

# **DLA J62D Information Operations DSS Mainframe CAC Registration Guide for (MUA) Production End-Users**

September 2016



# Table of Contents

<b>ABOUT THIS DOCUMENT .....</b>	<b>3</b>
<b>1.0 INTRODUCTION .....</b>	<b>4</b>
<b>2.0 (NEW) DSS USER CERTIFICATE REGISTRATION.....</b>	<b>4</b>
<b>3.0 MANAGING YOUR (EXISTING) DSS ACCOUNT / CERTIFICATE REGISTRATION.....</b>	<b>7</b>
3.1 *** CAC REGISTRATION *** (FIRST STEP TO DSS MAINFRAME SYSTEM CAC ENABLEMENT) .....	7
3.2 DSS CAC DEREGISTRATION (ISSUED NEW CAC CARD).....	12
<b>4.0 USING ZPAT FOR (SELF-SERVICE) PASSWORD RESETS .....</b>	<b>13</b>
4.1 REQUIREMENTS.....	13
4.2 SELF-SERVICE PASSWORD RESET PROCESS .....	13
4.2.1 <i>Initial Entry</i> .....	13
4.2.2 <i>Reset Password &amp; User Retrieval</i> .....	15
4.2.3 <i>Masked Display and Warning</i> .....	15
4.2.4 <i>Displaying and Hiding the Password Value</i> .....	16

## About this Document

This document was based on the DISA zPAT 1.0 User Guide and modified for use on the DLA Distribution Standard System (DSS) Mainframes.

The instructions in this guide relate to the DSS MUA production application and identify unique DLA registration entries and requirements.

### **(zPAT) - z/OS PKI Account Management Toolkit**

The zPAT tool, developed by DISA, is used to register CAC certificates to the mainframe security system – RACF environments. Once the CAC certificate and PIN has been registered and associated to your unique DSS MUA system USER ID, within the RACF security system, the MIAP CAC/PKI “**Production Operation**” selection may be used to sign-on, using only your CAC identification card inserted in your workstation.

**zPAT CAC Registration Instructions follow in this document.**

## 1.0 Introduction

The DISA z/OS PKI Account Management Toolkit or zPAT utility provides an end-user with the ability to register a CAC PKI certificate to the DSS MUA mainframe RACF Security System, deregister a CAC certificate (when a new CAC card is issued), and initiate a self-service password reset on the MUA mainframe Security System, with a valid registered CAC.

## 2.0 (New) DSS User Certificate Registration

**Note:** If you are an existing DSS user, please skip this section and continue on to:

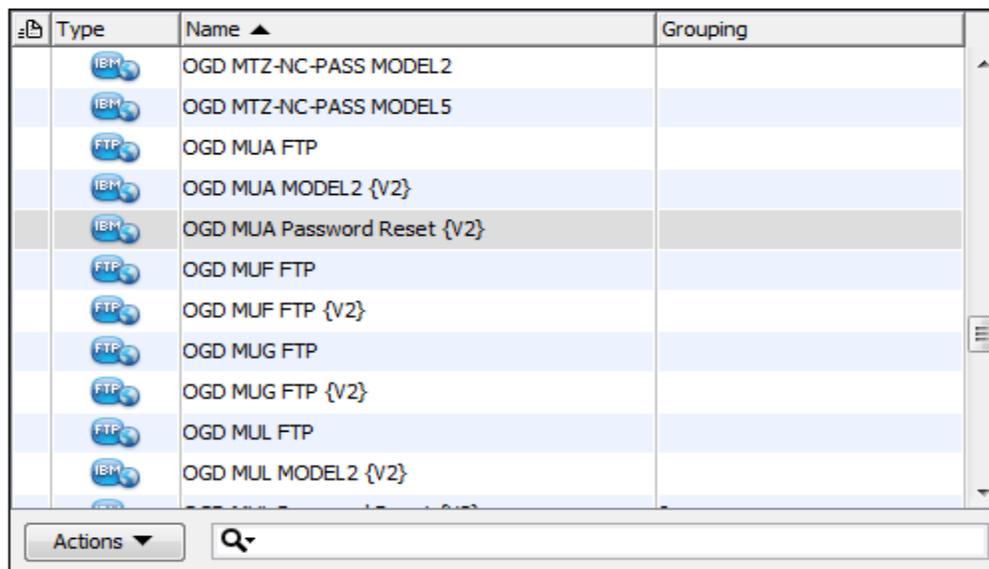
### 3.0 Managing your (Existing) DSS account / certificate registration on page 7.

In order to register your new CAC certificate to the DSS application RACF security system, you **MUST** first change your newly assigned Temporary password to a Permanent DSS password.

- 1.) First, you must enter MIAP using the following link:

<https://miap.csd.disa.mil>

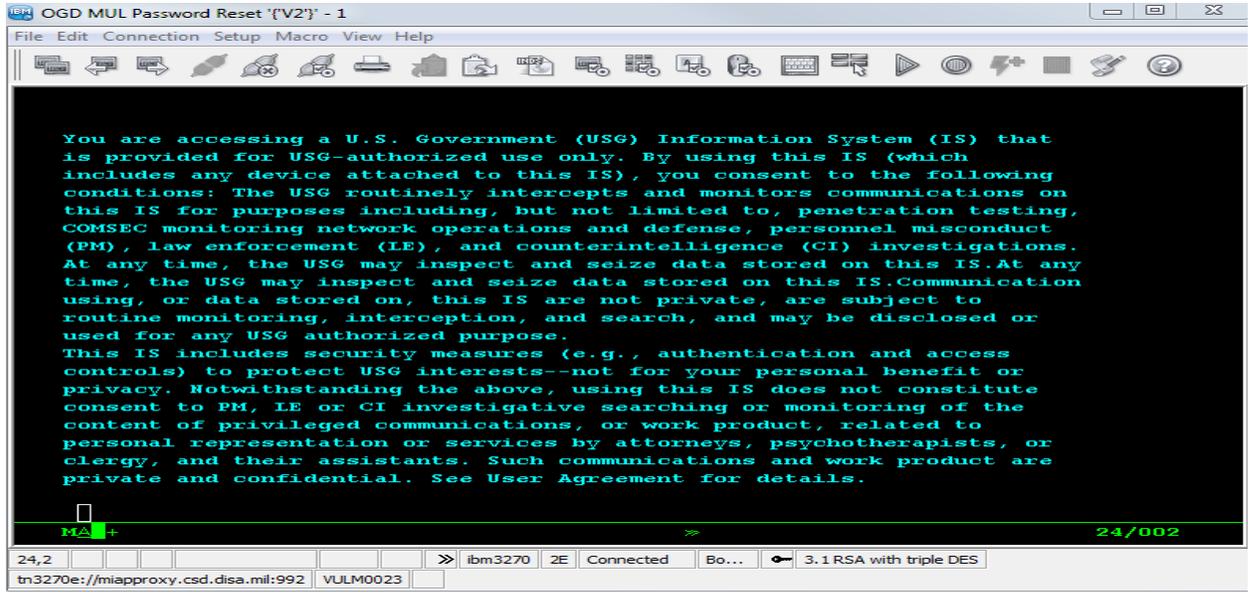
- 2.) Next, if you do not have an existing DISA MIAP account, you will have to use the “Create New Account” selection on this screen and enter your personal information.
- 3.) Once the MIAP account has been created and you able to display your DSS application menu, or better known as your Community of Interest / COI menu, find and select the following application: OGD MUA PASSWORD RESET {V2}, as shown below.



