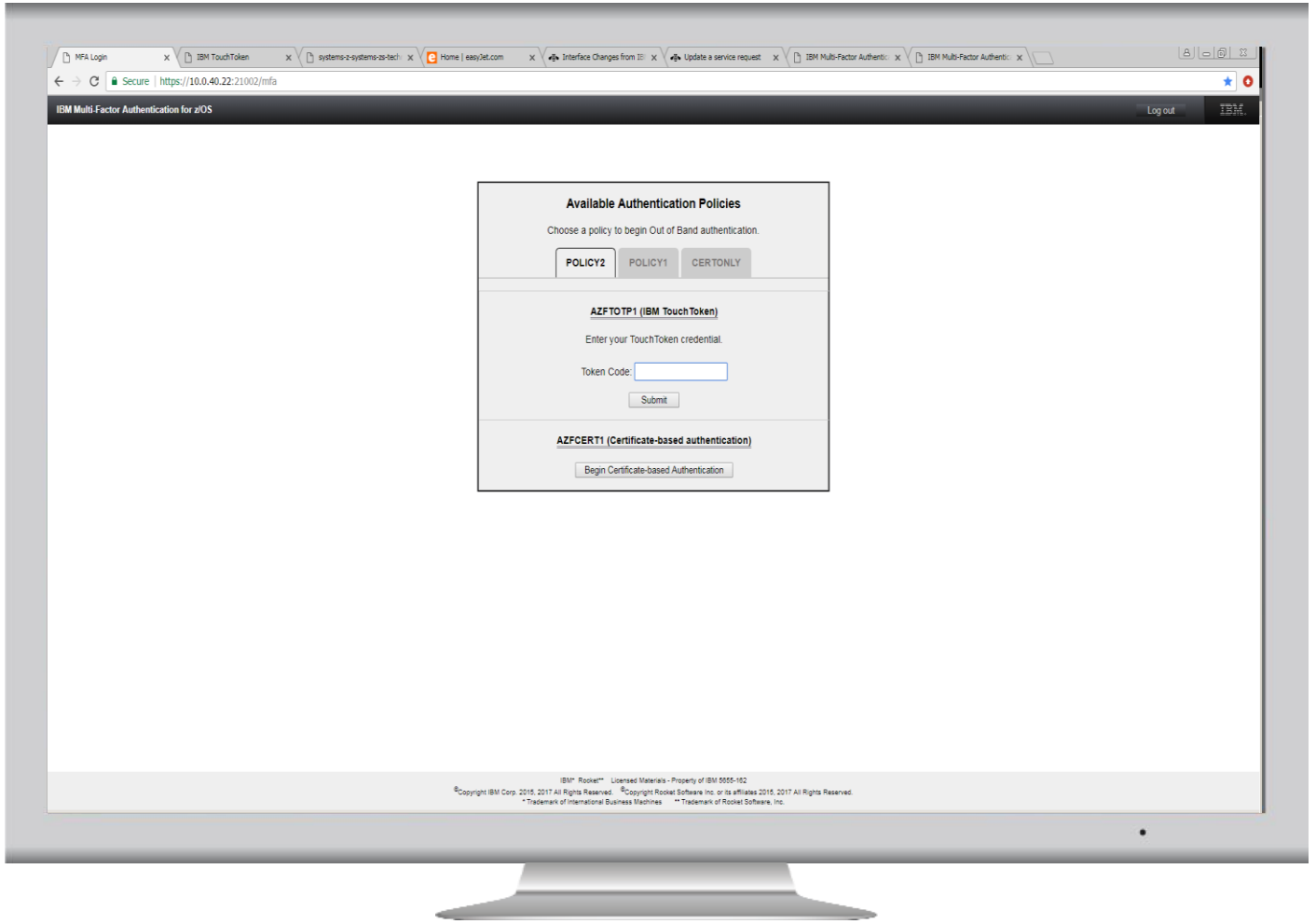
MFA – "Out-of-band"

