

DLA J62D Information Operations DSS CAC Enablement (MUA) End-User Guide for z/OS

September 2016



Table of Contents

1.0 INTRODUCTION	3
2.0 BACKGROUND	3
3.0 LIMITATIONS	4
3.1 MULTIPLE USERID ON A DSS LPAR.....	4
3.2 USERID / PASSWORD MAINTENANCE WHEN USING FTP, QMF, MFEEEE, DSS WEB &.....	4
CA-DISPATCH. (NON-CAC APPLICATIONS)	4
4.0 PREREQUISITES	6
5.0 *** CAC ENABLE LOGIN FLOW: END-TO-END USER CAC ENABLEMENT ***	7
6.0 CAC ENABLED SIGN-OUT INSTRUCTIONS FOR DSS MULTI-USER WORKSTATIONS	12
7.0 DSS LU NOT DEFINED TO WORKSTATION (ERROR MESSAGE)	14
7.1 CL SUPERSESSION ERROR MESSAGE (CS031).....	15
7.2 SESSION TIMEOUT MESSAGE	16
8.0 FREQUENTLY ASKED QUESTIONS	18

1.0 Introduction

This document is a training tool and reference guide for all DSS end-users who possess a Common Access Card (CAC) to access IBM z/OS MUA mainframe DSS application(s) via the Multi-Host Internet Access Portal (MIAP). Within this document are the instructions on using DISA's (Defense Information Systems Agency) solution for accessing the DISA hosted DSS mainframe application(s) on MUA, that have a CAC enabled logon.

2.0 Background

DoD is moving toward the elimination of the "USERID" or user account authentication and is now requiring PKI certificate authentication per CTO 07-015. This requirement has proven problematic for authentication to IBM z/OS mainframe applications since the mainframe still requires the use of a "USERID" in the host's local access control product (ACP). For DSS this is the IBM RACF Security System.

DISA has provided a simplified logon process for customers to use digital certificates for authentication purposes to the IBM z/OS mainframe legacy applications, such as TSO, CICS, DB2, and other online interfaces. DISA has leveraged the use of "pass-tickets" available within the existing mainframe product suite and MIAP Express Logon macros to enable the use of CAC logins for DSS on the z/OS MUA mainframe.

DISA has also implemented a CAC registration process which includes a self-service password reset facility also known as zPAT, in order to reduce the direct or indirect cost for the management of application USERIDs for account password resets with a DSS system registered CAC.

3.0 Limitations

Although the DISA solution was created to enable the widespread use of CAC logins to IBM z/OS mainframe applications, there are some limitations. To utilize this solution, DSS users **must have** a valid DoD Common Access Card (CAC) and use MIAP to access DSS applications on MUA. Other limitations are listed below.

3.1 Multiple USERID on a DSS LPAR

CAC logins are a **one-to-one relationship** that uses only **one** USERID per **logical partition (LPAR)** or Mainframe environment. A CAC login to an IBM z/OS mainframe requires users to register the digital certificate on their CAC against the current USERID that is already established for the DSS application and is registered in the RACF Security Systems on MUA. This is a **one-to-one relationship** where the digital certificate **can only be** registered to **one** USERID per RACF security database or DSS mainframe security system.

Therefore, if a user has multiple USERIDs on the same DSS LPAR for multiple DSS applications, they can only perform **one** CAC login to **one** DSS application on that LPAR. A suggestion for these DSS users would be to register their CAC Identity certificate against the USERID for the application they access the **most** on that LPAR, to best utilize the CAC login process.

Login to all other DSS applications using other DSS USERIDs that are assigned to that LPAR will need to be done via a valid USERID/password combination, using a non-CAC MIAP session.

3.2 UserID / Password Maintenance when using FTP, QMF, MFEEE, DSS Web & CA-DISPATCH. (NON-CAC Applications)

The z/OS DSS CAC login solution is for **Telnet Access Only**. DSS users who need to utilize these **NON-CAC enabled product applications** will need to maintain their USERID &

Password authentication on the LPAR supporting these products, using the following password reset utility from your MUA CAC enabled CL SuperSession Menu.

This figure below shows the AUACPP01 CL SUPERSESSION PW RESET selection.

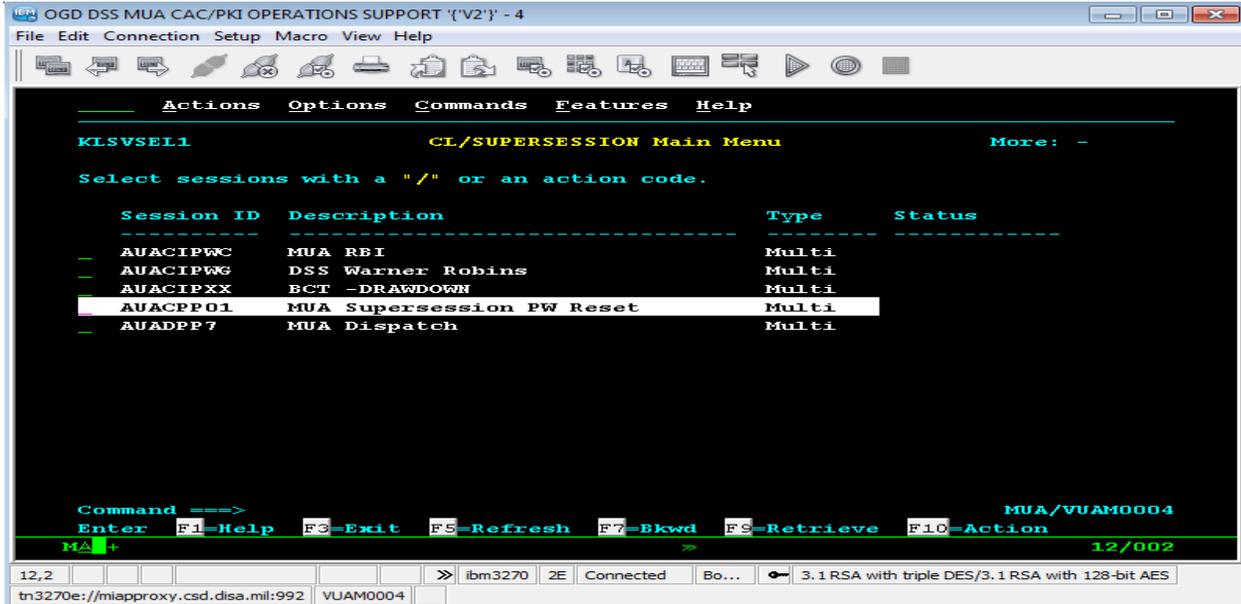


Figure 1 CL Supersession PW Reset

Once selected you will receive the MUL CL SuperSession UserID and Password Validation screen. The password field must be filled in with your OLD password and the Change Password Field must be changed to "Y" as shown below, then press <<Enter>>.