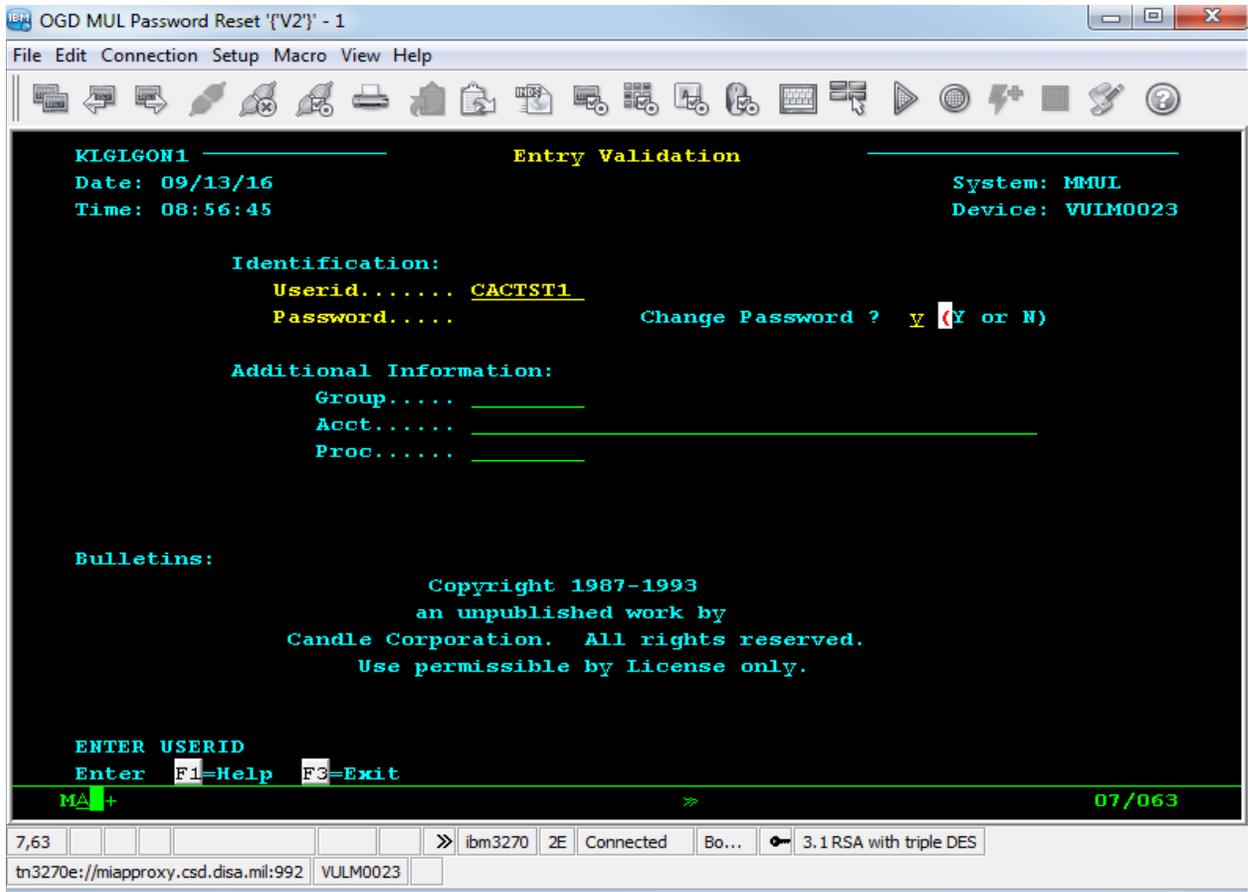
Type	Name ▲	Grouping
IBM	OGD MTZ-NC-PASS MODEL2	
IBM	OGD MTZ-NC-PASS MODEL5	
FTP	OGD MUA FTP	
IBM	OGD MUA MODEL2 {V2}	
IBM	OGD MUA Password Reset {V2}	
FTP	OGD MUF FTP	
FTP	OGD MUF FTP {V2}	
FTP	OGD MUG FTP	
FTP	OGD MUG FTP {V2}	
FTP	OGD MUL FTP	
IBM	OGD MUL MODEL2 {V2}	

