



IBM Systems

Guide Share Europe

March 2010

Recent Password Phrase Support (z/OS V1R10)

Eric Rosenfeld

Email Address: rosenfel@us.ibm.com

Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.

Session Objectives

- Describe changes related to Password Phrase support
 - Overview of updated support
 - How RACF changed
 - What changed in other components

What RACF External Are Affected?

- RACROUTE REQUEST=VERIFY allow
PASSWORD=PassTicket and NEWPHRASE=, without
requiring PHRASE=
- New field added to the User KERB segment (List only)
 - Reports on key source (password or password phrase)

Other RACROUTE Enhancements

- SETROPTS PASSWORD(WARNING(n)) support for password phrase
 - Now that TSO provides password phrase support in R10, wouldn't you like to see:
ICH70002I YOUR PASSWORD PHRASE WILL EXPIRE IN 10 DAYS
- Lift the restriction that ICH70001I and ICH70002I are not returned when MSGRTRN= and ACEE= are specified on RACROUTE REQUEST=VERIFY/X
 - Informal customer requirements voiced
- Fail a “passtingy mismatch” instead of ignoring it
 - E.g. PASSWORD=,NEWPHRASE=, or, PHRASE=,NEWPASS=
 - Ignoring it leaves ambiguous behavior in applications like LDAP. User thinks his change was accepted, but it wasn't

How RACF Password Phrase Support Changed For Kerberos

- When an administrator or end user changes **either** a password or password phrase, this becomes the current Kerberos password and keys will be generated
- This is **consistent with other products' view, like TSO/E**, that the user has a 1-100 character password
- **As before, the end user is responsible for knowing that whenever the RACF "password" changes, the Kerberos password (and key) has also changed**