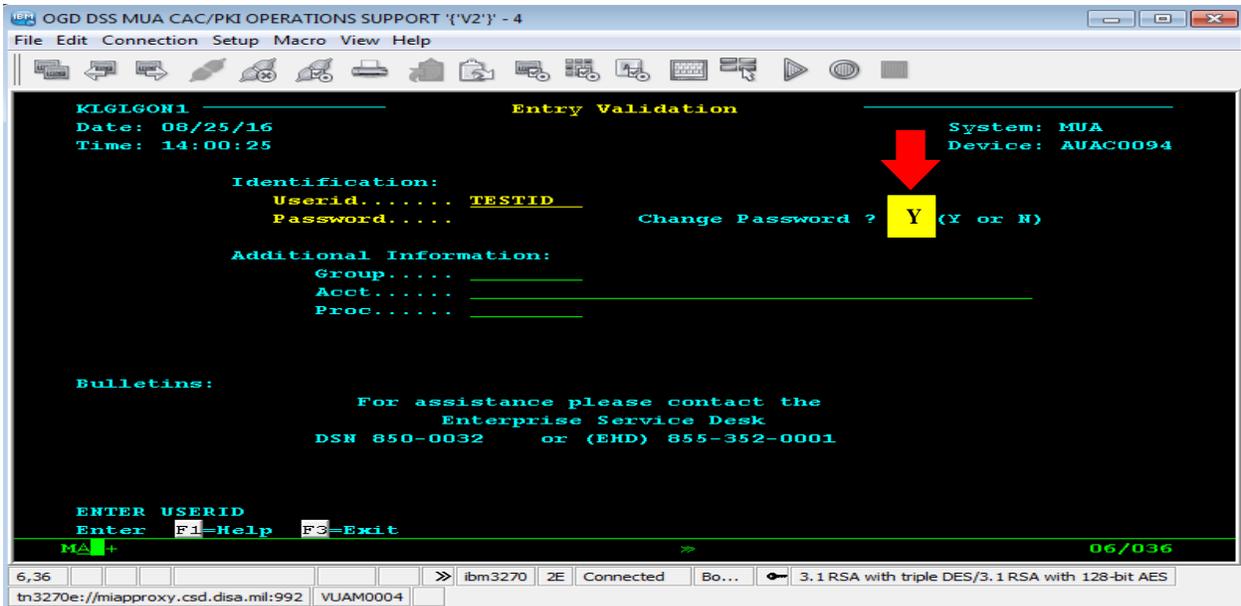


Figure 2 Entry Validation Screen

Next you will receive the following message if the password change was successful. Then Press <<Enter>> to continue.

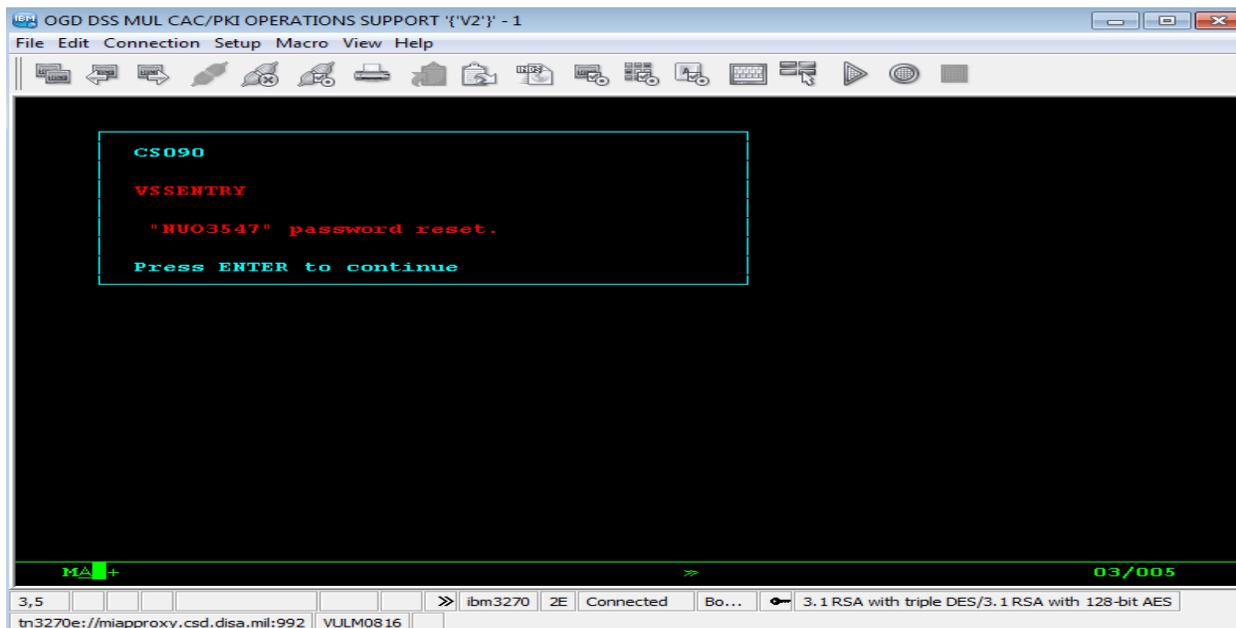


Figure 3 Password Reset Complete

4.0 Prerequisites

There are two prerequisites that are required for the DISA DSS z/OS CAC login process.

The first prerequisite requires that the targeted DSS LPAR mainframe name where the desired DSS application is hosted is the starting point and must be known. In this case, the MUA (Production) LPAR.

The second prerequisite requires that the user's CAC PKI certificate **be registered** to the DSS MUA RACF security database with a valid MUA USERID. The CAC registration process is covered in both the "*J62D DSS CAC Registration (MUA) Guide*" document and in the "*J62D DSS CAC Registration (MUA Quick-Ref)*" document.

5.0 * CAC Enable Login Flow: End-to-End User CAC Enablement *****

This section describes the DSS End-To-End User CAC Enablement for DSS Production Users connecting to the DSS MUA Mainframe.

Once the prerequisites above have been met, establish an Internet Explorer (IE) web browser session with MIAP <https://miap.csd.disa.mil/> and perform the normal DSS login process. At this point you may select either certificate, it does not matter. Use what you have used in the past.

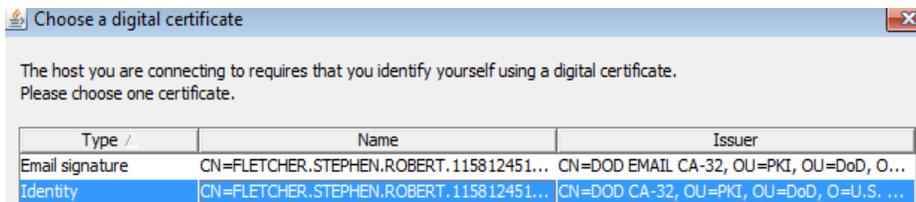


Figure 4 Certificate Selection

The list of MIAP sessions presented is based on individual user profile or MIAP Community of Interest (COI). Current DSS production end users should see something similar to the MIAP COI menu as shown in Figure 5, below.