Refresh Links List

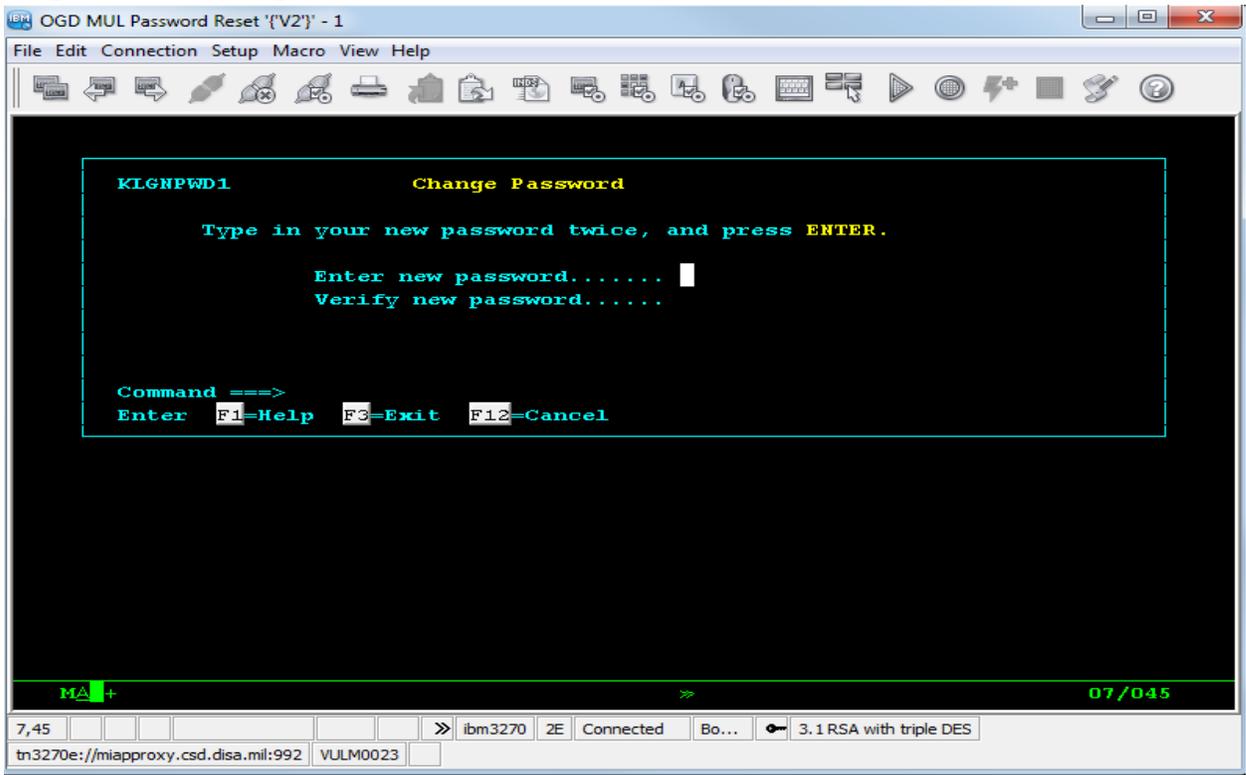
4.) You will next receive a U.S. Government banner page, select <<ENTER>> to continue on.



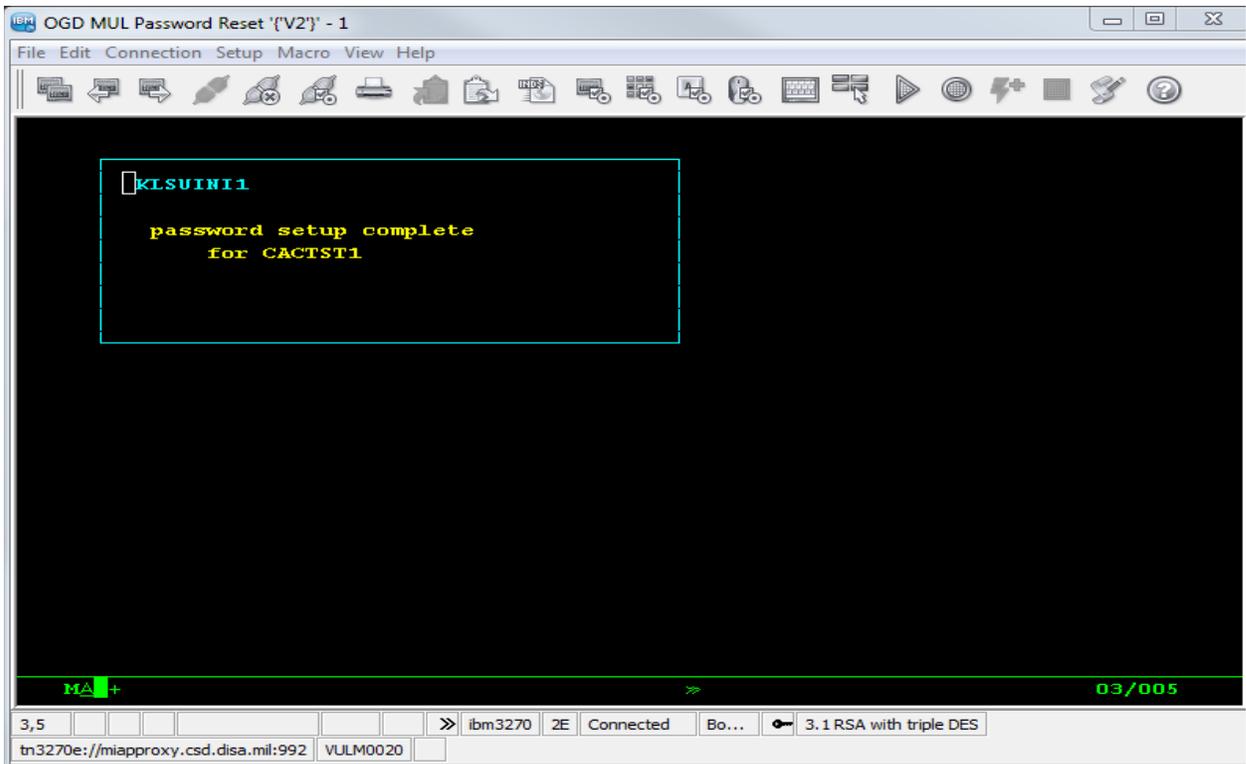
5.) Once you get to the following "Entry Validation" screen, enter your new DSS User ID, Temporary Password and select <<ENTER>>.



