
DLA J62D Information Operations DSS Mainframe CAC Registration Guide for MUA, MUY & MUL

Revised September 2020



ABOUT THIS DOCUMENT	3
<u>1. INTRODUCTION</u>	4
<u>2. MANAGING YOUR DSS CERTIFICATE REGISTRATION</u>	4
<u>2.1 CAC REGISTRATION.....</u>	4
<u>2.2 CAC DEREGISTRATION.....</u>	9
<u>3. USING ZPAT FOR SELF-SERVICE PASSWORD RESETS.....</u>	10
<u>3.1 REQUIREMENTS</u>	10
<u>3.2 SELF-SERVICE PASSWORD RESET PROCESS</u>	10
<u>3.2.1 Initial Entry.....</u>	10
<u>3.2.2 Reset Password & User Retrieval.....</u>	16
<u>3.2.3 Masked Display and Warning.....</u>	17
<u>3.2.4 Displaying and Hiding the Password Value</u>	18

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 the DSS 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 cards to the mainframe security system – RACF environments. Once the CAC card and PIN has been registered and associated to your unique DSS system USER ID, within the RACF security system, on the desired DSS mainframe environment, the MIAP CAC/PKI “Community-of-Interest” menu selection may be used to sign-on, using only your CAC and PIN.

zPAT CAC Registration instructions follow in this document.

Introduction

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

2.0 Managing Your DSS 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 sign-on is to get your CAC certificate registered to the DSS mainframe(s) you are authorized access to.

2.1 *** CAC REGISTRATION *** (First Step to DSS Mainframe System CAC enablement)

First, using your Internet Browser, navigate to one of the following DSS URL's to register your CAC card & PIN to that DSS system(s) RACF security environment. (NOTE: If (all) three DSS systems are required, you MUST register your CAC card to all three RACF security systems separately.)

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

MUY use <https://muy2.csd.disa.mil/zpat>

MUL use <https://mul2.csd.disa.mil/zpat>

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.

https://mul2.csd.disa.mil/zpat/manage.html

DISA Department of Defense > Defense Information System Agency > JCS PPK Account Toolkit v1.2.1

Manage Certificate Registration

Home

User ID: NOT REGISTERED

Certificate

Common Name: JAMES.G.
Country: US
State or Providence:
Locality:
Organization: U.S. Government
Organizational Unit: CONFIDENTIAL
Serial Number:

Issuer

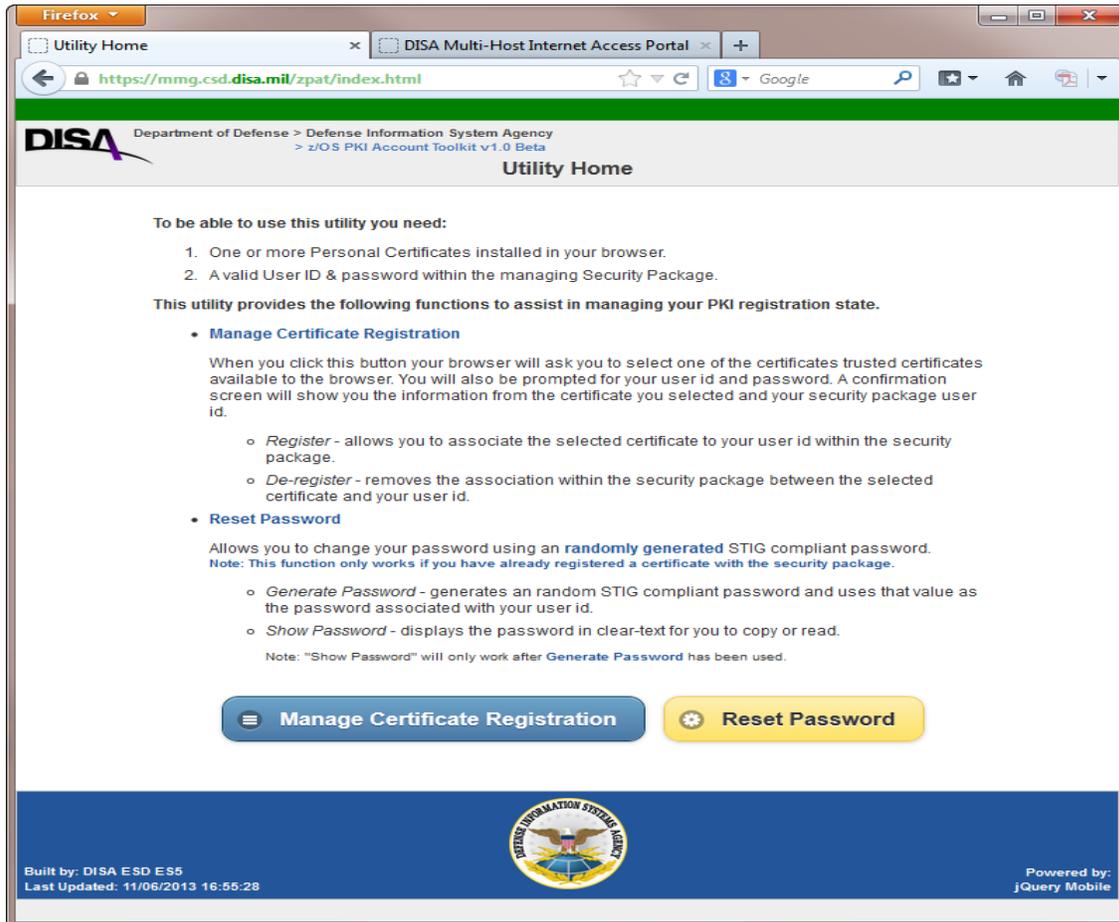
Common Name DOD ID CA-59 **Correct**
Country: US
State or Providence:
Locality:
Organization: U.S. Government
Organizational Unit: PRI

+ Register - Deregister

Built by: DISA ISC SEZ
Last Updated: 10/21/2019 10:40:57

Powered by: Query 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 choose the **“Manage Certificate Registration”** button to register your CAC certificate and PIN to the DSS mainframe Security System - RACF. Note: that a CAC registration or deregistration can only be successful for users with a **Current Userid and Password** on the DSS mainframe you are selecting. If you do not have a current DSS password for the mainframe you are selecting, skip down to the 3.0 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, choose “Register” as shown (below).**

The screenshot shows a web browser window with the URL `https://mul2.csd.disa.mil/zpatr/manage.html`. The browser's address bar and menu are visible. The page content includes the DISA logo and the title "Manage Certificate Registration". A "Home" button is located in the top left. The main content area displays the following information:

User ID: NOT REGISTERED

Certificate

Common Name: [REDACTED] JAMES.G [REDACTED]
Country: US
State or Providence:
Locality:
Organization: U.S. Government
Organizational Unit: [REDACTED]
Serial Number: [REDACTED]