- 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

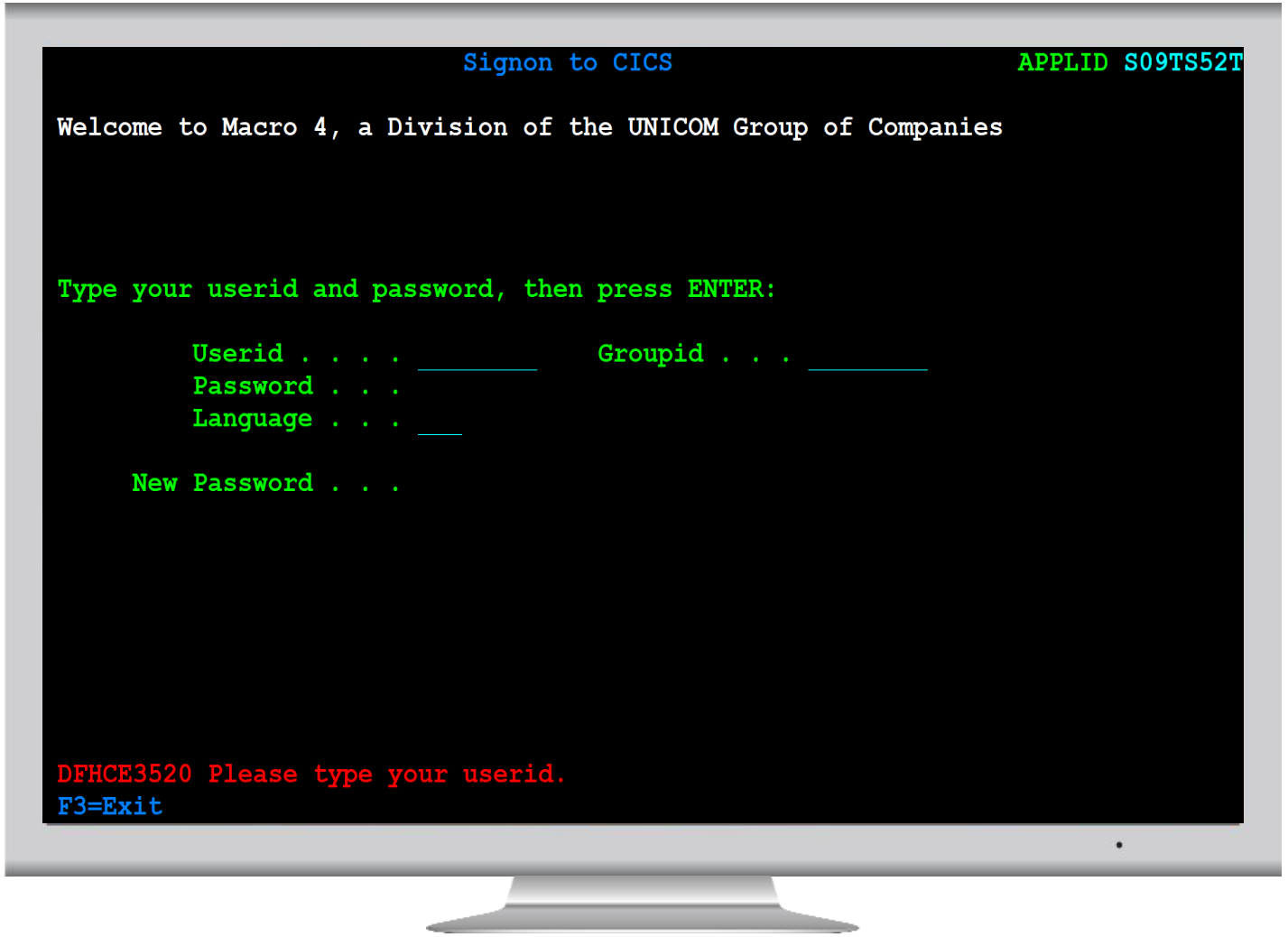
- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- MFA – Why?
- MFA – How?
- Summary and Q&A

Why do you need MFA?

