Defense Manpower Data Center

Personnel Security & Assurance

Public Key Infrastructure (PKI) Technical Troubleshooting Guide

Document Version 4.8

6/15/2017

Please try ALL of the applicable troubleshooting steps PRIOR to calling the PKI issuer or the DMDC Contact Center. Please document the steps that you have tried, people you have talked to, and any error messages that you have received. You will need all of that information in case these troubleshooting techniques do not work.

Contents

1. General Steps / Configuration for ALL credential types 6
1.1. Verify system time 6
1.2. Verify that JPAS/SWFT/DCII is currently available by checking the Alerts page 6
1.3. Ensure Middleware is installed and properly configured (as necessary) 6
1.4. Verify browser settings (SSL/TLS Encryption) 7
1.4.1. General Browser Recommendations 7
1.4.2. Internet Explorer & Chrome 7
1.4.3. Firefox 9
1.5. Verify JPAS/SWFT/DCII server credentials are properly configured (Proxy Server) 11
1.6. Verify you have the correct assurance level credential 12
1.7. Test your PKI Credential 13
1.8. Test your Certification Path 14
2. Credential Specific Configuration Steps 17
2.1. DoD Common Access Card (CAC) 17
2.1.1. Ensure DoD Certificates are properly installed 17
2.1.2. Remove any Potential DoD Cross Certificates in your Certification Path 17
2.1.3. Cross Certificate Re-Population Fixes 20
2.2. External Certification Authority (ECA) 21
2.2.1. Ensure ECA Root Certificates are properly installed 21
2.2.2. Remove any Potential ECA Cross Certificates in your Certification Path 22
2.2.3. Cross Certificate Re-Population Fixes 23
2.3. Federally issued Personal Identity Verification (PIV) 24
2.3.1. Federal PIV Certification Paths 24
2.3.2. Potential Reasons for Auto-Population of Cross Certificates 26
2.4. “Other” DoD Approved PKI / PIV-Interoperable 26
2.4.1. PIV-I Certification Paths 26

2.4.2. Potential Reasons for Auto-Population of Cross Certificates 28
3. Common Logon Errors and Potential Resolution 29
4. Self-Registration 31
5. Other Possible Reasons for PKI Logon Issues 33
6 If all else fails 34
6.1 Submit your case to the DMDC Contact Center 34
6.1.1 How to export a digital certificate from Internet Explorer: 34
Appendix A – Advanced Trust Store Management 35
Appendix B – DMDC Contact Center PKI Escalation Report 39

List of Figures

Figure 1 – Temporary Internet Files 8
Figure 2 – Internet Options 8
Figure 3 – Session Encryption Options 9
Figure 4 - Key InstallRoot options 10
Figure 5 - Firefox Security Devices 11
Figure 6 - Loading Middleware into Firefox 11
Figure 7 – Proper JPAS/SWFT/DCII server certificate 12
Figure 8 – ECA Certificate Policy OID Example 13
Figure 9 - Positive Credential Test 14
Figure 10 – Positive Certification Path Test 15
Figure 11 - Negative Certification Path Test 15
Figure 12 – Internet Options, Content Tab 18
Figure 13 – Selection of an Identity (non-Email) Certificate 18
Figure 14 – Incorrect and Correct DoD CAC Certification Paths 19
Figure 15 – DoD Cross Certificate for Manual Removal 20
Figure 16 - Windows Certificate Manager 21
Figure 17 – Incorrect and Correct ECA Certification Path 23
Figure 18 - ECA Cross Certificates for Removal 24
Figure 19 – Valid external PKI Certification Path 28
Figure 20 - SWFT Self-Registration Screen 32
Figure 21 - SWFT Password Reset Screen 32
Figure 22 - DCII Smartcard Registration Screen 32
Figure 23 - Windows Mass Management Console 35
Figure 24 - MMC File Options 36
Figure 25 - MMC Certificate Snap-in 36
Figure 26 - Snap-in Selection 37
Figure 27 - Local Computer Certificate Manager 37

General Information:

JPAS, SWFT, and DCII accept 3 general types of hardware PKI with assurance levels of Medium Hardware (if you are working with ECA providers they have an equivalent called Medium Token). Please see our PKI FAQ (Question 29) for additional information:

1. DoD Common Access Card / DoD sponsored External Certification Authority (ECA)
2. Federally Issued Personal Identity Verification (PIV), and
3. "Other" DoD approved PKI, often referred to as "PIV-I" in colloquial terminology

For a full list of publicly available PKI providers that are "DoD Approved" please see our DoD Approved PKI Providers slide.