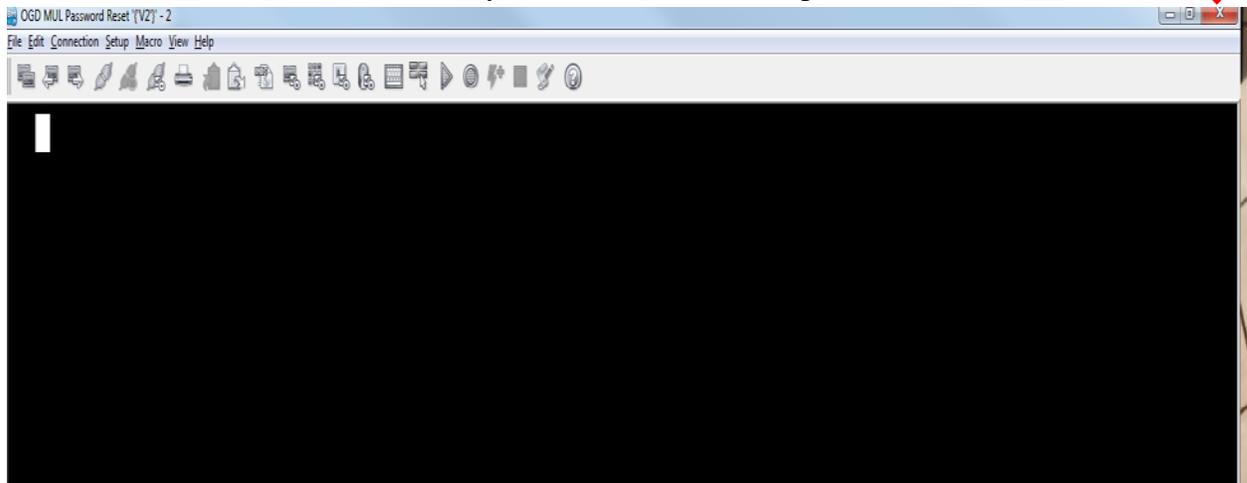
- 6.) This CL SuperSession screen will then prompt you for a new password, Enter a new password in both password fields, then select <<ENTER>>.



- 7.) If the passwords match, you will receive the following message screen, please select <<ENTER>> to continue.



Next select the “X” in the corner and you’re done with this step!



\*\*\* After your Temporary Password has been changed to a Permanent Password, please continue on with the following instructions to Register your CAC certificate. \*\*\*

### **3.0 Managing your (Existing) DSS account / certificate registration**

Using the DISA zPAT tool you can now manage the certificate you have registered to the DSS mainframes. The (first step) to the DSS CAC enablement MUA sign-on is to get your CAC certificate registered to the DSS MUA mainframe RACF security system.

#### **3.1 \*\*\* CAC REGISTRATION \*\*\* (First Step to DSS Mainframe System CAC enablement)**

First, using your IE Internet Browser, navigate to the following DSS MUA URL to register your CAC card & PIN to the DSS MUA RACF system security environment.

**MUA** use <https://mua2.csd.disa.mil/zpat> Link

A display page will be presented to you with the DoD banner page. You will then be asked to choose a certificate from the browser certificate store. **For DSS CAC Enablement, YOU MUST CHOOSE the “DoD CA Identity Certificate”; NOT THE “DOD CA EMAIL Certificate”.** The email certificate will not work for this CAC enablement process.



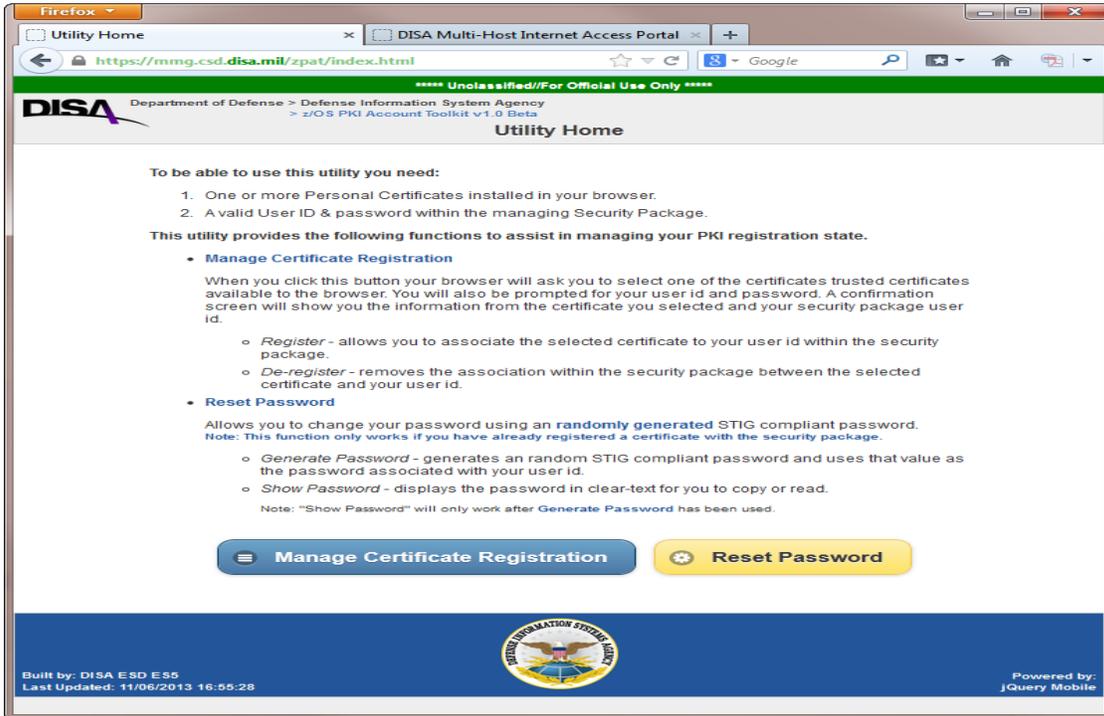
Click “OK” to continue.

**Note: The Most Common Error with DSS CAC Registration/CAC Enablement is DSS Users Registering the Wrong CAC Certificate, which will NOT allow them to access the DSS LPAR via their CAC Sign-In Selection from MIAP.**

The screenshot shows the 'Manage Certificate Registration' page in a browser. The user ID is NU03547. Under the 'Certificate' section, the following details are listed: Common Name: FLETCHER.STEPHEN.ROBERT.1158124510, Country: US, State or Providence, Locality, Organization: U.S. Government, Organizational Unit: CONTRACTOR, and Serial Number: 3e:9e:b3. Under the 'Issuer' section, the 'Common Name: DOD CA-32' is highlighted with a red box and a red arrow pointing to it, with the word 'Correct' written next to it. Below the issuer information are two buttons: '+ Register' and '- Deregister'. The footer includes the DISA logo, 'Department of Defense > Defense Information System Agency > z/OS PKI Account Toolkit v1.1', and the text 'Built by: DISA ESD E55 Last Updated: 06/11/2014 08:33:37' and 'Powered by: jQuery Mobile'.