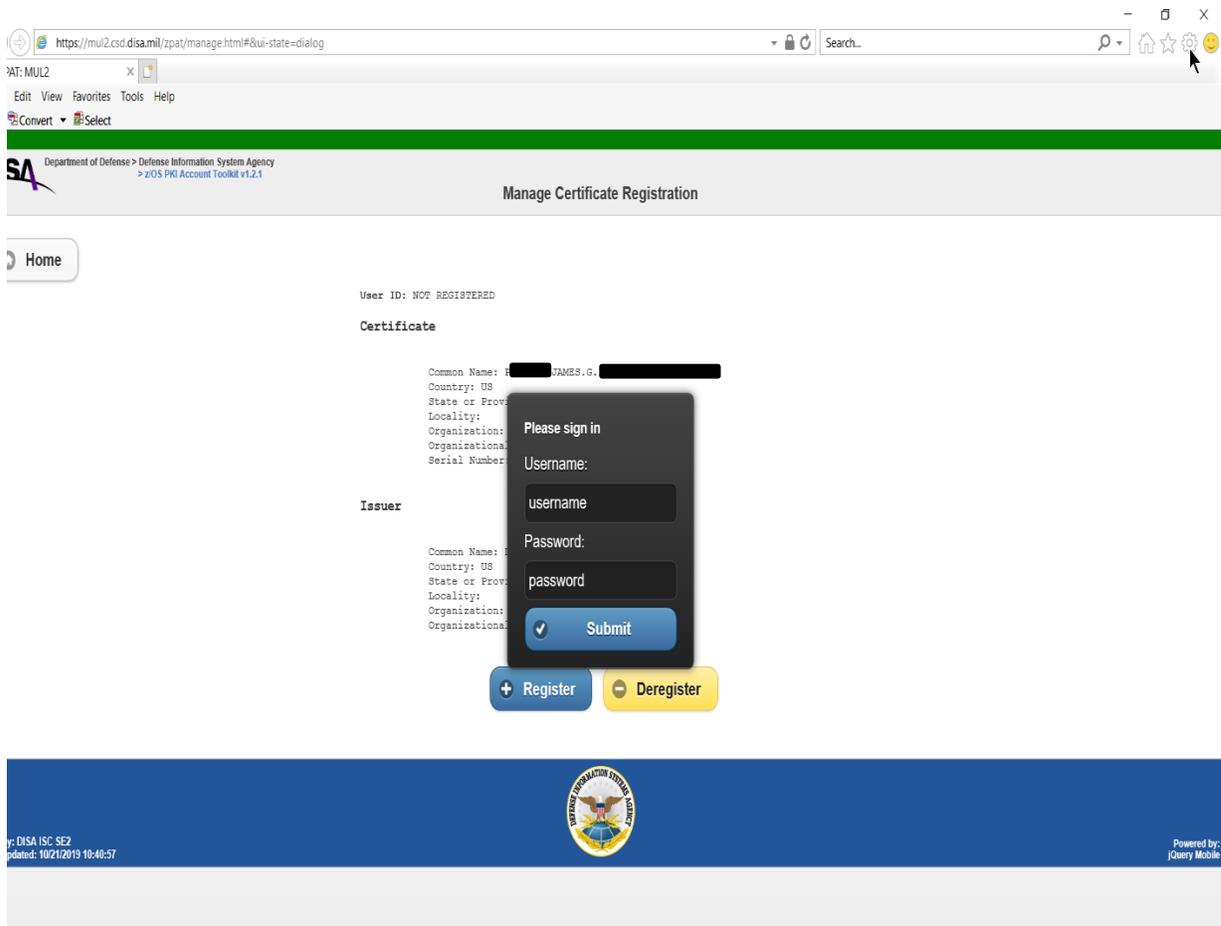
Issuer

Common Name: DOD ID CA-59
Country: US
State or Providence:
Locality:
Organization: U.S. Government
Organizational Unit: FBI

At the bottom of the main content area, there are two buttons: a blue "+ Register" button and a yellow "- Deregister" button.

The footer of the page is a dark blue bar containing the following text on the left: "Built by: DISA ISC SEZ", "Last Updated: 10/21/2019 10:40:57", and the DISA logo in the center. On the right side of the footer, it says "Powered By: jGentry Mobile".

Once you have clicked **“Register”**, you will be prompted for your **Current Userid and Password**. Here you will fill in your UserID/Username and Password for the DSS mainframe to which you are registering your certificate: MUA, MUY or MUL.



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

2.2 DSS CAC DEREGISTRATION (Issued new CAC Card)

To remove/deregister an (old) certificate from the DSS mainframe security system, follow the same process and choose “**De-register**”. You will again be prompted for your **current** 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.

NOTE: 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 mainframe you select, a user will **(not)** be able to perform a Self-Service Password reset – using z/PAT.