General Note: Some organizations have locked certain configuration options on their desktops or laptops so that end users do not have administrative control of their machines. If this is the case, please contact your Support or IT team if you do not have the proper accesses to complete the following troubleshooting steps.

Card Readers: Due to the vast array of smart card readers available on the market, please note that this guide **does not** include guidance on hardware setup. If you are having issues with the card reader itself, please note the manufacturer and model number and attempt to find the correct device driver on the manufacturer's website or have your operating system try to download the appropriate driver.

PKI Credential Assurance Level: JPAS, SWFT, and DCII only accept PKI of medium assurance or medium token assurance levels, both of which are **only** issued on a hardware form factor such as a smartcard or encrypted USB token. If you have the certificate installed on your hard drive without a form factor, you have a software certificate which is not the correct level for system access.

Operating System/Browser Notes: Though JPAS will work with most operating systems and browser combinations, small populations of users that have a **Windows Home** edition Operating System are reporting an inability to manually remove certificates. We are working with these users to try to find a work around, but if you fall into this category of users, also try to move cross certificates by placing them into your untrusted store as shown in Figure 16 of section 2.1.3. If you are unable to complete the group policy editor or access the Windows Credential Manager, please try to enable usage with Mozilla Firefox as your browser. This browser has an independent certificate manager from the OS and is able to be edited by the user.

Windows 7, Windows 8, and Windows 10 do have the ability to consume Federal PIV and DoD CAC credentials without the use of middleware. Given various software and driver compatibility issues, sometimes it can be beneficial to uninstall any middleware that you have in order to test logging on to the application. Additionally, uninstalling existing drivers using device manager and allowing the OS to download the proper drivers via 'plug & play' installation has been known to work for some PIV and CAC holders.

Network Notes: Some networks enable proxy servers which can actually interrupt the client authenticated SSL/TLS session that must be established when logging onto JPAS, DCII, or SWFT. Please coordinate with your IT/network administrators to ensure that your network/machine is not configured to go through a proxy before attempting to access the application.

Use with Apple computers: Specific instructions for enabling operation with Apple systems are available at the following site: http://www.militarycac.com/apple.htm. You will need to know your specific version of MAC operating system.

Application Specific Notes:
SWFT supports versions IE9 and higher. Users of other browsers, such as Chrome and Firefox, are not supported and users of these browsers may experience issues while running SWFT. Additional steps may need to be taken if you are using IE11. These steps can be found on the PSA website here. Additionally, SWFT users need to ensure that the name on their credential exactly matches the name on the account. For instance, if the name on a SWFT account is John O'Doe and the PKI credential has John ODoe, then the account will have to be updated to reflect what is on the PKI credential to allow access (this point is reiterated in Chapter 4).

JPAS has been tested to work with all versions of IE; however, certain configurations might be required to ensure full functionality with all aspects of the application, such as reports.

DCII has been tested to work with all versions of IE; however certain configurations might be required to ensure full functionality of the application.

1. General Steps / Configuration for ALL credential types

1.1. Verify system time

- Ensure your computer's date and time are correct
  - i. Although many computer systems are networked and receive a regular automated time update, some may not reflect the proper date and time
  - ii. If the computer system is set for a date outside of the time period of validity of a PKI certificate, the certificate cannot be validated/trusted
  - iii. It is recommended that if you have not enabled your system to update time from a trusted server that you enable synchronization with an official time provider such as NIST. For a list of their available servers see the link below:
    http://tf.nist.gov/tf-cgi/servers.cgi
    The NIST server most commonly used is: http://nist.time.gov

1.2. Verify that JPAS/SWFT/DCII is currently available by checking the Alerts page

- DMDC JPAS/SWFT/DCII Website:
  https://psa.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS
  https://psa.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT
  https://psa.dmdc.osd.mil/psawebdocs/docPage.jsp?p=DCII
- A web page with a red color coded scheme stating the application is unavailable will be displayed if the system is down. A yellow indicator may also indicate that the system is experiencing intermittent issues or delays. Either status will be followed by a short description of the issue.