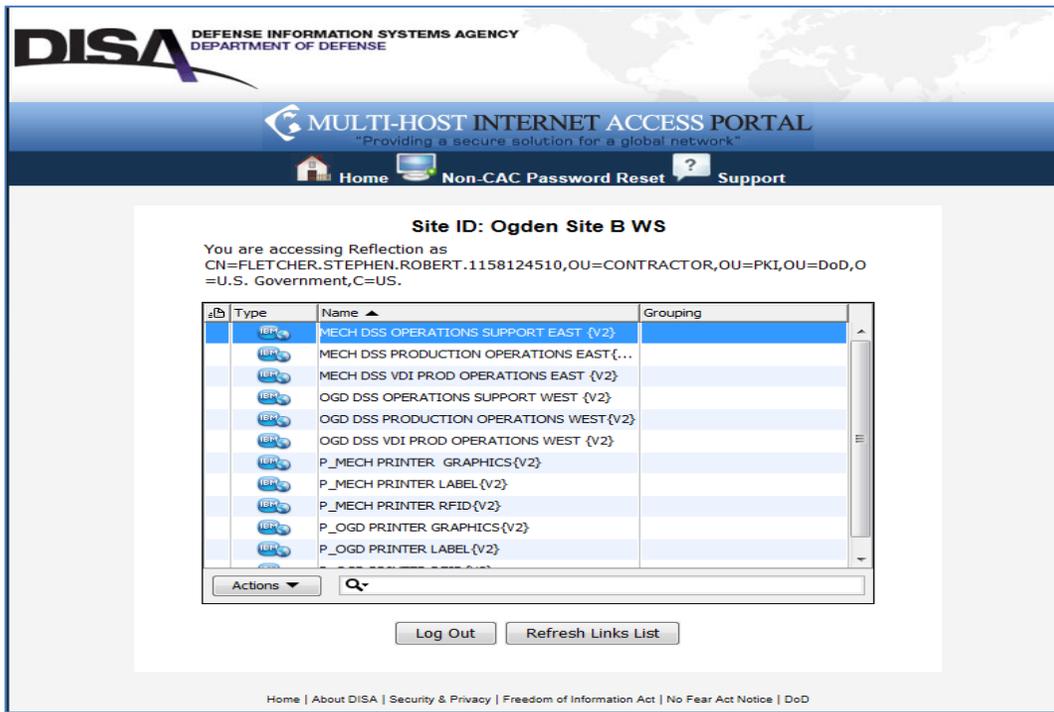


Figure 5: (Current) MIAP Community of Interest (COI) Menu

As shown below, your **new MIAP COI** menu will display various DSS CAC/PKI Selections. Find and select the “OGD DSS MUA CAC/PKI PRODUCTION OPERATION” for a static LU-Printer/Stacker/Carousel connection or “OGD DSS MUA CAC/PKI OPERATIONS SUPPORT” for a Virtual LU connection. Clicking on the name will highlight the name selected in the MIAP COI menu as shown in Figure 6, below.

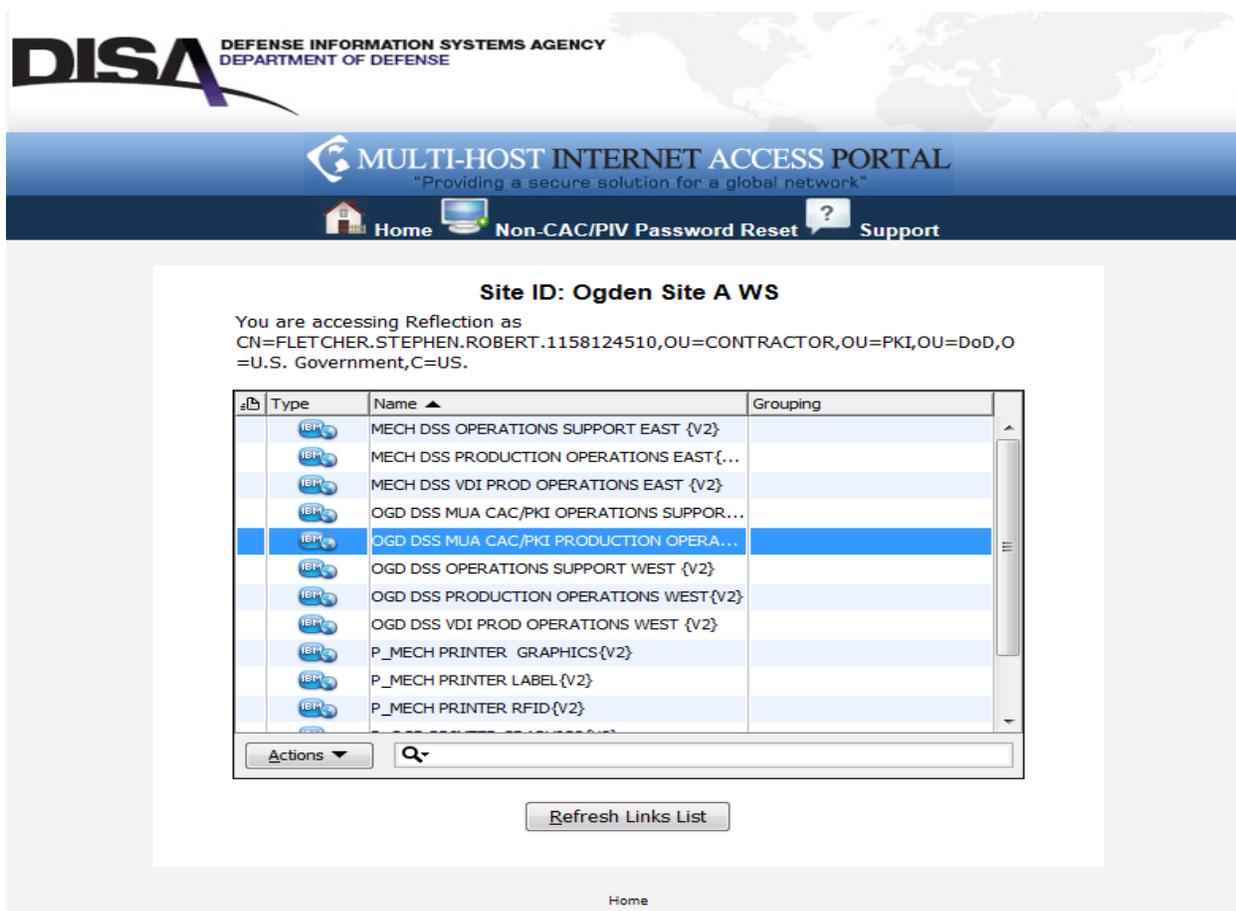


Figure 6: (New) MIAP Community of Interest (COI) Menu with CAC/PKI selections

If you have successfully registered your CAC PKI Certificate using the DISA zPAT utility on the MUA mainframe, then the MUA TN3270 session will validate your CAC PKI credentials against your existing MUA RACF USERID. This will launch the **CAC-Enabled login** process to the DSS MUA LPAR / mainframe and display the MUA Banner Page as shown in Figure 7, below.