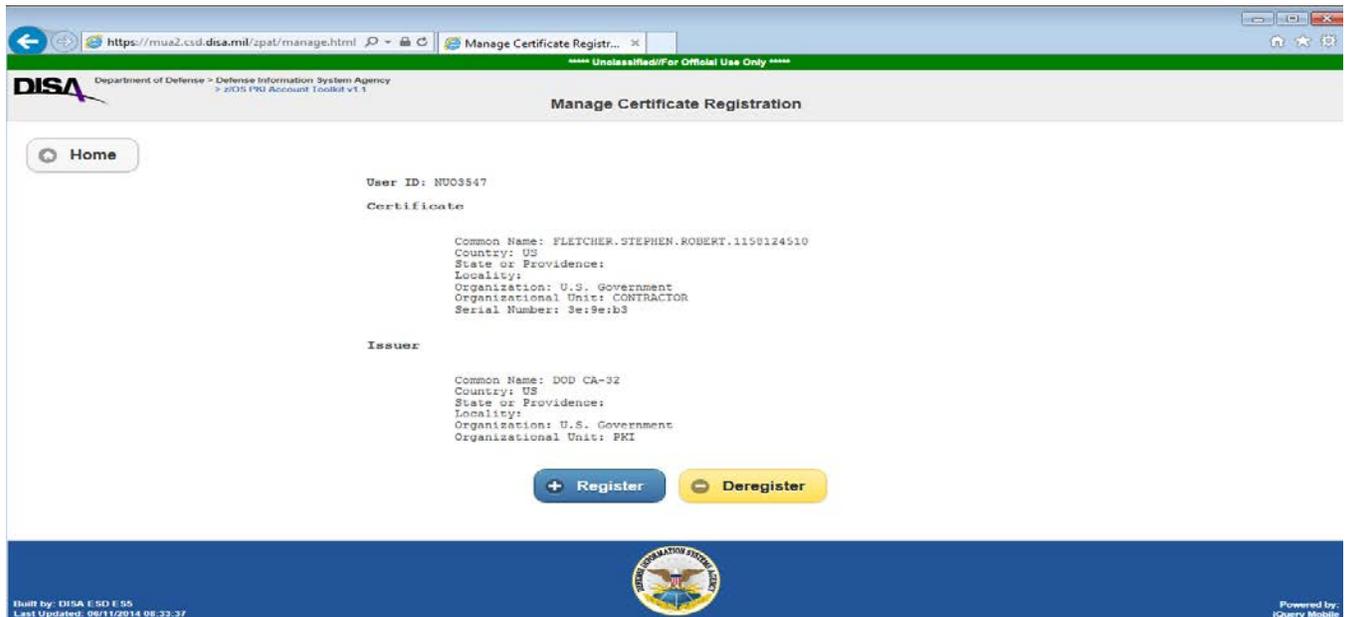
The screenshot shows the 'Manage Certificate Registration' page in a browser. The user ID is 'NOT REGISTERED'. Under the 'Certificate' section, the following details are listed: Common Name: FLETCHER.STEPHEN.ROBERT.1158124510, Country: US, State or Providence, Locality, Organization: U.S. Government, Organizational Unit: CONTRACTOR, and Serial Number: 40:93:6c. Under the 'Issuer' section, the 'Common Name: DOD EMAIL CA-32' is highlighted with a red box and a red arrow pointing to it, with the text 'In-Correct' written next to it. A large red 'X' is drawn over the issuer information. Below the issuer information are two buttons: '+ Register' and '- Deregister'. The footer includes the DISA logo, 'Department of Defense > Defense Information System Agency > z/OS PKI Account Toolkit v1.1', and the text 'Built by: DISA ESD E55 Last Updated: 06/11/2014 08:33:37' and 'Powered by: jQuery Mobile'.

When the Certificate is accepted, the following screen should be displayed:

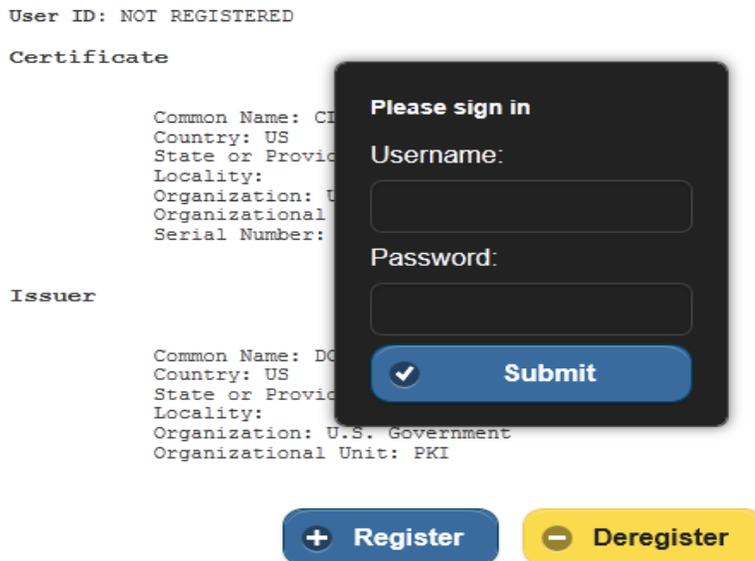


This is the DISA zPAT Home page, displayed above. From here, you are given the choices of: **Manage Certificate Registration** or **Reset Password**. For CAC Registrations, please select the “**Manage Certificate Registration**” button to register your CAC certificate and PIN to the DSS mainframe RACF Security System. **Note:** that a CAC registration or deregistration can only be successful for users with a Current MUA UserID and permanent password on the DSS mainframe environment you are selecting; in this case, the DSS MUA Production Environment. If you do not have a current DSS password for the MUA mainframe, please skip down to the 4.0 zPAT (Self-Service) password resets on page (8) of this document.