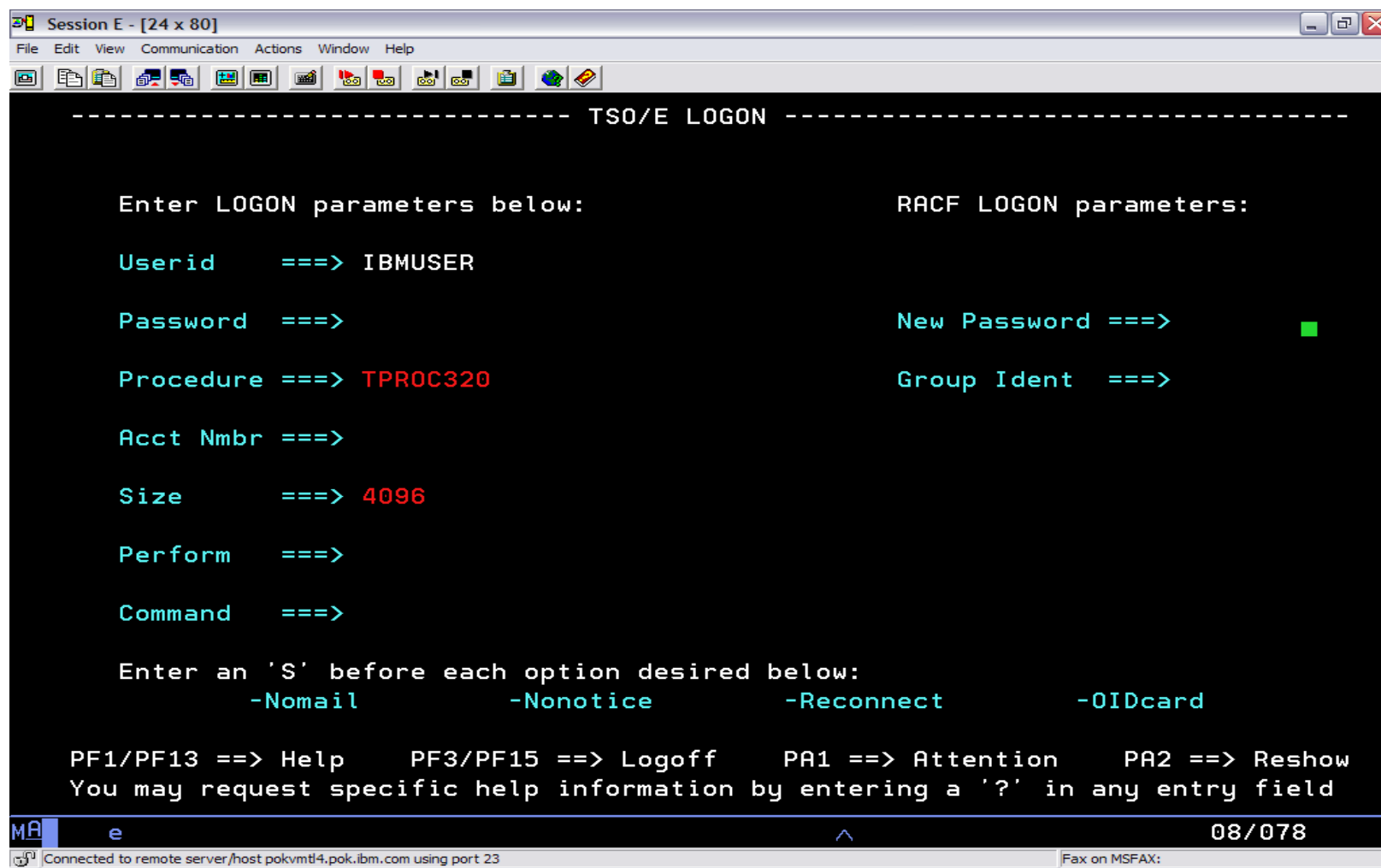
Migration & Coexistence Considerations

- Systems will require a toleration PTF to be installed for APAR OA22588 to ensure proper key processing for Kerberos
 - z/OS V1R6 UA39331
 - z/OS V1R7 UA39332
 - z/OS V1R8 UA39333
 - z/OS V1R9 UA39334

TSO/E Updates

- Using [this line item](#), the customer can:
 1. Logon with either a password or a password phrase
 2. Change the setting dynamically via an IKJTSOxx update
 - Activated by the following to the IKJTSOxx member:
 - LOGON PASSPHRASE(ON)
- Value:
 1. New panel still allows for eight character or less passwords
 2. Changes can be made without an IPL and easily displayed

Password change with PASSPHRASE(OFF) – Step 1



The screenshot shows a terminal window titled "Session E - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main display area is black with white and red text. It shows the "TSO/E LOGON" prompt and two columns of input fields. The left column is for "LOGON parameters" and the right column is for "RACF LOGON parameters". The user has entered "IBMUSER" for the Userid, "TPROC320" for the Procedure, and "4096" for the Size. The RACF parameters include "New Password" and "Group Ident". At the bottom, there are instructions for using function keys (PF1/PF13 for Help, PF3/PF15 for Logoff, PA1 for Attention, PA2 for Reshow) and a note about entering a '?' for help. The terminal status bar at the bottom shows "MR e" on the left, "08/078" on the right, and "Connected to remote server/host pokvmt14.pok.ibm.com using port 23" and "Fax on MSFAX:" at the very bottom.

```
----- TSO/E LOGON -----  
  
Enter LOGON parameters below:                                RACF LOGON parameters:  
  
Userid    ==> IBMUSER                                        New Password ==>   
  
Password  ==>                                             Group Ident  ==>   
  
Procedure ==> TPROC320  
  
Acct Nbr  ==>   
  
Size      ==> 4096  
  
Perform   ==>   
  
Command   ==>   
  
Enter an 'S' before each option desired below:  
          -Nomail          -Nonotice          -Reconnect          -OIDcard  
  
PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow  
You may request specific help information by entering a '?' in any entry field  
  
MR e 08/078  
Connected to remote server/host pokvmt14.pok.ibm.com using port 23 Fax on MSFAX:
```

Password change with PASSPHRASE(OFF) – Step 2

```
Session E - [24 x 80]
File Edit View Communication Actions Window Help
----- TSO/E LOGON -----
IKJ56447A Reenter the new password in the NEW PASSWORD field for verification

Enter LOGON parameters below:                                RACF LOGON parameters:

Userid    ==> IBMUSER
Password  ==>
Procedure ==> TPROC320
Acct Nbr  ==>
Size      ==> 4096
Perform   ==>
Command   ==>

Enter an 'S' before each option desired below:
      -Nomail      -Nonotice      -Reconnect      -OIDcard

PF1/PF13 ==> Help   PF3/PF15 ==> Logoff   PA1 ==> Attention   PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

MR e 08/071
Connected to remote server/host pokvmt14.pok.ibm.com using port 23 Fax on MSFAX:
```