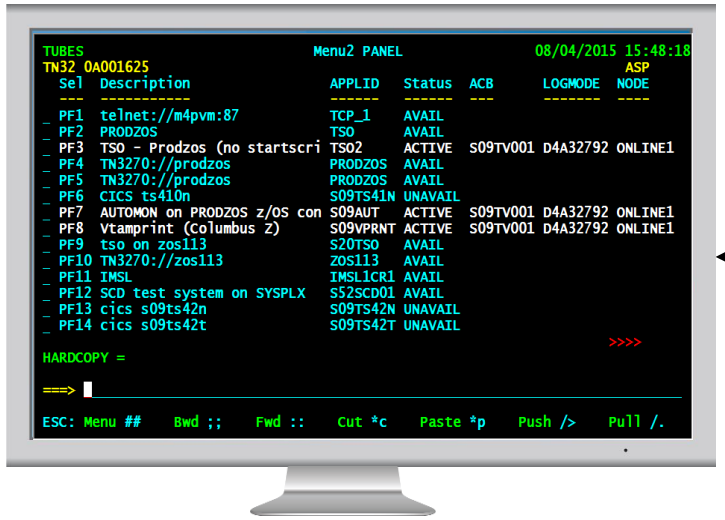
Agenda

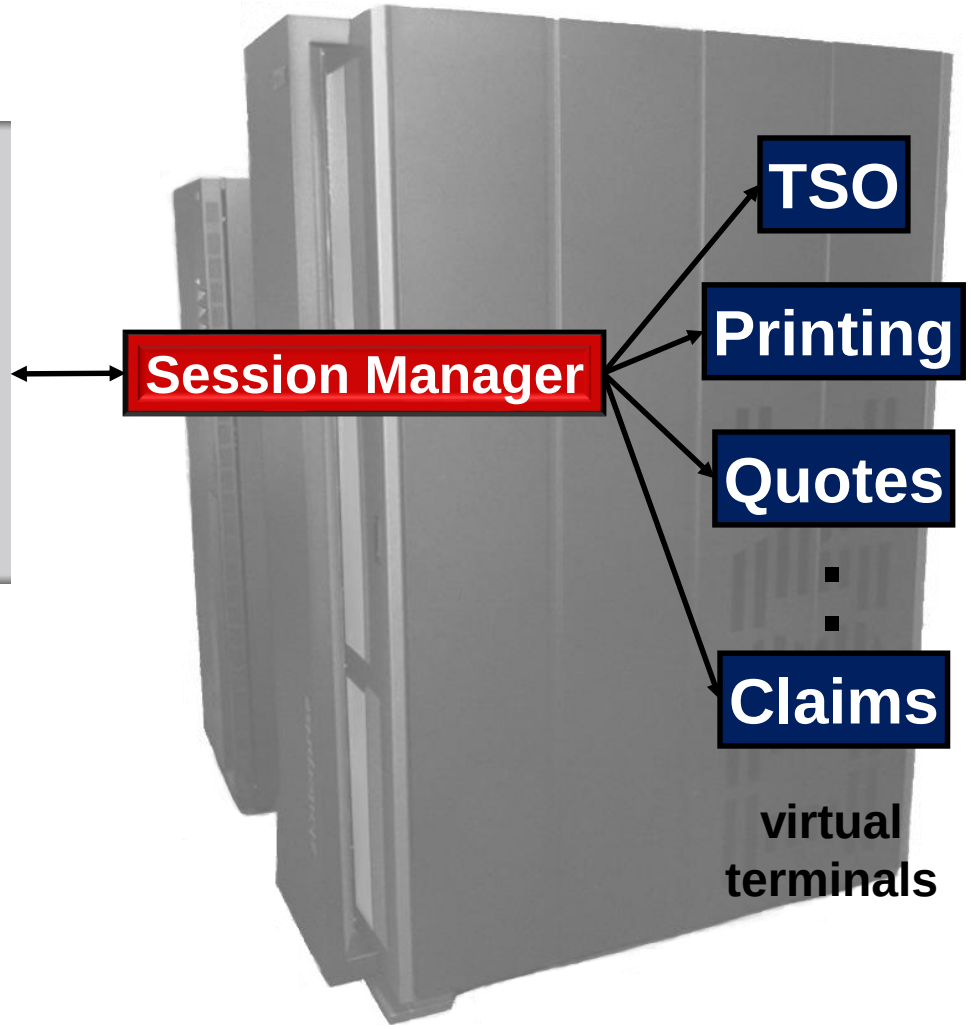
- Single Factor Authentication (SFA) - what is the problem?
- MFA – What?
- MFA – Why?
- MFA – How?
- Summary and Q&A

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?

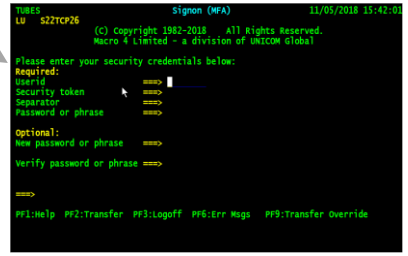
Acquire local security token

Enter security token, separator and password

External security manager passes security token to MFA server

MFA server passes security token to specific token server

Access security token server



IBM RACF

If OK, logon to your Session Manager

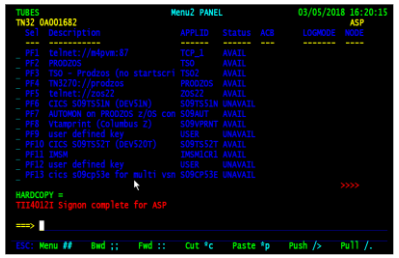
MFA result returned to your Session Manager