The Manage Certificate Registration screen will display the certificate for your verification and give you the option of either registering or deregistering your CAC. **To register your certificate, select “Register” as shown (below).**



Once you have clicked **“Register”**, you will be prompted for your **Current MUA Userid and Permanent Password** - (Temporary, first time, Passwords will not work). Here you will fill in your UserID/Username and Password for the DSS MUA mainframe to which you are registering your certificate.



Upon successful registration, the “Response” line at the top left of your screen will change to:  
**Response: success**

### 3.2 DSS CAC DEREGISTRATION (Issued new CAC Card)

To remove/deregister an (old) certificate from the DSS MUA mainframe security system, follow the same process and choose “**De-register**”. You will again be prompted for your **current** MUA Userid and Password. If entered correctly, your CAC certificate will be deregistered. You can then register a (new) CAC card to replace your old CAC certificate on the MUA LPAR.

**NOTE: PLEASE BE SURE TO DEREGISTER YOUR (OLD) CAC CARD (BEFORE) SURRENDERING IT AND RECEIVING A (NEW) CAC CARD REPLACEMENT!**

The steps required to deregister a CAC PKI certificate follow the same flow as the CAC registration process; however, users need to be aware of the following: Without a registered CAC certificate on the DSS MUA mainframe, a user will **(not)** be able to perform a Self-Service Password reset – using z/PAT.

In the normal process flow (DSS MUA users deregister the (old) CAC certificate and subsequently register a (new) CAC certificate, this should not be an issue because during CAC deregistration, the current DSS MUA Userid & Password (**are needed**). Since these two steps normally occur within a few days of each other, the password used to deregister the old certificate will be used to register the new certificate. If you have forgotten your password for deregistration, follow the self-service password reset, using zPAT, in this document. Then deregister your (old) MUA CAC certificate. Do not forget this (new) reset password, you will need it to register your new CAC certificate.

In a scenario where the user deregisters their CAC PKI certificate on MUA, then forgets their password, they will not be able to use zPAT to either register a new CAC PKI certificate (which requires a current MUA userid & password) or perform a self-service password reset (which requires a registered CAC certificate to the MUA RACF security system). In this case, you will need to contact the DLA Enterprise Help Desk to get your password reset on the DSS MUA system.

## 4.0 Using zPAT for (Self-Service) password resets

### 4.1 Requirements

To initiate a Self-Service password reset, you first **must have** a current CAC, which has been **registered** to the DSS MUA mainframe security system before starting this process.

### 4.2 Self-service password reset process

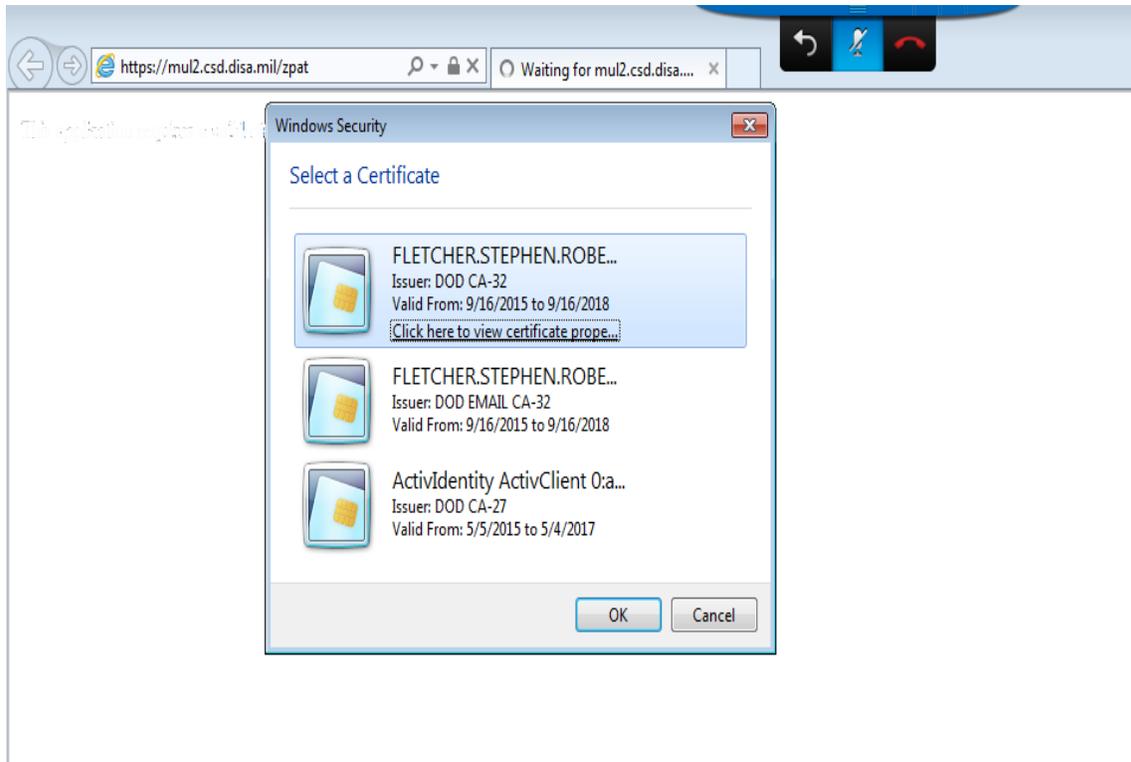
Using your Internet Browser, navigate to the DSS MUA URL.