Password change with PASSPHRASE(ON) – Step 1

```

Session E - [24 x 80]
File Edit View Communication Actions Window Help
----- TSO/E LOGON -----
IKJ56714A Enter current password for IBMUSER

Enter LOGON parameters below:                RACF LOGON parameters:

Userid    ==> IBMUSER
Password  ==>
Procedure ==> TPROC320
Group Ident ==>

Acct Nbr  ==>
Size      ==> 4096
Perform   ==>
Command   ==>

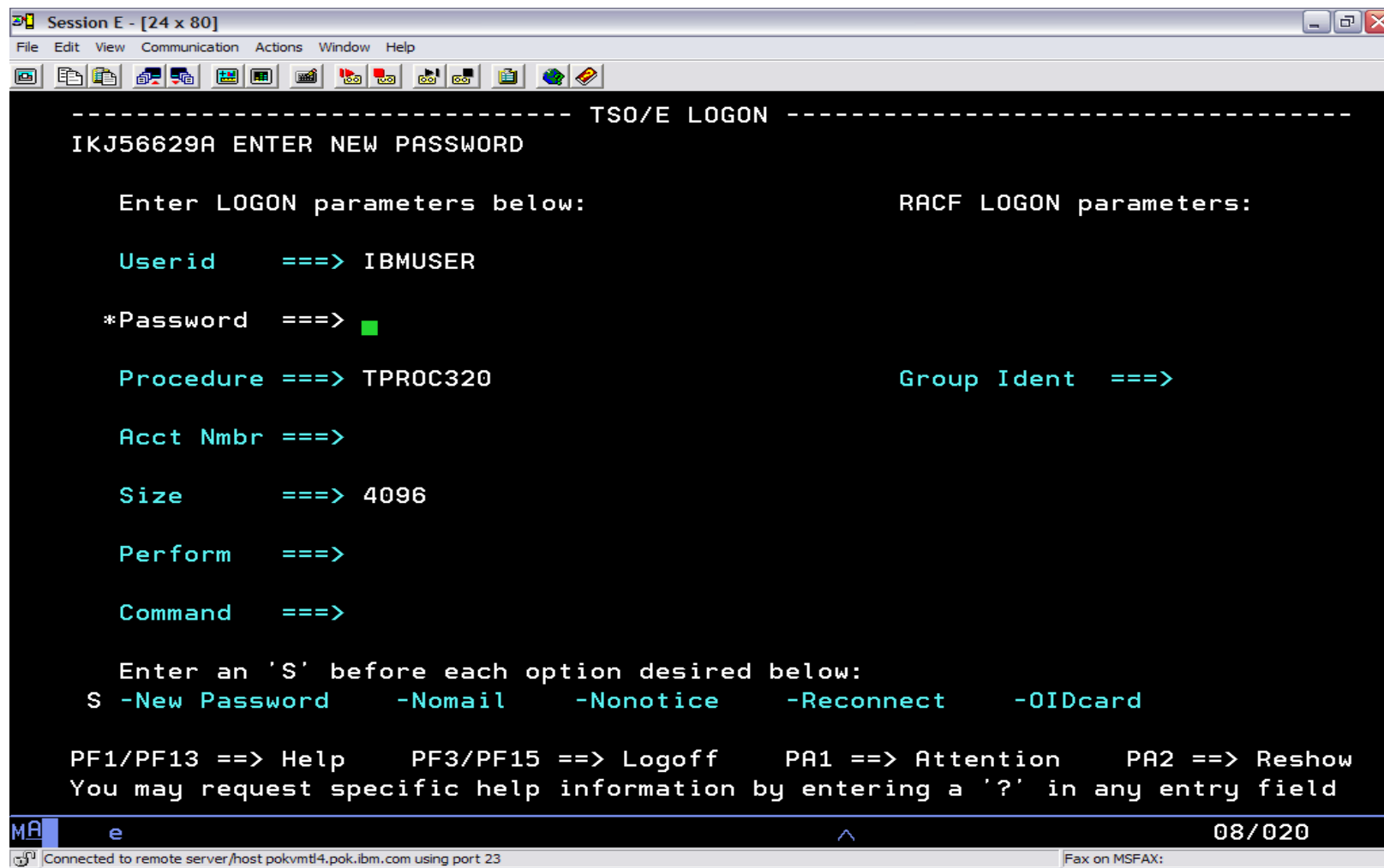
Enter an 'S' before each option desired below:
S -New Password  -Nomail  -Nonotice  -Reconnect  -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff  PA1 ==> Attention  PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

MR e 09/039
Connected to remote server/host pokvmt14.pok.ibm.com using port 23 Fax on MSFAX:

```

Password change with PASSPHRASE(ON) – Step 2



The screenshot shows a terminal window titled "Session E - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main content is a TSO/E LOGON prompt for user IKJ56629A. The prompt asks for LOGON parameters and RACF LOGON parameters. The user has entered: Userid (IBMUSER), *Password (redacted), Procedure (TPROC320), Acct Nmbr, Size (4096), Perform, and Command. Below the parameters, there are options to select: S -New Password, -Nomail, -Nonotice, -Reconnect, and -OIDcard. At the bottom, there are function key instructions: PF1/PF13 ==> Help, PF3/PF15 ==> Logoff, PA1 ==> Attention, and PA2 ==> Reshow. A footer bar shows "MR e" on the left, a cursor in the middle, and "08/020" on the right. The status bar at the bottom indicates "Connected to remote server/host pokvmt14.pok.ibm.com using port 23" and "Fax on MSFAX:".

```
----- TSO/E LOGON -----
IKJ56629A ENTER NEW PASSWORD

Enter LOGON parameters below:                RACF LOGON parameters:

Userid    ==> IBMUSER

*Password ==> █

Procedure ==> TPROC320                Group Ident ==>

Acct Nmbr ==>

Size      ==> 4096

Perform   ==>

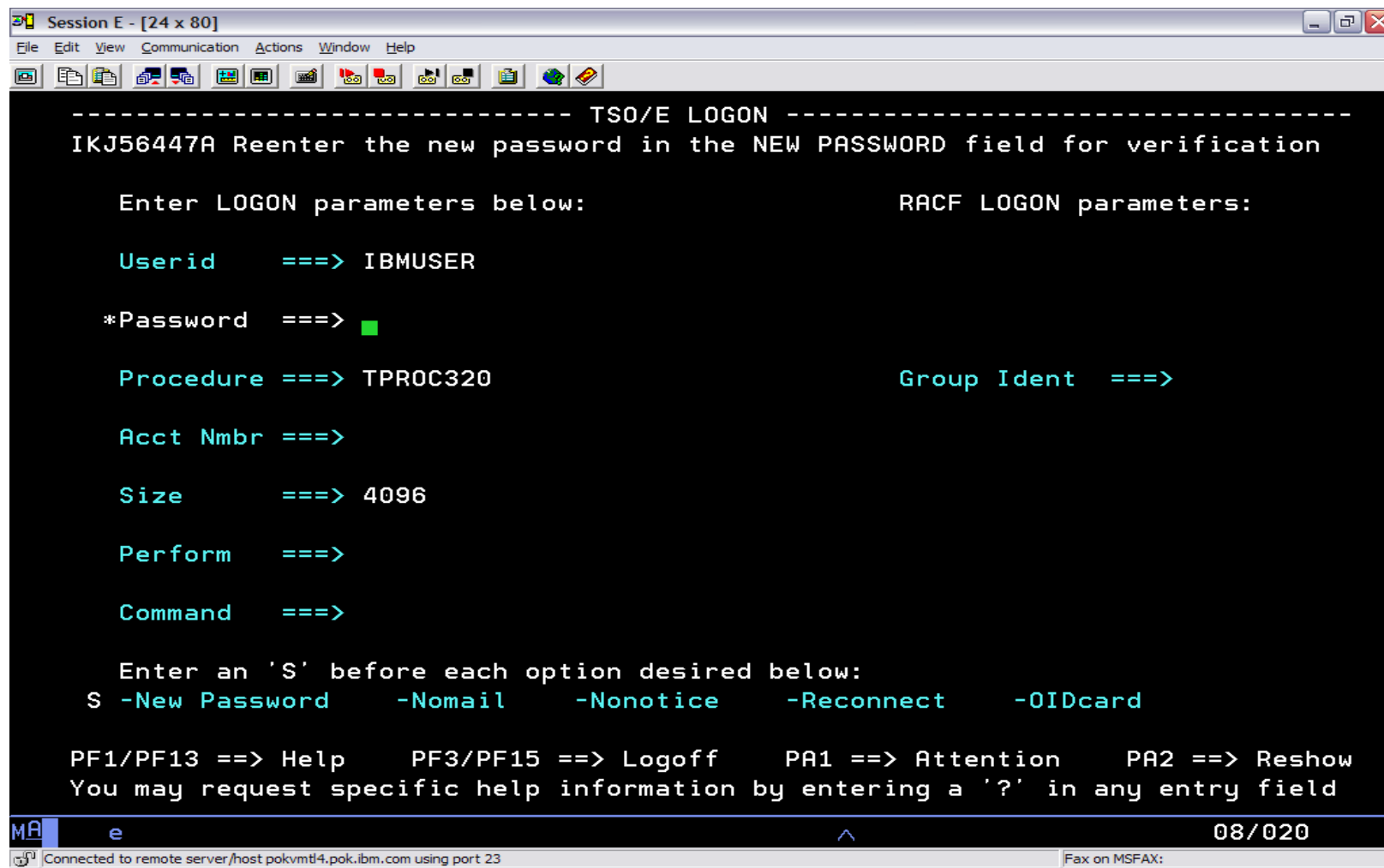
Command   ==>

Enter an 'S' before each option desired below:
S -New Password  -Nomail  -Nonotice  -Reconnect  -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff   PA1 ==> Attention   PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

MR e                                     08/020
Connected to remote server/host pokvmt14.pok.ibm.com using port 23  Fax on MSFAX:
```