MFA status returned

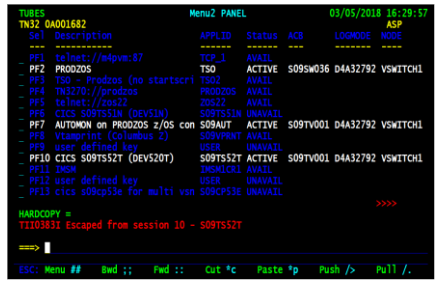
Security token status returned

Example

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



Request Passticket

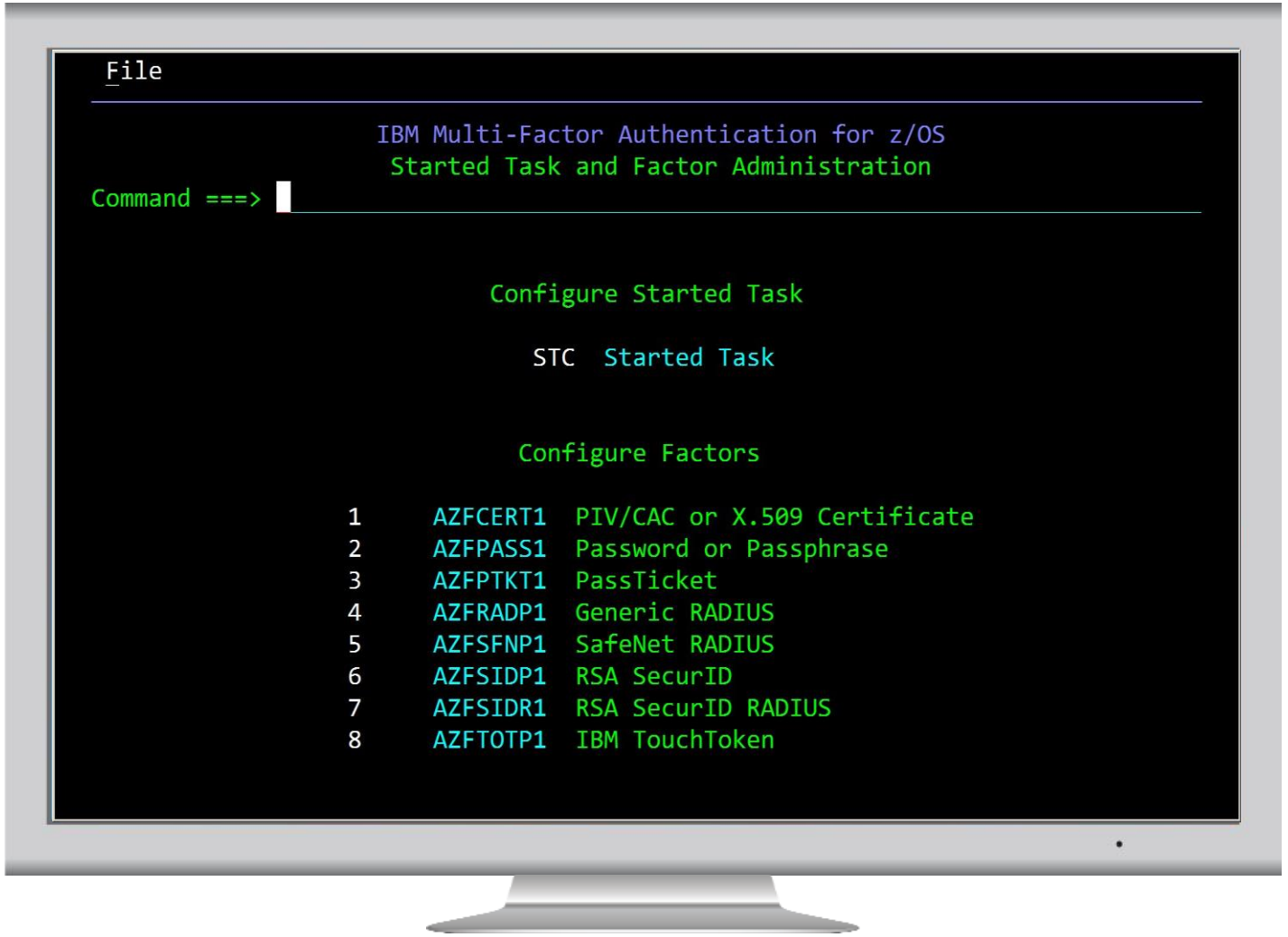


Passticket gives access to all applications with a single, secure logon