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

3.0 Using zPAT for (self-service) password resets

3.1 Requirements

To initiate a Self-Service password reset, you **must have** a current CAC, which has been registered to the DSS mainframe security system you are selecting. If this is your first time in zPAT to register your CAC certificate, and you do not have a current password for the DSS system you are selecting, you will need to call the DLA Enterprise Help Desk to get your password reset, before starting this registration process.

3.2 Self-service password reset process

First, using your Internet Browser, navigate to one of the following DSS URL's.

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

MUY use <https://muy2.csd.disa.mil/zpat>

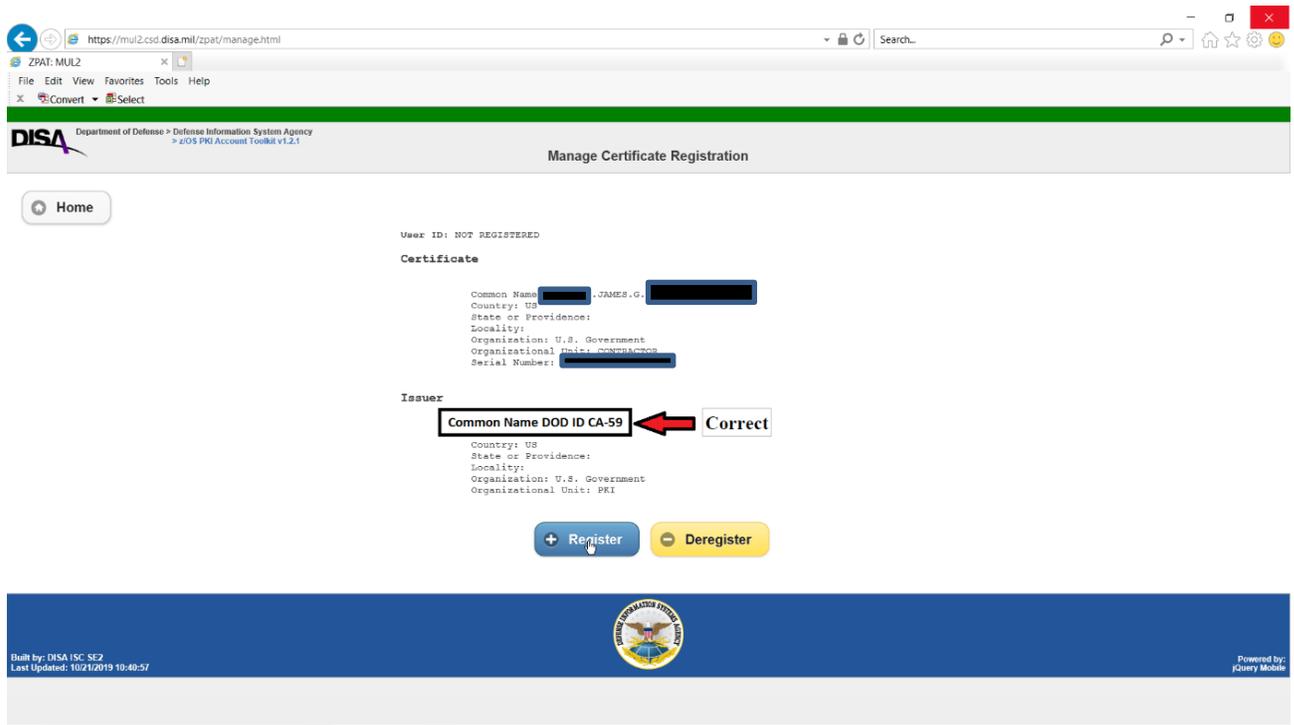
MUL use <https://mul2.csd.disa.mil/zpat>