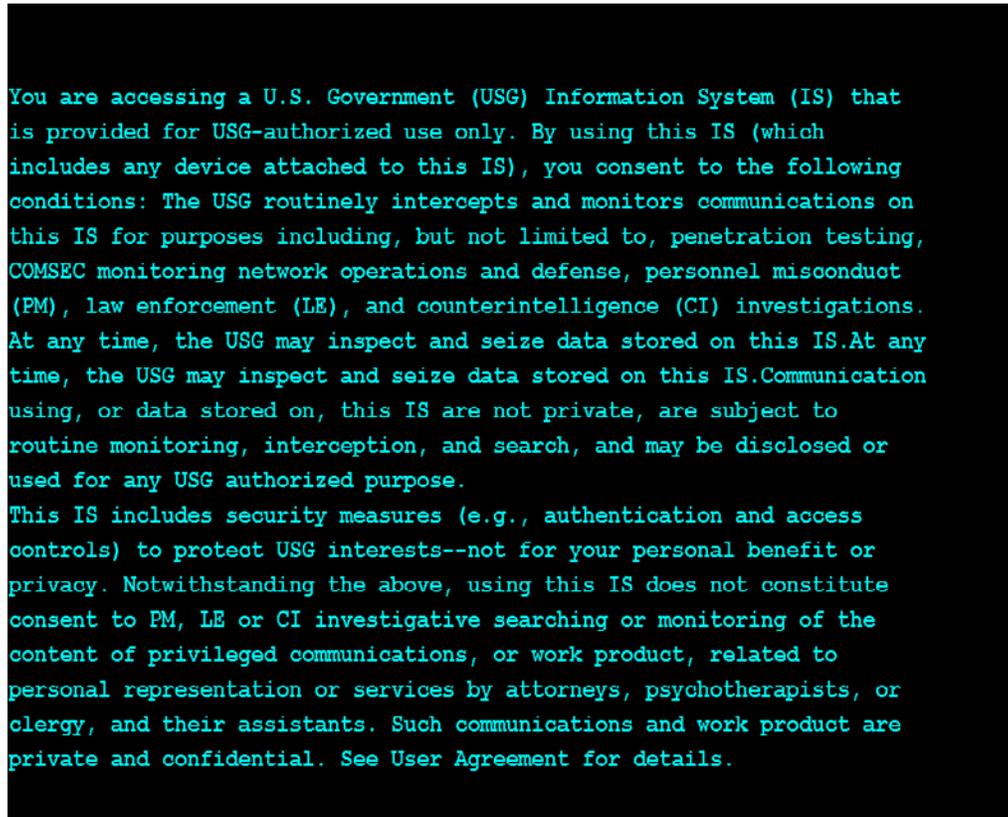


Figure 7: MUA Banner Page

Acknowledge this banner page by pressing the <<**Enter**>> key on your keyboard.

After the <<**Enter**>> key is pressed, the login (Entry Validation) screen as shown in Figure 4 below, will be momentarily displayed. **No user action is required** for this screen (i.e., the entering of information) as this screen will disappear.

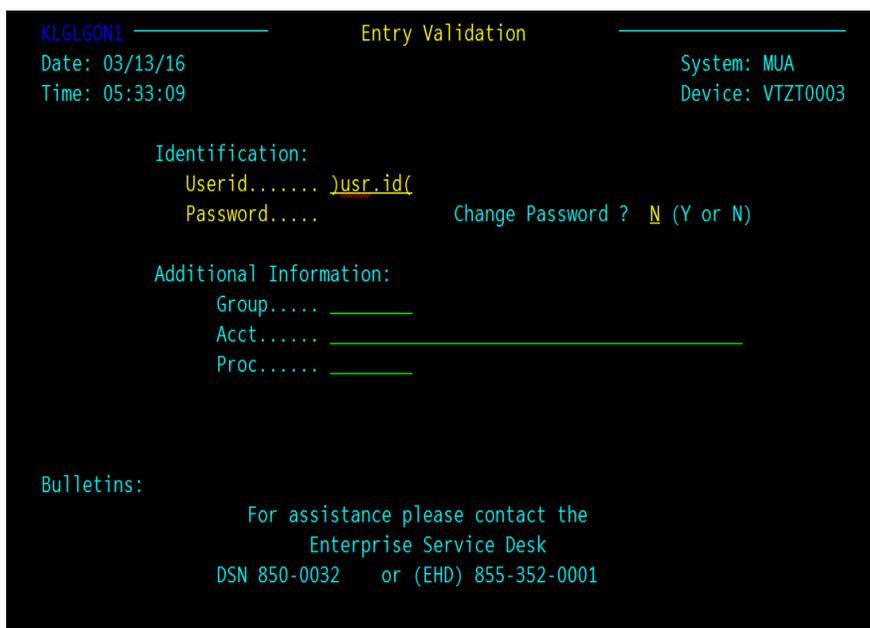
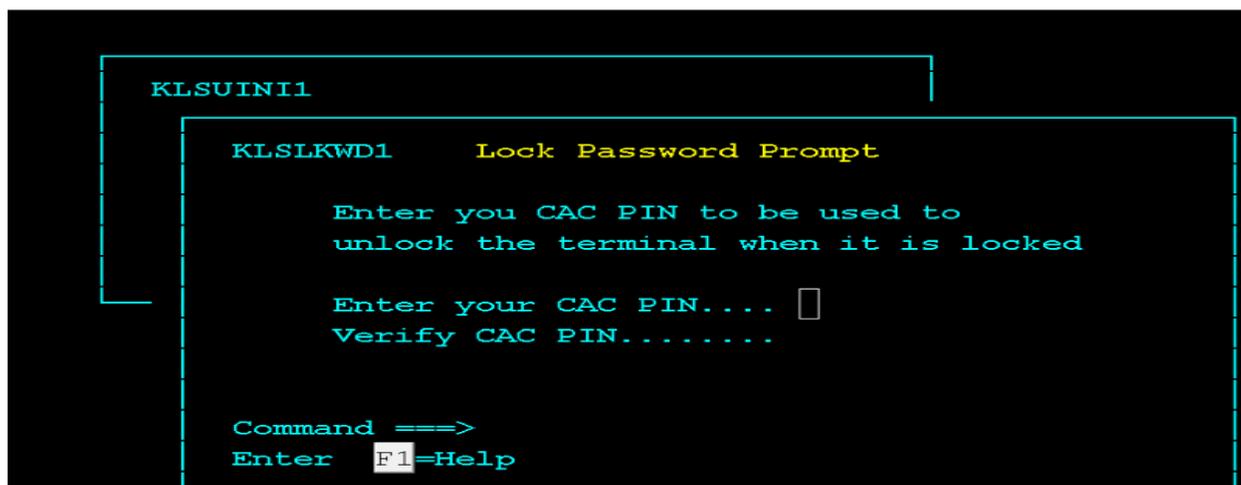


Figure 8: Login (Entry Validation) Screen – No action required

After the login (Entry Validation) screen disappears, a **CL/SuperSession Menu** will be displayed by the MUA CL SuperSession session manager. The menu **will look similar** to the one that is displayed in Figure 9 below, depending on what has been authorized to you through AMPs.