* Other ESMs and MFA solutions are available

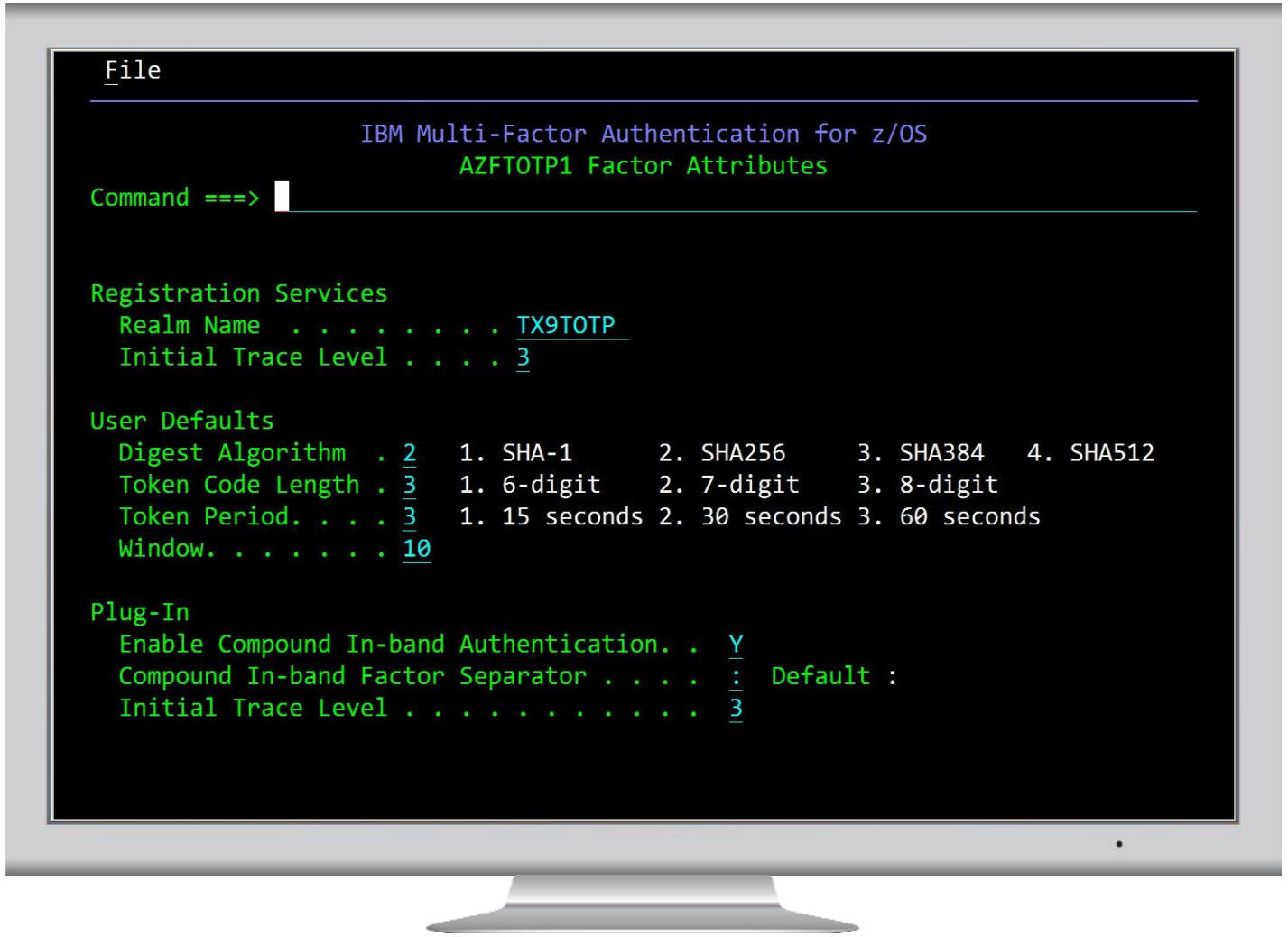
MACRO 4
A Division of UNICOM Global

MFA options – AZFEXEC command

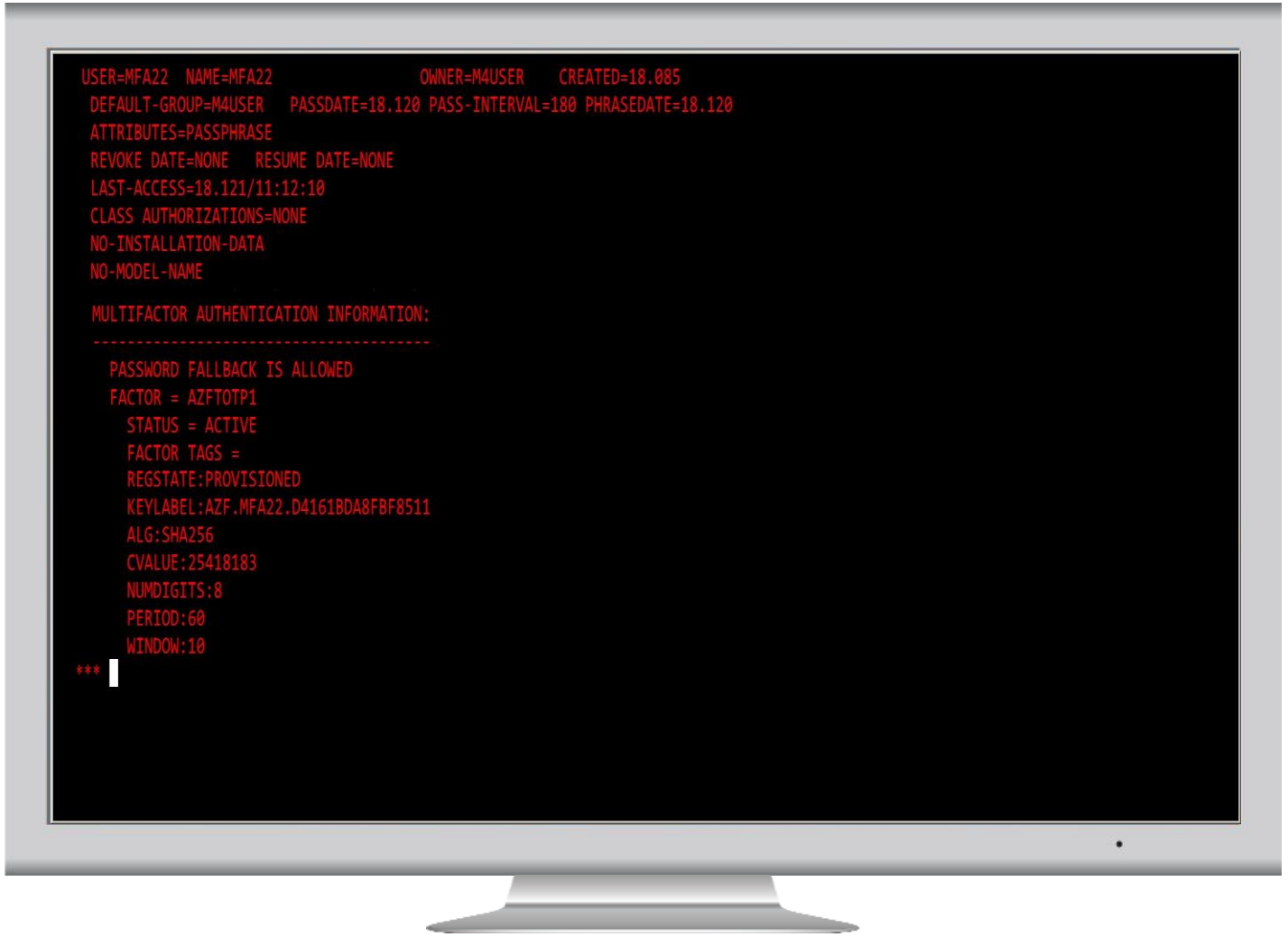


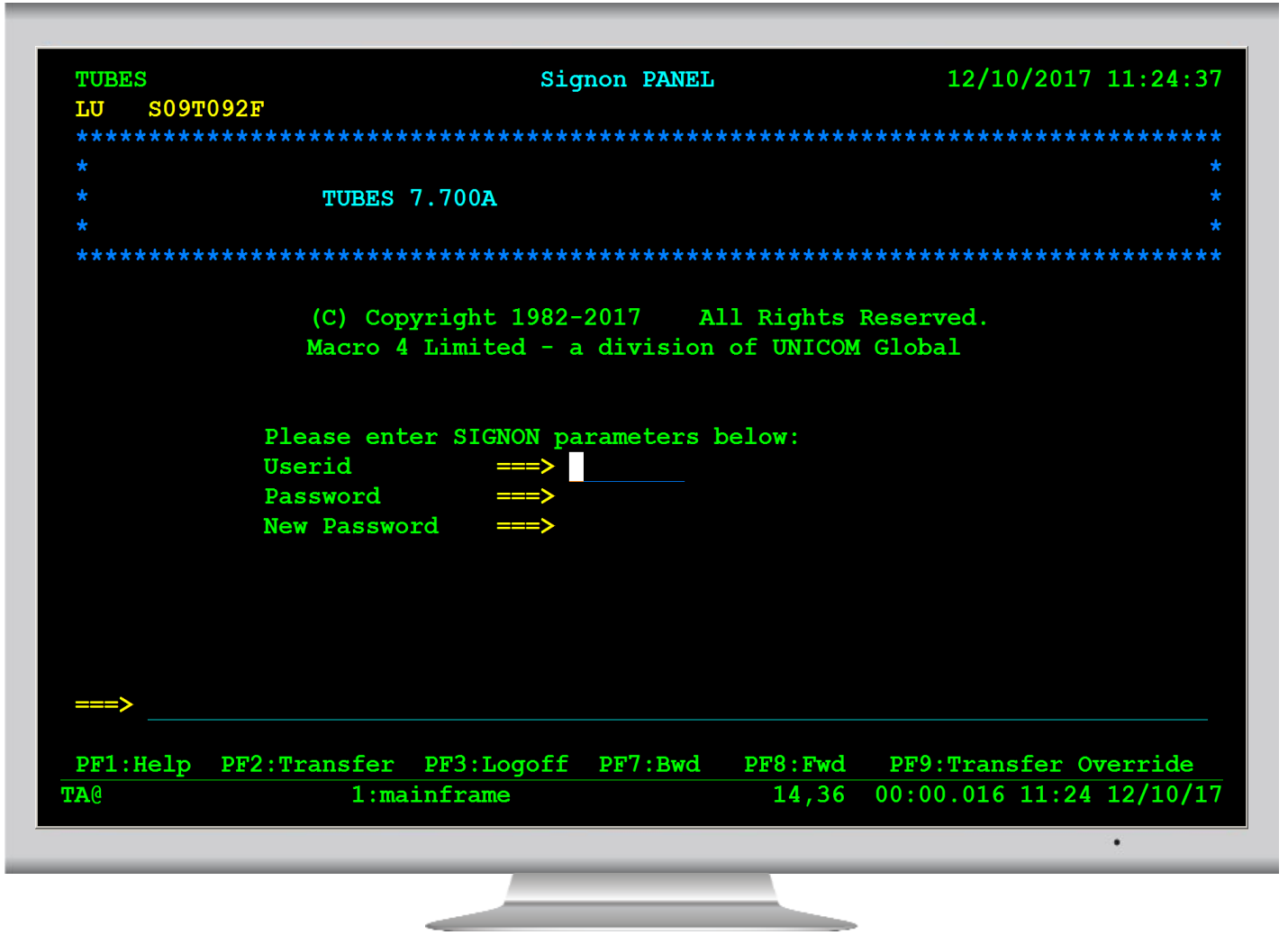