3.2.1 Initial Entry

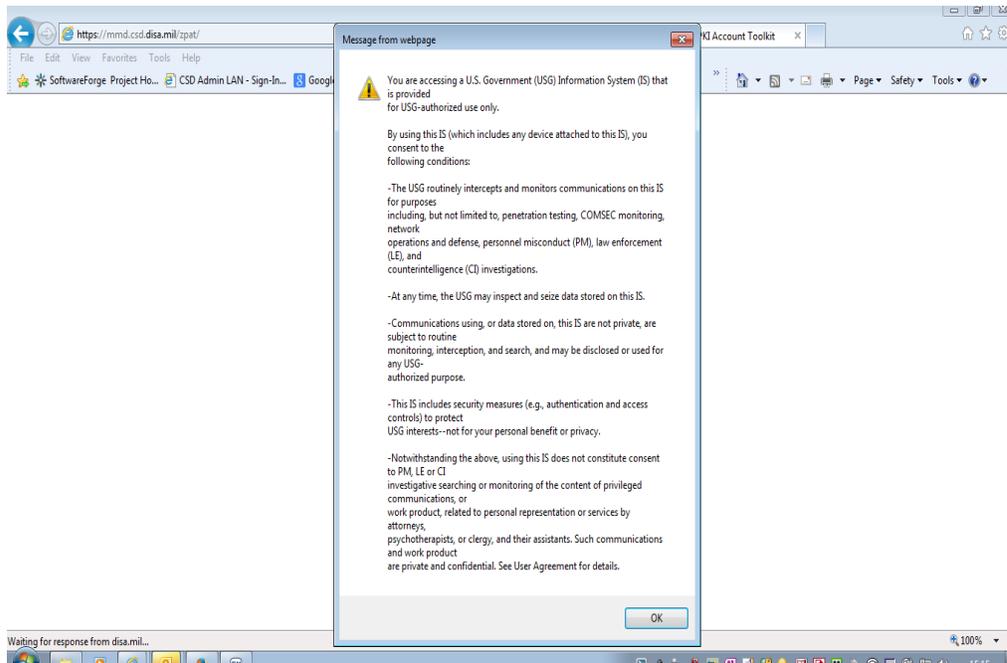
Upon entry to the DISA zPAT URL, you will be presented with the DoD banner page and asked to choose a certificate from the browser certificate store. **For DSS CAC (self-service) password resets using zPAT, YOU MUST CHOOSE the “DoD CA Identity Certificate”; NOT THE “DOD CA EMAIL Certificate”.** The email certificate will not work for CAC-Enabled MIAP Logins.

The initial entry is shown below:

The CAC prompt tiles below are displayed, followed by the login banner:



Login Banner -



zPAT Home Page

Firefox

Utility Home

DISA Multi-Host Internet Access Portal

https://mmg.csd.disa.mil/zpat/index.html

Google

DISA Department of Defense - Defense Information System Agency
z/O5 PKI Account Toolkit v1.0 Beta

Utility Home

To be able to use this utility you need:

1. One or more Personal Certificates installed in your browser.
2. A valid User ID & password within the managing Security Package.

This utility provides the following functions to assist in managing your PKI registration state.

- **Manage Certificate Registration**
When you click this button your browser will ask you to select one of the certificates trusted certificates available to the browser. You will also be prompted for your user id and password. A confirmation screen will show you the information from the certificate you selected and your security package user id.
 - *Register* - allows you to associate the selected certificate to your user id within the security package.
 - *De-register* - removes the association within the security package between the selected certificate and your user id.
- **Reset Password**
Allows you to change your password using an randomly generated STIG compliant password.
Note: This function only works if you have already registered a certificate with the security package.
 - *Generate Password* - generates a random STIG compliant password and uses that value as the password associated with your user id.
 - *Show Password* - displays the password in clear-text for you to copy or read.
Note: "Show Password" will only work after Generate Password has been used.