<https://mua2.csd.disa.mil/zpat>

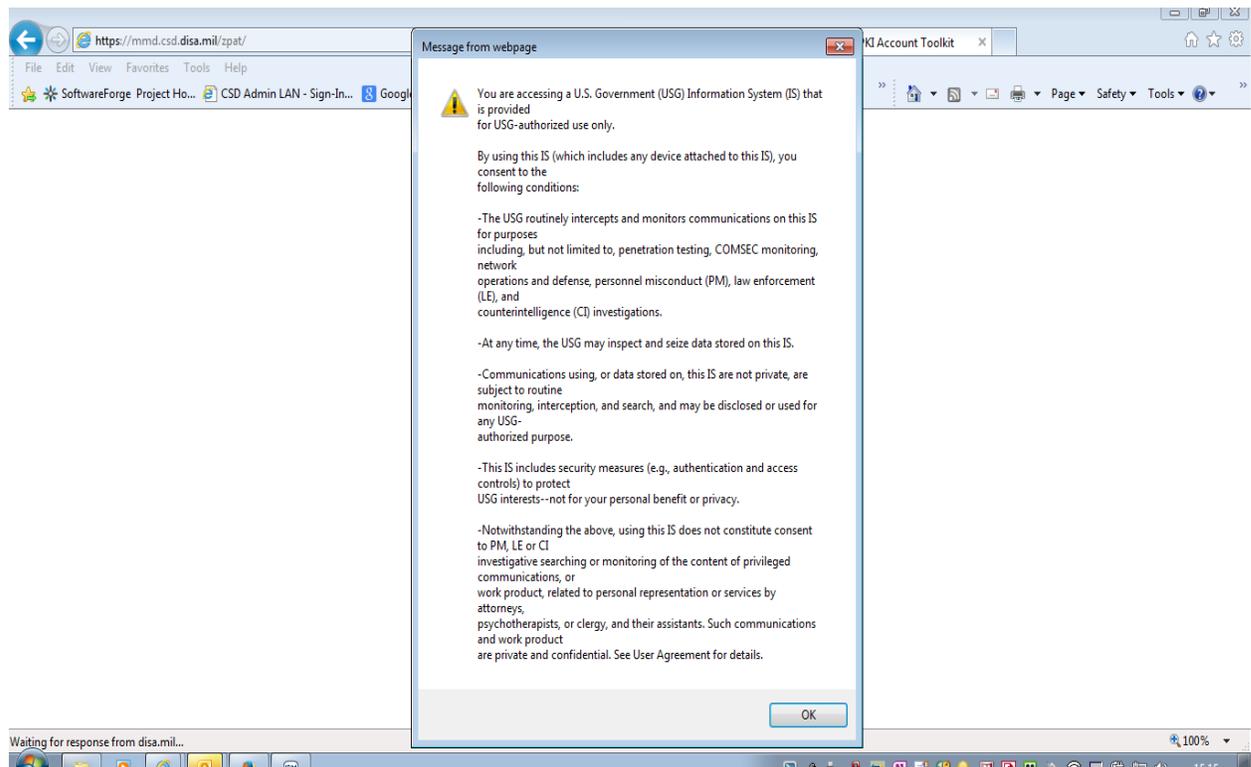
#### 4.2.1 Initial Entry

Upon entry to the DISA zPAT URL, you will first be presented with a Browser Certificate Store follow by the DoD banner page. On the Browser Certificate Store display, select your Identity Certificate.