Password change with PASSPHRASE(ON) – Step 3



The screenshot shows a terminal window titled "Session E - [24 x 80]" with a menu bar (File, Edit, View, Communication, Actions, Window, Help) and a toolbar. The main display area contains the following text:

```
----- TSO/E LOGON -----  
IKJ56447A Reenter the new password in the NEW PASSWORD field for verification  
  
Enter LOGON parameters below:                                RACF LOGON parameters:  
  
Userid      ==> IBMUSER  
*Password   ==>   
Procedure   ==> TPROC320                                Group Ident ==>  
  
Acct Nbr    ==>  
  
Size        ==> 4096  
  
Perform     ==>  
  
Command     ==>  
  
Enter an 'S' before each option desired below:  
S -New Password   -Nomail   -Nonnotice   -Reconnect   -OIDcard  
  
PF1/PF13 ==> Help    PF3/PF15 ==> Logoff   PA1 ==> Attention  PA2 ==> Reshow  
You may request specific help information by entering a '?' in any entry field
```

At the bottom of the terminal, there is a status bar with "MR" on the left, "e" in the center, and "08/020" on the right. Below the terminal window, a connection bar shows "Connected to remote server/host pokvmt14.pok.ibm.com using port 23" and "Fax on MSFAX:".

Migration & Coexistence Considerations

- Check logon exits (IKJEFLD, IKJEFLD1, IKJEFLN1, and IKJEFLN2)
 - Should allow 100 character passwords and new passwords
 - IKJEFLD also needs to allow for a new maximum size of 255
- Check any custom logon panels
 - Need to look at IKJLQENU not just IKJLPENU
- Toleration APAR OA20525 allows the new LOGON statement in the IKJTSoxx parmlib member to be ignored on lower levels and ensures correct output for the PARMLIB LIST ROUTE command
 - UA39737 (HTE7709)
 - UA39738 (HTE7730)
 - UA39739 (HTE7740)

UNIX System Services/LE

- Password phrase support is added to the following services
 - z/OS UNIX Assembler callable services
 - BPX1PWD/BPX4PWD
 - BPX1TLS/BPX4TLS
 - BPX1SEC/BPX4SEC
 - C Functions
 - __passwd() / __passwd_applid()
 - pthread_security_np() / pthread_security_applid_np()
 - __login() / __login_applid()

LDAP Password Phrase Use

- During bind
 - Can use a RACF password phrase instead of a password in any bind involving RACF
 - Can be changed specifying old and new phrase

- Changelog support
 - RACF creates separate changelog entry when password phrase changed
 - SDBM search specifying new **racfPassPhraseEnvelope** attribute retrieves password phrase envelope from RACF

Additional Updates

- Password phrase support is added to the following:
 - rlogin
 - passwd
 - su
 - OpenSSH

QUESTIONS?