MACRO 4
A Division of UNICOM Global

AZFTOTP1 option



LISTUSER command

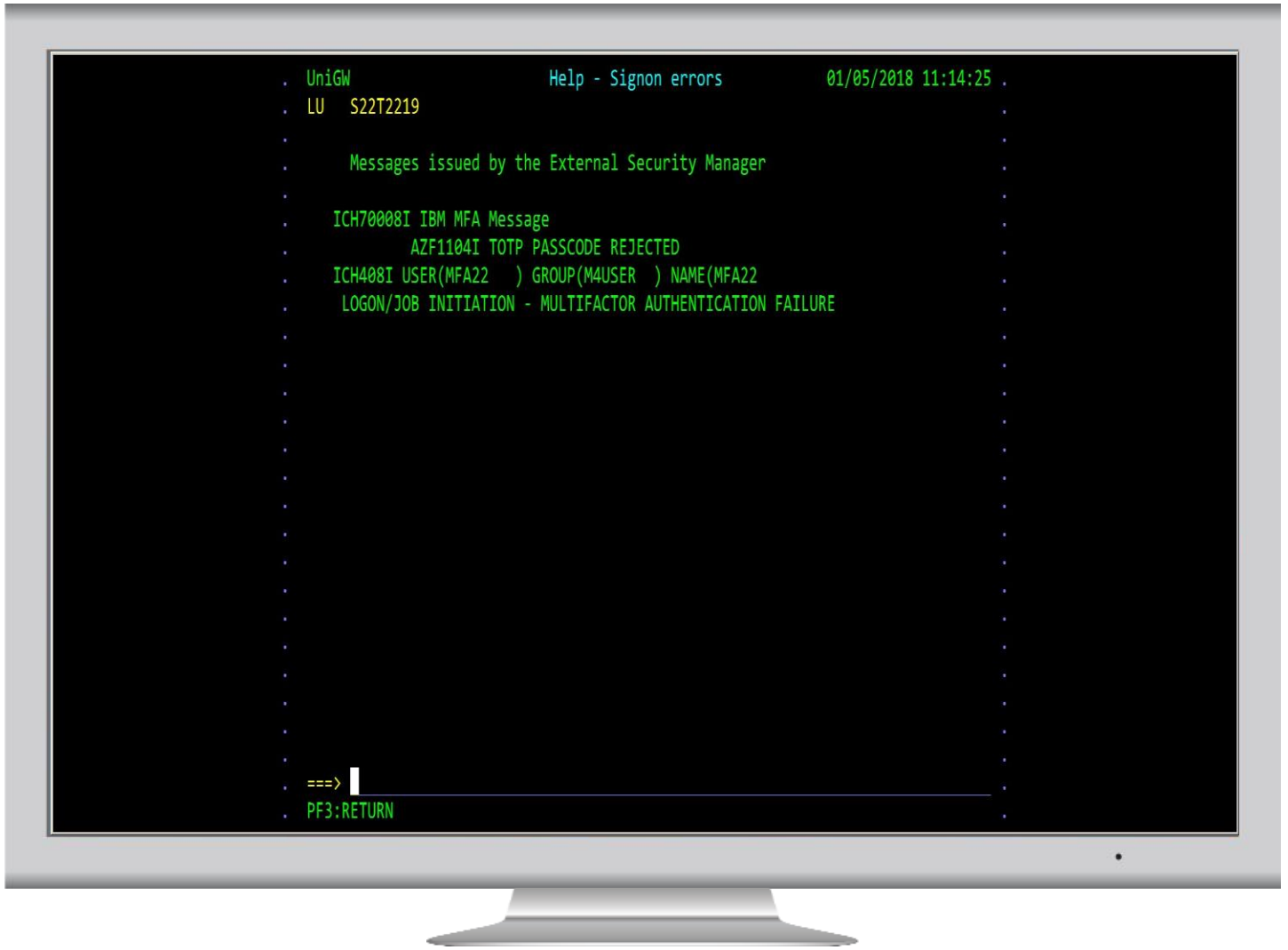




MFA “In-Band” security

Invalid credentials

MFA error messages



MACRO 4
A Division of UNICOM Global

Still utilise PassTickets