***** Note *****

FIRST TIME IN – ONLY! CL SuperSession will prompt you to enter your PIN twice in the following screen. Carefully, enter your PIN, Hit TAB and enter your PIN a second time.



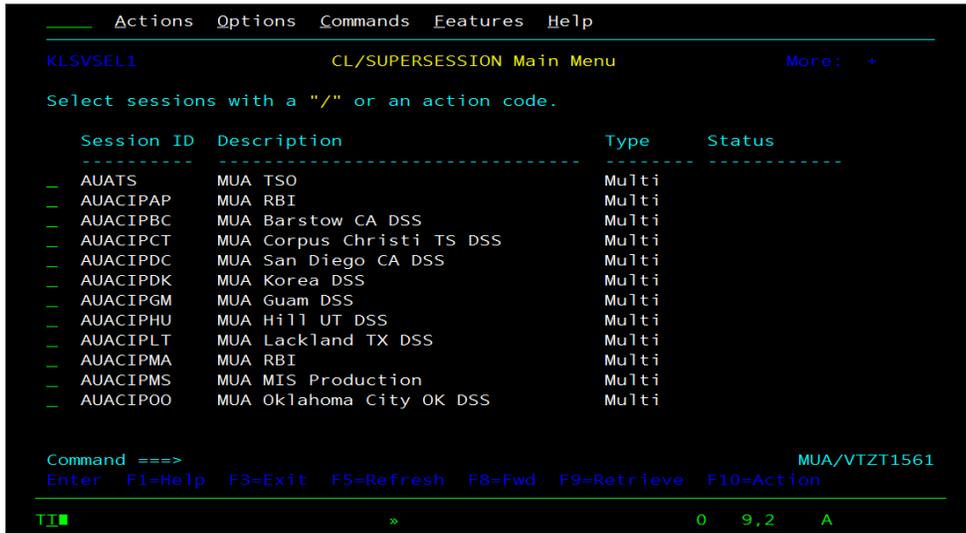


Figure 9: CL SuperSession Menu

From this menu, place your cursor next to the desired session ID (e.g. a specific DSS Site application, such as AUACIPHU for MUA Hill, UT, DSS as shown in the menu above) that you have been authorized to access through AMPS.

After the placement of cursor next to the desired DSS Site, press the <<Enter>> key on your keyboard to display that site's **Site Selection Menu**. In this example, DDHU was selected as shown in Figure 6, below.

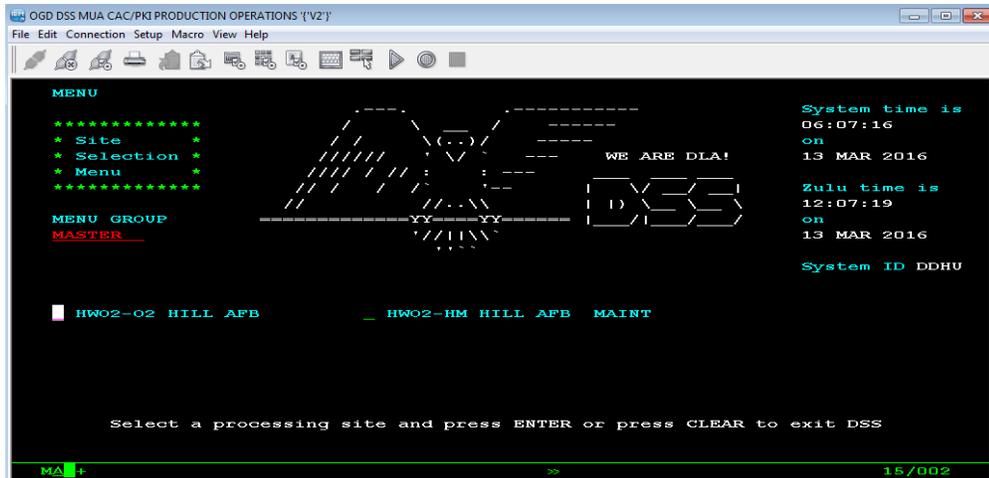


Figure 10: DSS Site Selection Menu

You should now be signed into your desired DSS region.

6.0 CAC ENABLED SIGN-OUT INSTRUCTIONS for DSS Multi-User Workstations

When signed into DSS CAC Enabled through “OGD DSS MUA CAC/PKI PRODUCTION” OPERATIONS (As shown below)