[Manage Certificate Registration](#) [Reset Password](#)

Built by: DISA ESD E55
Last Updated: 11/06/2013 16:55:28

Powered by: JQuery Mobile

Next, 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, choose “**Register**” as shown below.

https://mul2.csd.disa.mil/zpat/manage.html

ZPAT: MUL2

File Edit View Favorites Tools Help

X Convert Select

DISA Department of Defense - Defense Information System Agency
z/O5 PKI Account Toolkit v1.2.1

Manage Certificate Registration

[Home](#)

User ID: NOT REGISTERED

Certificate

Common Name: JAMES.G
Country: US
State of Providence:
Locality:
Organization: U.S. Government
Organizational Unit: COMUSMACV
Serial Number:

Issuer

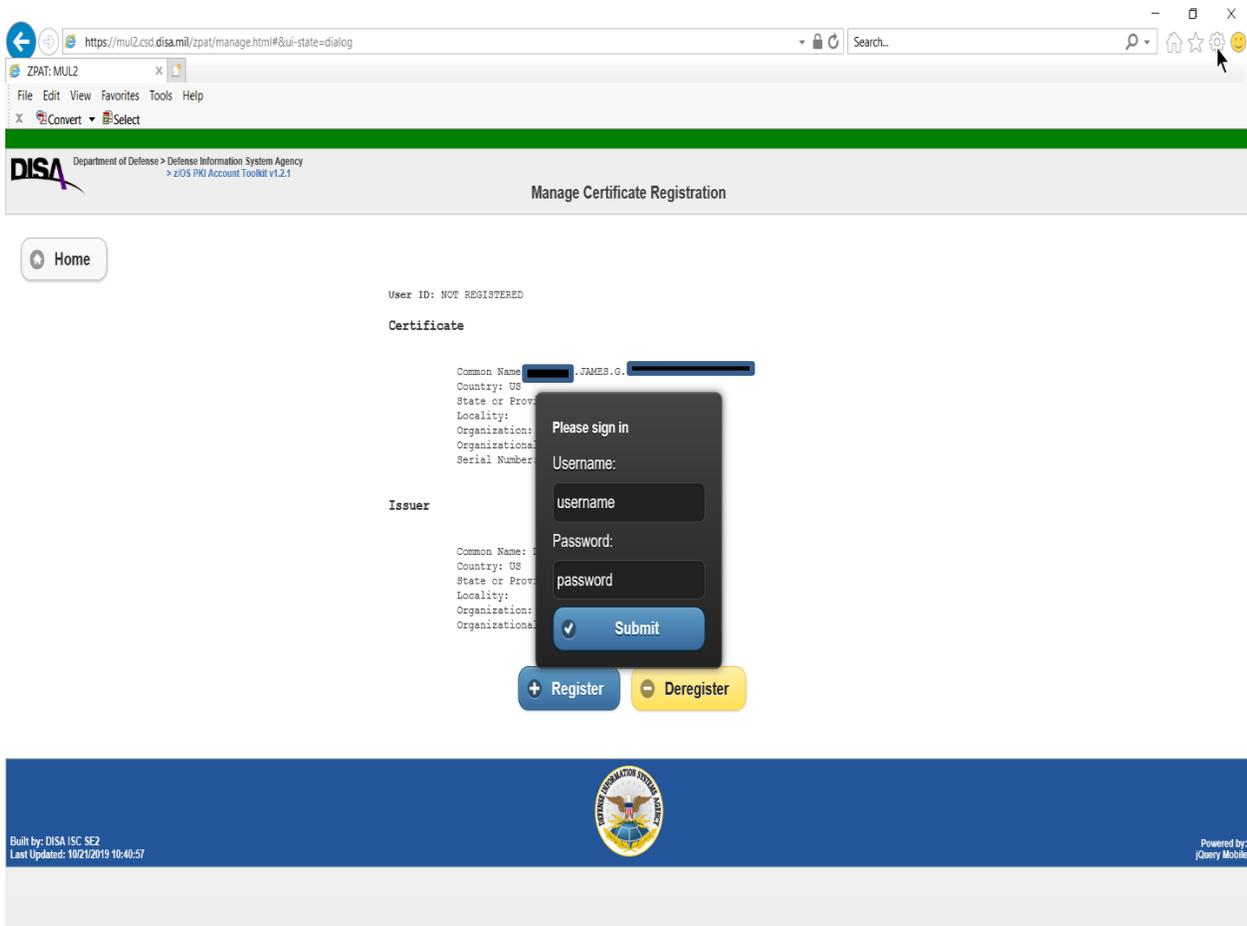
Common Name: DOD ID CA-59
Country: US
State of Providence:
Locality:
Organization: U.S. Government
Organizational Unit: EKI