1.3. Ensure Middleware is installed and properly configured (as necessary)

- Many of the more recent operating systems (such as Windows 7/8/10) do not require the use of middleware in order to consume hardware PKI credentials issued by the Federal Government (such as the DoD CAC or Federal PIV). In some of these cases (especially Windows 8 and IE11) uninstalling any middleware may be beneficial for proper operation; however,
- Most legacy operating systems (such as Windows XP, Vista, NT, etc.) do require the use of a middleware (such as ActivClient, Oracle Fusion, Spyrus, SafeNet, eToken or various other vendors), and even if you are a Windows 7/8/10 user with an ECA or other publicly available PKI credential, you will still more than likely require the middleware for proper operation. Coordinate with your provider for additional information.
  - i. Active Duty Military generally have access to middleware via an Enterprise License. Contact your local IT staff as necessary to coordinate how to acquire your respective software installation packages.
  - ii. Partners who purchase PKI credentials from a DoD approved vendor might also have middleware options available through that particular vendor.

- **Important Note**: Some middleware may require the log on prior to Token/Smartcard usage
- **Also Note**: Middleware and Browsers need to communicate on the same processing standard (32-bit or 64-bit only). If you are having trouble connecting to JPAS/SWFT/DCII, it might be due to what speed of browser you are using. IE8 and 9 users might find both versions in the start menu under all programs, please test both if you are experiencing logon issues. IE10 and 11 users might have to toggle the "Enable Enhanced Protection Mode" under the advanced options to switch browsing bit-speeds.

1.4. Verify browser settings (SSL/TLS Encryption)

1.4.1. General Browser Recommendations

- Clear your browser SSL cache by closing all browser instances before attempting to logon to JPAS/SWFT/DCII, and cycle your browser for each logon test
- Add "https://psa.dmdc.osd.mil" and "https://*.dmdc.osd.mil" to your list of trusted sites
  - In IE, go to Tools → Internet Options → Security tab → Select the 'Trusted Sites' icon → Click the "Sites" button and copy the above address in the text dialog; be sure to apply changes
  - Your network policy might limit this action to administrators only, please coordinate with your IT departments, as needed

1.4.2. Internet Explorer & Chrome

- Chrome inherits many of the user's Operating System and Browser settings such as: SSL/TLS encryption and the certificates installed in the Windows Credential Manager; hence, several settings that will effect Chrome must be configured in Windows/Internet Explorer
- Close all IE browsers. No instances should appear on your task bar
- Delete contents of the Temporary Internet Files Folder
  - see http://support.microsoft.com/kb/260897 for details
- Once IE window is reopened, select the Tools menu
- Select Internet Options
  - The default tab selected should be the General Tab
    - Click 'Settings' button under Browser History header
    - Ensure the "Every time I visit the webpage" option is selected, then click Ok (Figure 1)

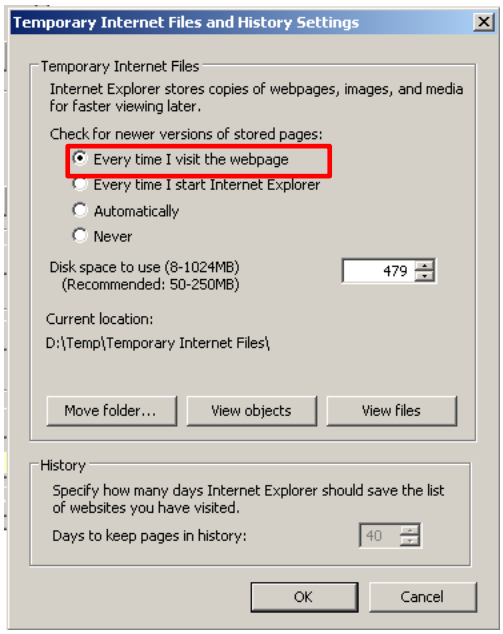


Figure 1 – Temporary Internet Files

- Next, select Content Tab and click Clear SSL state (Figure 2)