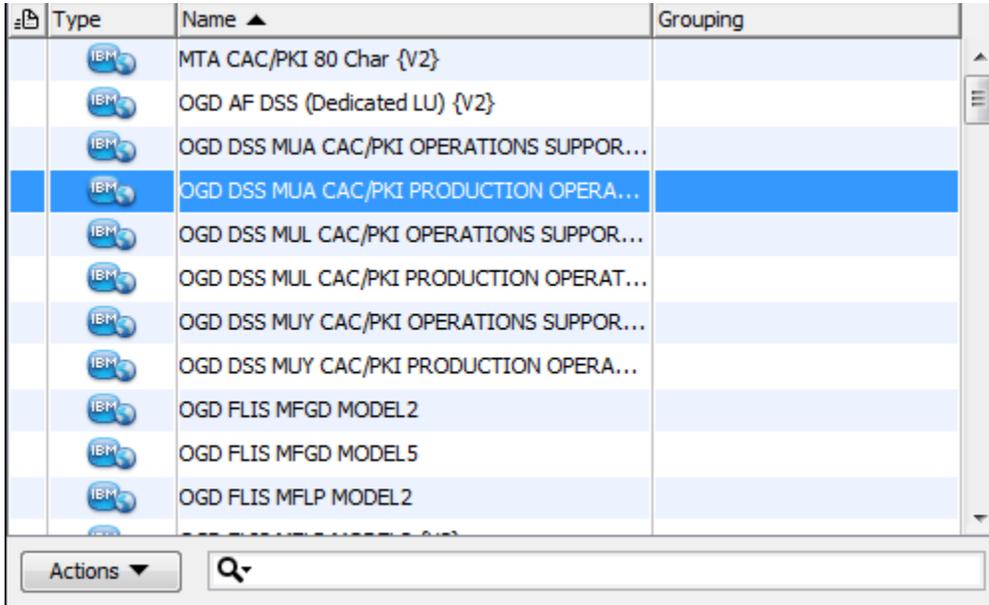


Figure 11 MIAP Menu

Into your Sites Specific Region – Using the “HILL” region as an example below

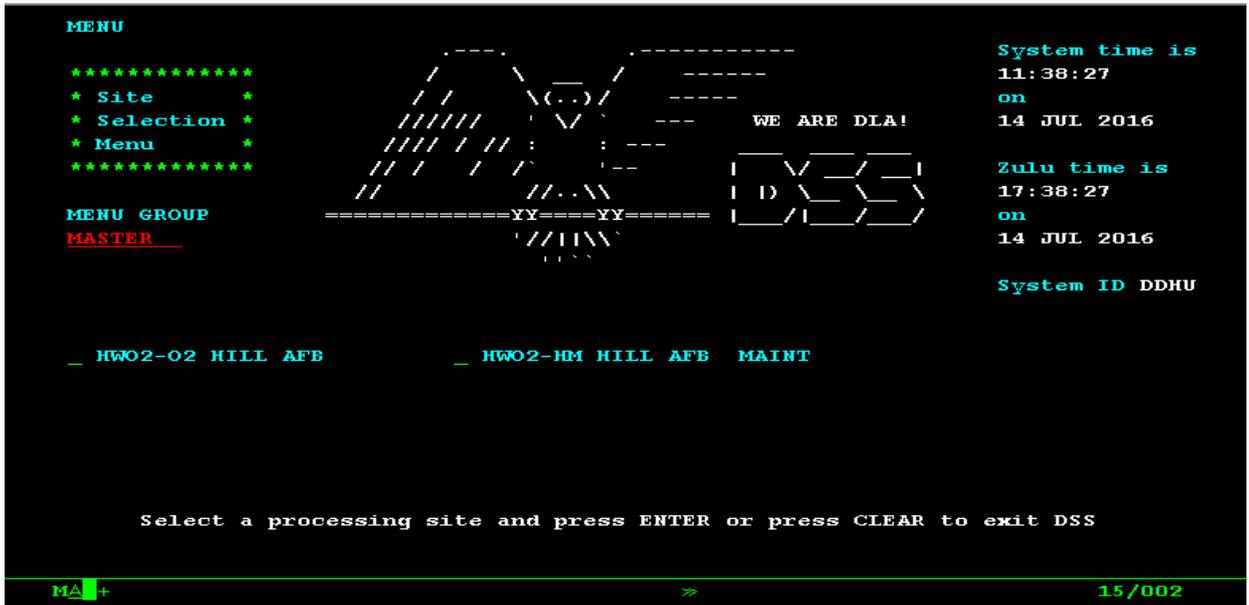


Figure 12 Site Specific Region

***** PLEASE FOLLOW THESE Very Important STEPS when SIGNING OUT OR YOUR WORKSTATION will become LOCKED with a “Session not Bound” error message for Follow-On, NON-CAC users ONLY, of this DSS Workstation. *****

Again, using the “HILL” Site as the example.

- 1.) <<PF3>> – The First PF3 clears you from the HILL site region to the CICS screen shown in figure 12, above:

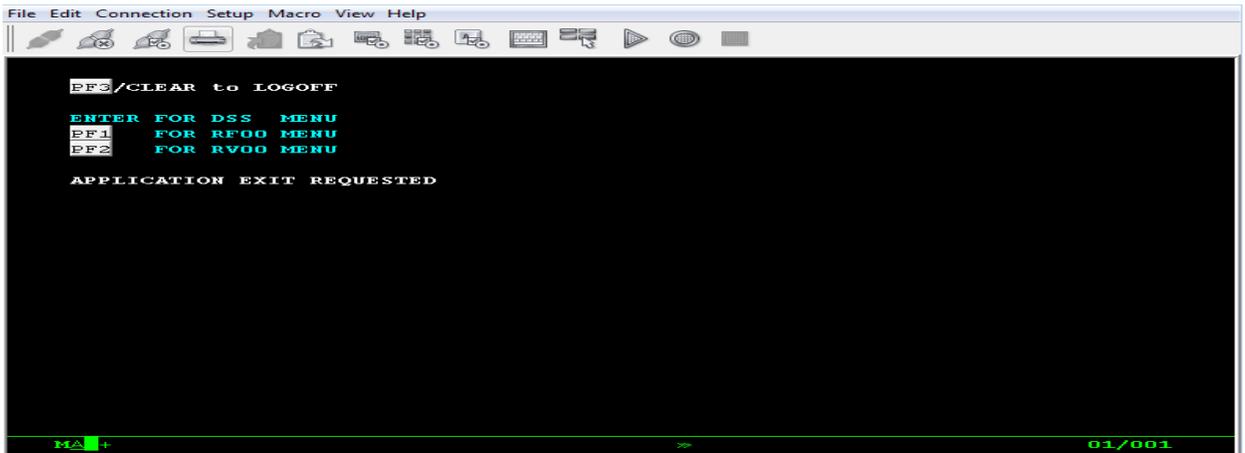


Figure 13 Clearing CICS Screen

- 2.) <<PF3>> again – Clears you from the CICS SCREEN shown in figure 13, above.
- 3.) **Most CRITICAL** – You **MUST** do one more <<PF3>> followed by an <<ENTER>> or “1” to clear you from the CL SuperSession Application as shown in figure 14 below.