[+ Register](#) [- Deregister](#)

Built by: DISA ISC SE7
Last Updated: 10/21/2013 10:40:57

Powered by: JQuery Mobile

Once you have clicked “**Register**”, you will be prompted for username and password. Here you will enter your DSS username/UserID and password **for the mainframe to which you are registering** your certificate:



Upon successful CAC registration, the “Response” line at the top left of this page will change to:

Response: success

https://mul2.csd.disa.mil/zpat/manage.html

ZPAT: MUL2

File Edit View Favorites Tools Help

Convert Select

DISA Department of Defense > Defense Information System Agency
P: OCS PPO Account Toolkit v1.2.1

Manage Certificate Registration

Home

Response: success
User ID: kjp0122

Certificate

Common Name: [REDACTED].JAMES [REDACTED]
Country: US
State or Providence:
Locality:
Organization: U.S. Government
Organizational Unit: CONTRACTOR
Serial Number: [REDACTED]

Issuer

Common Name: DOD ID CA-59
Country: US
State or Providence:
Locality:
Organization: U.S. Government
Organizational Unit: PKI

Update MIAP Profile Register Deregister

Built by: DISA ISC SE2
Last Updated: 10/21/2019 10:40:57



Powered by: JQuery Mobile

Once you have clicked "Update MIAP Profile", next screen select the Authentication Certificate

Windows Security

Select a Certificate

Site auth.miap.csd.disa.mil needs your credentials:

 Authentication - [REDACTED].JAMES.G. [REDACTED]
Issuer: DOD ID CA-59
Valid From: 8/10/2020 to 10/31/2022
[Click here to view certificate properties](#)

More choices

 Signature - [REDACTED].JAMES.G. [REDACTED]
Issuer: DOD EMAIL CA-59
Valid From: 8/10/2020 to 10/31/2022

 Authentication - [REDACTED].JAMES.G. [REDACTED]
Issuer: DOD ID CA-59
Valid From: 8/10/2020 to 10/31/2022

 ID - [REDACTED].JAMES.G. [REDACTED]
Issuer: DOD ID CA-59
Valid From: 8/10/2020 to 10/31/2022

OK Cancel

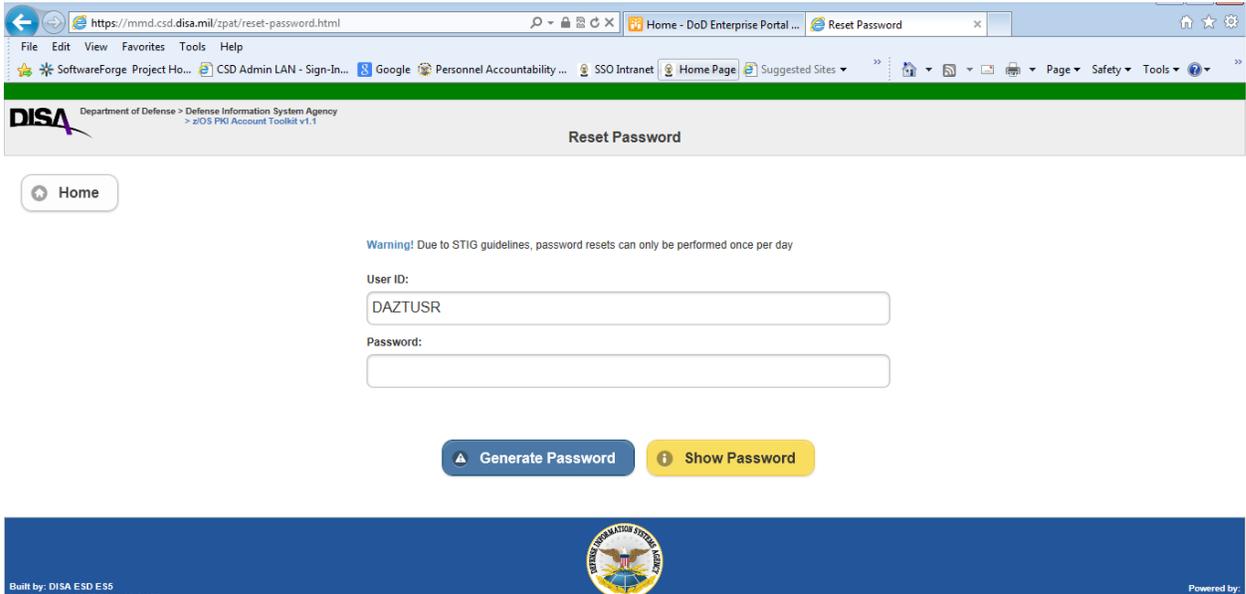
****Note: By using this Certificate for all MIAP access you will automatically be logged into the IBM Mainframe without using your USERID & PASSWORD****