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

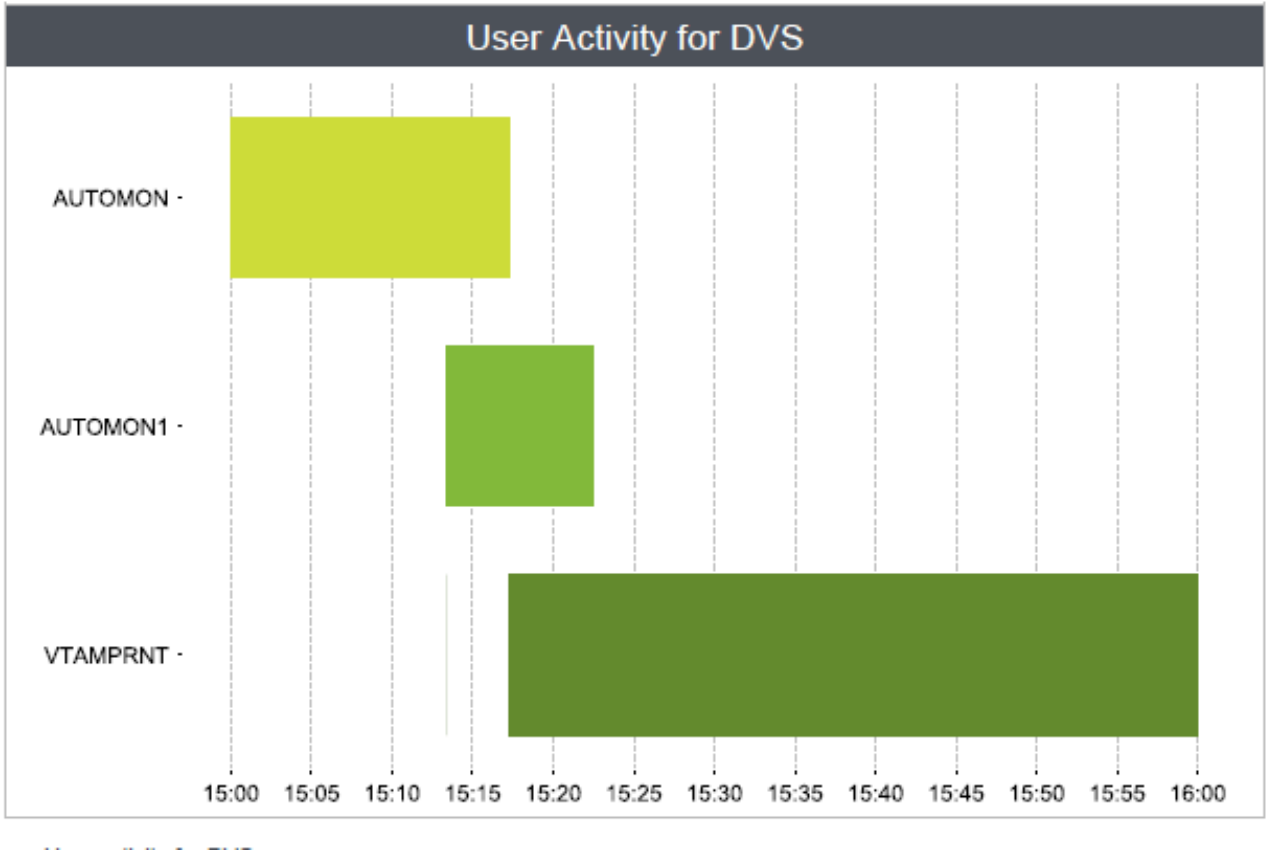
There is a fall back option

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

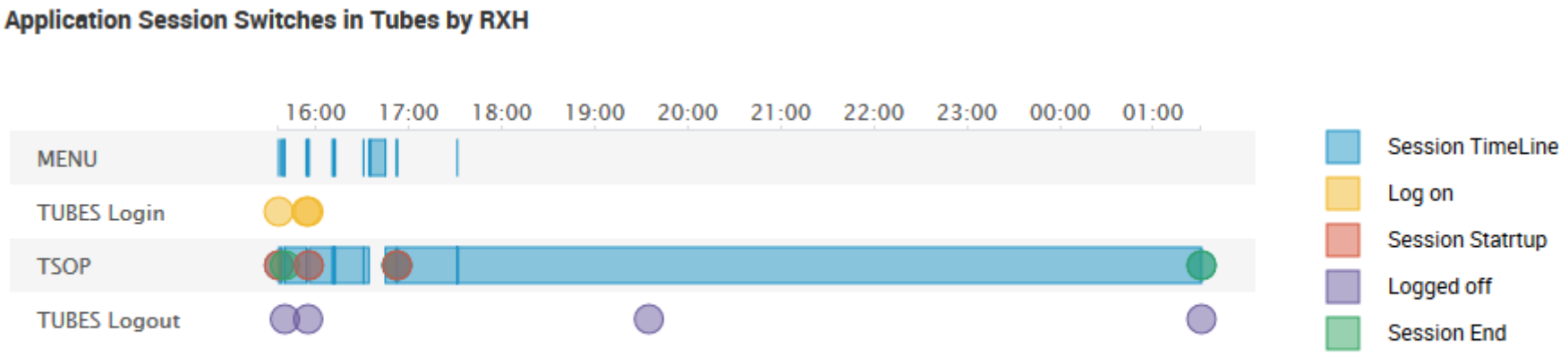
Auditing

- 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



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!

MACRO 4
A Division of UNICOM Global

ANY QUESTIONS?

Summary

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

THANK YOU

keith.banham@macro4.com

MACRO 4
A Division of UNICOM Global