**Browser Certificate Store** - Select Identity Certificate, shown below.

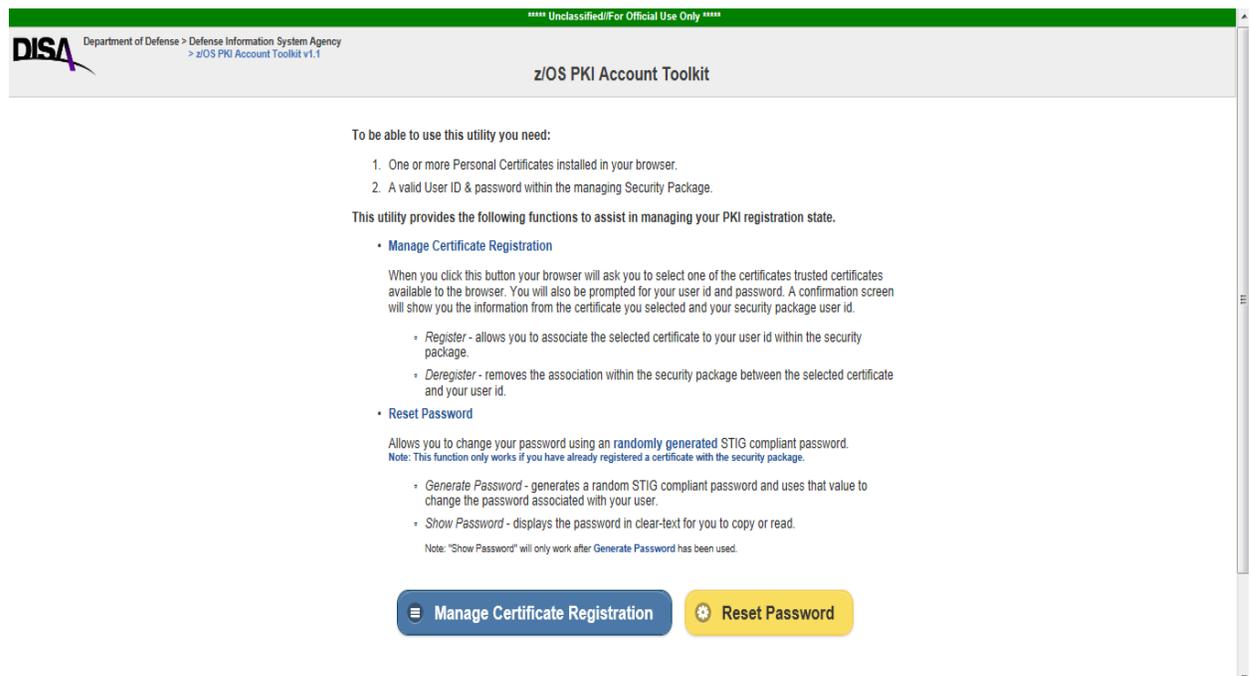


## Login Banner- Click “OK”



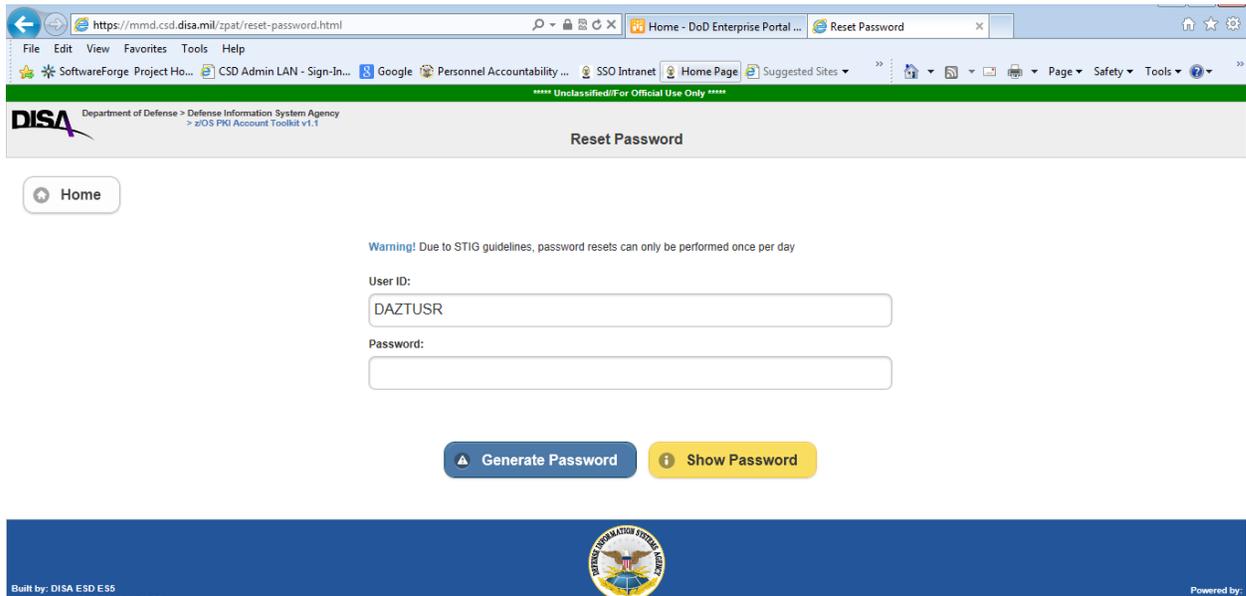
Select “RESET PASSWORD” from the zPAT Home Page, Shown below.

zPAT Home Page -



## 4.2.2 Reset Password & User Retrieval

After selecting the “Reset Password” button to gain access to the Reset Password screen – the password is not actually reset at this point. The requestor’s userid will be retrieved and populated for the password reset function. The retrieval may take a few moments. The retrieved userid cannot be edited or changed.



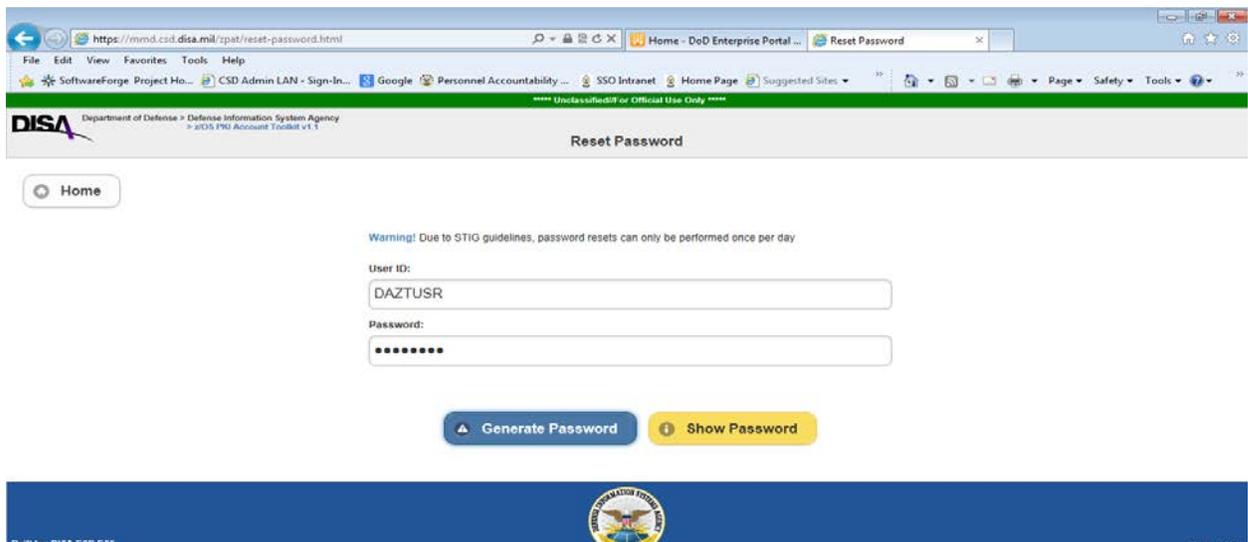
The screenshot shows a web browser window with the URL <https://mmd.csd.disa.mil/zpat/reset-password.html>. The page title is "Reset Password". The interface includes a "Home" button, a warning message: "Warning! Due to STIG guidelines, password resets can only be performed once per day", and two input fields: "User ID:" with the value "DAZTUSR" and "Password:". Below the input fields are two buttons: "Generate Password" and "Show Password". The footer of the page contains the text "Built by: DISA ESD ESS" and "Powered by:" next to the DISA logo.

### Generate Password

To perform the actual MUA password reset, use the “Generate Password” button, as shown above. This will cause zPAT to make a request to the RACF security system, to reset the password for the requestor’s userid shown. This operation will take a few moments. The password will only be reset on the DSS MUA system.

## 4.2.3 Masked Display and Warning

Upon successful completion, the password is returned and displayed as “\*\*\*\*\*”. The requestor is advised and mandated to protect passwords IAW (DISA Form 787), therefore, do not display the password using the “Show Password” button until you are certain that no one else is able to view your workstation display. When it is safe to do so, use the “Show Password” button to display the password. Note that the “Show Password” button now becomes a “Hide Password” button which is used to return the field to the masked “\*\*\*\*\*” display, as shown below.



#### 4.2.4 Displaying and Hiding the Password Value

The displayed MUA password is indicated in the following display. **Note that for security reasons, zPAT will re-hide the password after a 5 second delay.** You can re-display the password using the “show password” button.

**NOTE:** Once you have this zPAT MUA temporary password, you may sign into your DSS application and change the password to a new 8 character password, which must include a – special character, number, lower & up case alphabetic character(s) OR used to register your (new) MUA CAC certificate using zPAT.