****Once you have clicked “Update MIAP Profile”, the following screen will show success for MIAP.**



3.2.2 Reset Password & User Retrieval

Use the “Reset Password” button to gain entry to the password reset page – the password is not actually reset at this point. When this option is selected, 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/changed.

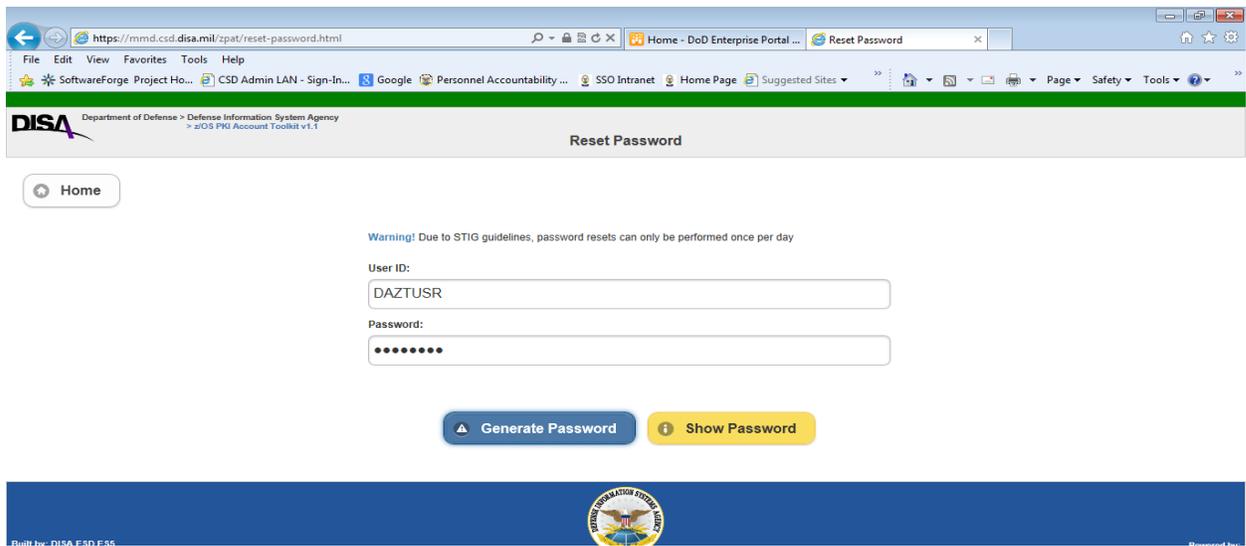


Generate Password

To perform the actual password reset, use the “Generate Password” button. 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 zPAT system selected, MUA, MUY or MUL.

3.2.3 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.



3.2.4 Displaying and Hiding the Password Value

The displayed 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 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).