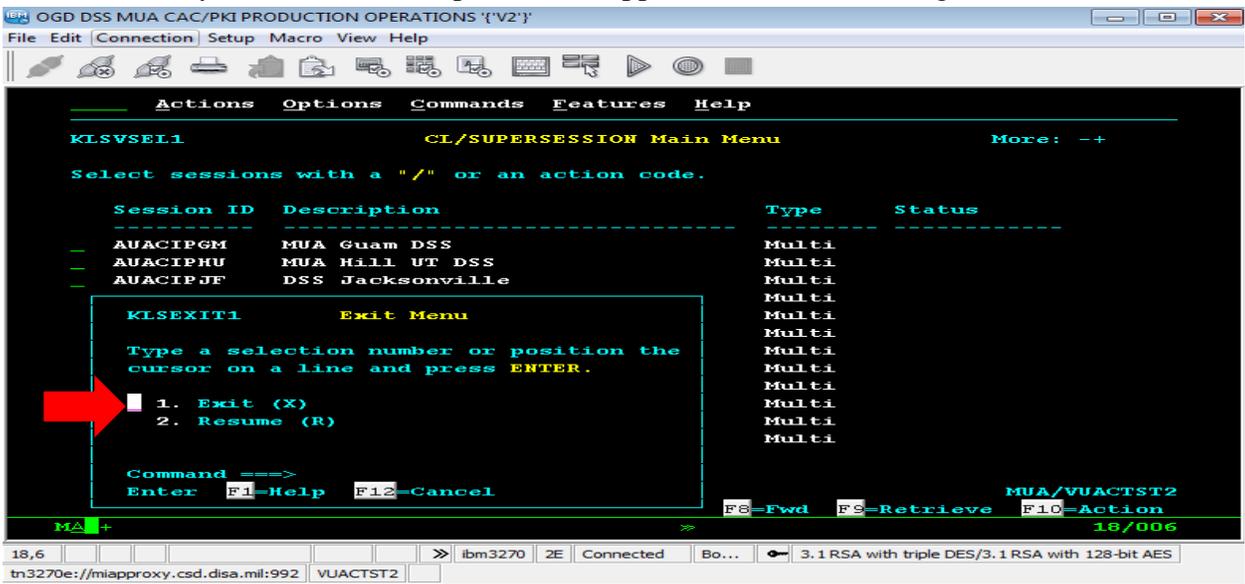


Figure 14 Clearing CL SuperSession

If (NOT) completed in this correct sign-out sequence – the following user coming in NON-CAC enabled using this Multi -user workstation will receive a “Session Not Bound” Error Message.

Clearing a LOCKED Terminal

To clear this LOCK terminal once the “**Session Not Bound**” error message is received is to have a DSS CAC enabled user sign back in CAC Enabled and sign-out again following the Sign-Out Steps outlined above or the NON-CAC user can wait 15 to 20 minutes and the locked workstation will AUTO clear it-self.

7.0 DSS LU Not Defined to Workstation (Error Message)

If you receive the DSS CITRIX / VDI TERMINAL ID SCAN dialog box that displays “Please Scan your Terminal Barcode” as shown in Figure 15 below, this means that your **DSS terminal has not been updated with the DSSLU registry file** for your workstation hardware.

This file is mandatory for a successful PKI/CAC logon for DSS End-to-End production static LU terminals to find their associated printer, stacker or carousel.

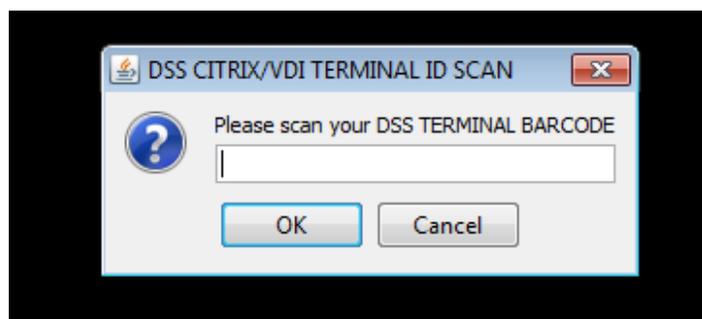


Figure 15: DSS CITRIX / VDI TERMINAL ID SCAN Dialog Box

If this occurs, please contact the DLA EHD (Enterprise Help Desk) with your DSS workstation IP address. The help desk will open an EHD Ticket/Work Order for your DSS terminal and send an email to the DLA Infrastructure Operations J64-TFS team to update your workstation registry.

7.1 CL SuperSession Error Message (CS031)

If you are using your MIAP CAC selection - **OGD DSS MUA CAC/PKI OPERATIONS SUPPORT**, to connect to MUA applications, you will have no issues selecting applications from your AUACPP01 CL SuperSession Menu. If however, you are using OGD MODEL2 or OGD MODEL5, to connect to the AUACPP01 CL SuperSession, **non-CAC enabled**, CL SuperSession will display a menu for you, but will **FAIL** when connecting to any MUA applications. You will receive a CS031 CL SuperSession error message - "Session establishment failed because the Virtual Session Manager could not allocate resources. Contact your Candle products administrator." (See figure 16 below)

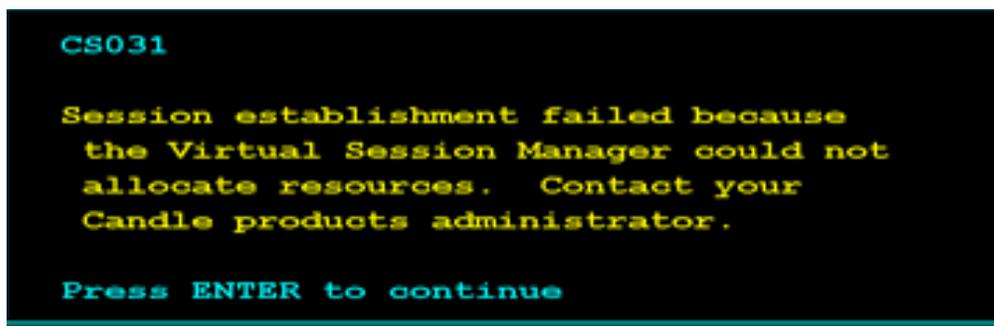


Figure 16 CL Supersession Error Message

If you need to use a MODEL2 non-CAC enabled Session with MUA, a new MIAP selection has been provided for you, to correct this issue - **OGD MUA MODEL2 {V2}**. This selection will allow you to connect to the MUA CL SuperSession - AUACPP01 **NON-CAC enabled** and successfully select from the DSS applications displayed. If you have not yet registered your CAC certificate on the DSS mainframe systems, we encourage you to do so, so that you are able to use the new DSS CAC/PKI selections to DSS without any issues.

7.2 Session Timeout Message

If a User allows the CAC/PKI session to timeout, they will receive the following message screen:

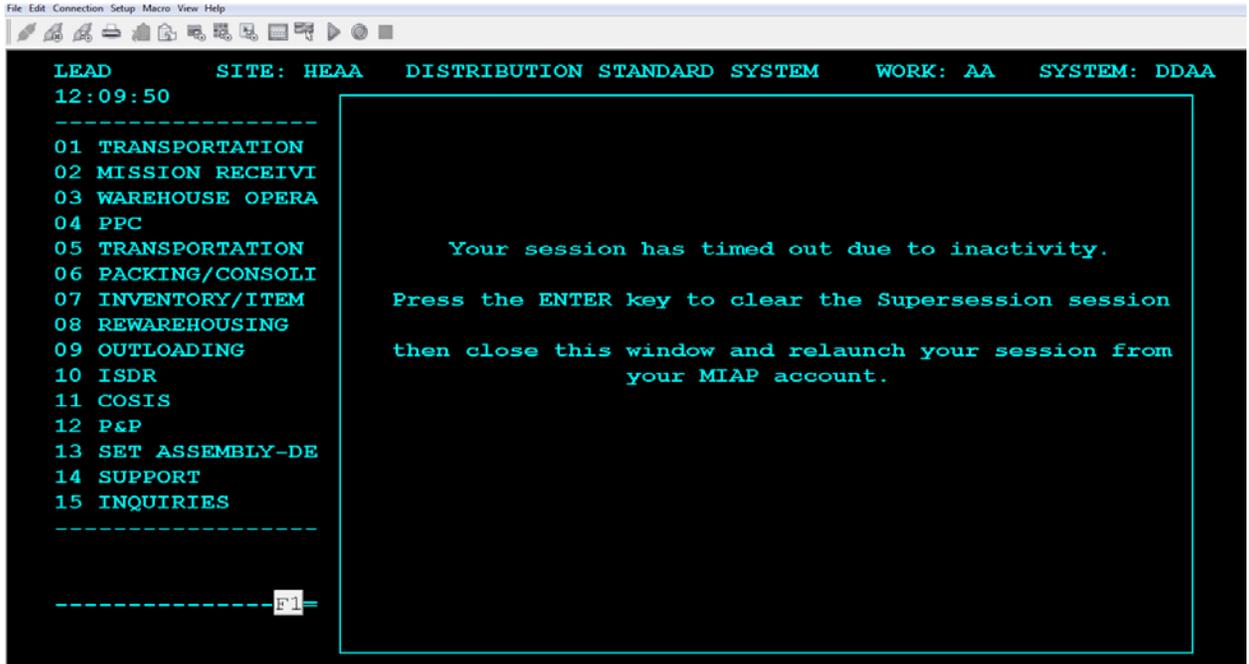


Figure 17 Session Timeout Message

As the message states, the user must select <<ENTER>> at this point and close the black screen that follows, as shown below.

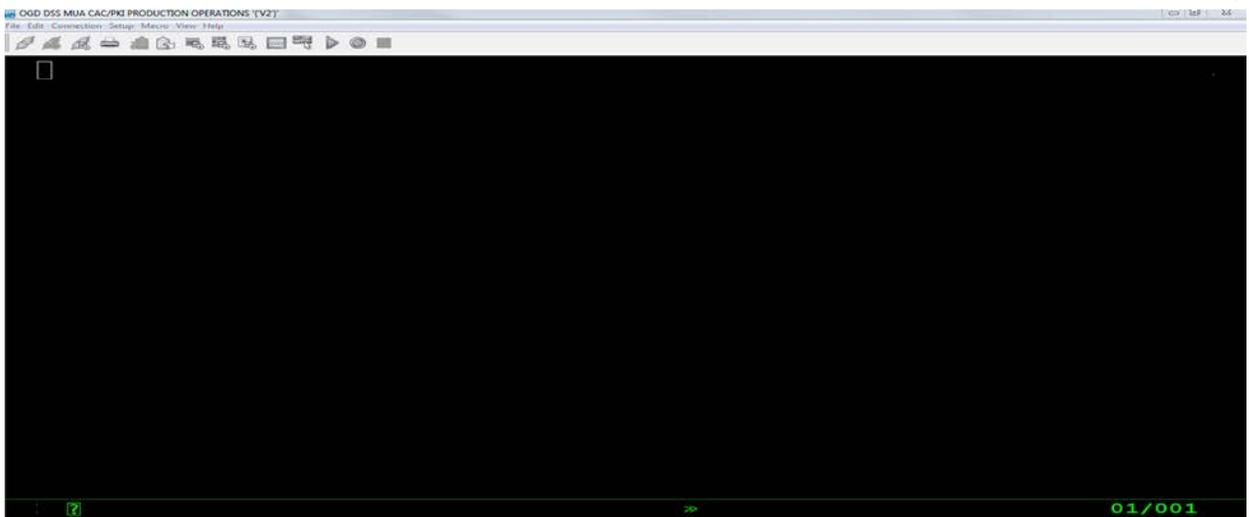


Figure 18 Close this BLACK Screen – DO NOT SELECT <<ENTER>> on this screen (See Note Below)

Then relaunch your MIAP CAC/PKI MUA Session –

Type	Name ▲	Grouping
IBM	MECH DSS OPERATIONS SUPPORT EAST {V2}	
IBM	MECH DSS PRODUCTION OPERATIONS EAST {...	
IBM	MECH DSS VDI PROD OPERATIONS EAST {V2}	
IBM	MTA CAC/PKI MODEL2 {V2}	
IBM	OGD AF DSS (Dedicated LU) {V2}	
IBM	OGD DSS MUA CAC/PKI OPERATIONS SUPPOR...	
IBM	OGD DSS MUA CAC/PKI PRODUCTION OPERA...	
IBM	OGD DSS MUL CAC/PKI OPERATIONS SUPPOR...	
IBM	OGD DSS MUL CAC/PKI PRODUCTION OPERAT...	
IBM	OGD DSS MUJ CAC/PKI OPERATIONS SUPPOR...	
IBM	OGD DSS MUJ CAC/PKI PRODUCTION OPERA...	

Figure 19 Relaunch the OGD DSS MUA CAC/PKI Session

NOTE: If the User Selects <<ENTER>> from the BLACK Screen shown above, the user will be prompted for a UserID and Password. Session will no-longer be CAC Enabled. And if the User has been on CAC for a while, they will more than likely find their MUA password expired.

If you have any other production CAC enablement issues with MUA, please contact the DLA EHD who will open an EHD Ticket/Work Order for the problem.

Enterprise Help Desk for IT Support.
Enterprise Help Desk
Hours of Operation: 24 x 7
Call: 855-352-0001
E-mail: [DLA Enterprise Help Desk](#)
Website: [DLA EHD Portal](#)

Thank you for your participation in the DSS Production CAC/PKI enablement project.

8.0 Frequently Asked Questions

Question: Once we register our CAC's and get the approval message, is there a way to test it and determine if the registration process worked, or are we just testing the process of registering?

Answer: You are not testing the registration process. Your CAC is registered in the "live" RACF database for that system. Once you get the "success" message, you **will not be able to test** your CAC logon until your DISA MIAP selections/COI has been changed, adding the new CAC/PKI sign-on for our DSS systems. This COI will soon be rolled out in phase II of the DSS CAC enablement project.

Question: During the zPAT registration process, I entered my current DSS username and password. When my password changes do I have to register again with the correct information?

Answer: No, you do not have to register again. Once your CAC has been registered within the RACF Security System it becomes another security element within your RACF security profile. Your CAC will remain registered until you change it by using the zPAT utility - deregister/register selections in your documentation. RACF Password changes will have "no" effect on your currently registered CAC/PKI credentials.

Question: Does the CAC login satisfy the DISA 30/45 day suspend/delete policy?

Answer: Correct! Your CAC logins will update the RACF account "Last Used Count" to keep your ID active, the same as when you sign-in using your current RACF USERID and password. So the answer is "yes" it will satisfy the 30/45 day inactivity rules outlined in the DISA STIGs.