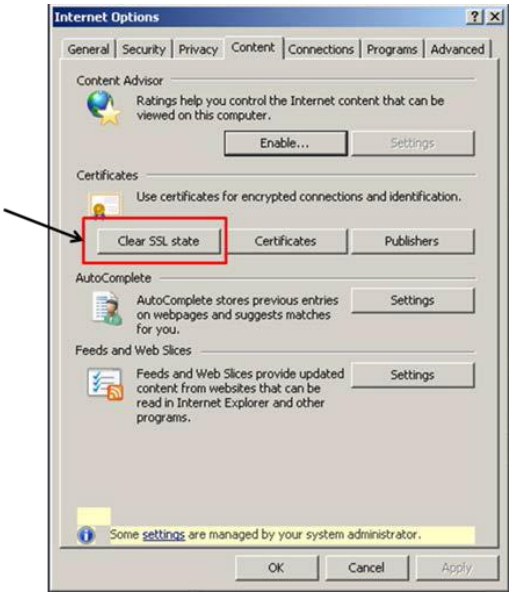


Figure 2 – Internet Options

- Finally, select the Advanced Tab (Figure 3)
  - Ensure the following options toward the bottom of the slider are checked:
    - Use TLS 1.0
    - Use TLS 1.1
    - Use TLS 1.2

- Newer browser versions (IE10 and above) can negotiate a TLS handshake properly regardless of the enabled encryption options
- Ensure "Do not save encrypted pages to disk" is unchecked
- IE11 users might also have to ensure that "Enable Enhanced Protected Mode" is also checked under the advanced settings, and restart the system so changes can take effect
- IE 11 users might have to ensure that "osd.mil" is added to the list of compatibility view mode sites from the tools menu

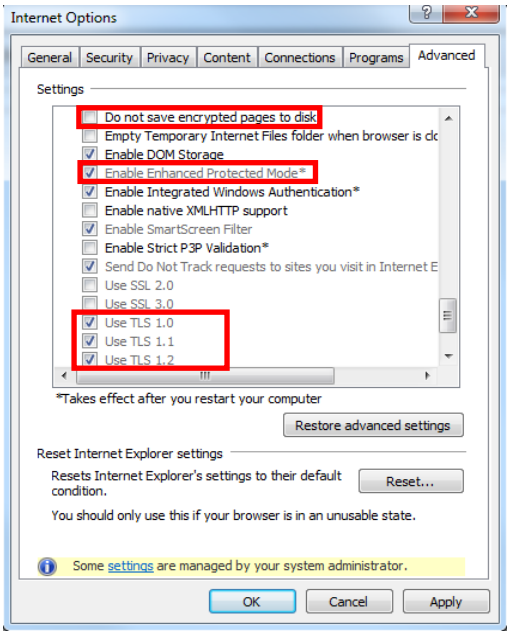


Figure 3 – Session Encryption Options

1.4.3. Firefox

- General configuration guidance:
  - Newer versions of **Mozilla Firefox** come pre-configured to use specific SSL and TLS protocols and the process to reconfigure these settings are significantly more complex then Section 1.4.2 provides for Internet Explorer. As a result, it is recommended that the user does not attempt to change these configurations.
  - CAC holders can access additional PKE team configuration guidance for Firefox at the following link: https://powhatan.iiie.disa.mil/pki-pke/landing_pages/downloads/unclass_config_firefox_dod-cac.pdf

- **Important**: Given the fact that Firefox has an independent trust store from the operating system, an additional burden of installing several DoD and PKI provider certificates directly to the browser is required:
  - It is recommended that Firefox users install the root and intermediate DoD and ECA certificates using the following utility:
    - The DISA PKI team provides InstallRoot: NIPR Windows Installer tool that can assist in the installation of the proper certificates into the Firefox browser. The tool can be found at the following link:
      - http://iase.disa.mil/pki-pke/Pages/tools.aspx
      - Under the "Trust Store" tab
      - Please read the User's Guide to assist in installing the tool and certificates
  - When utilizing the InstallRoot GUI tool please take care to select **Yes** to the " Firefox store was discovered" message (see Figure 4), and ensure both DoD and ECA certificates are checked for the installation in the Firefox trust store

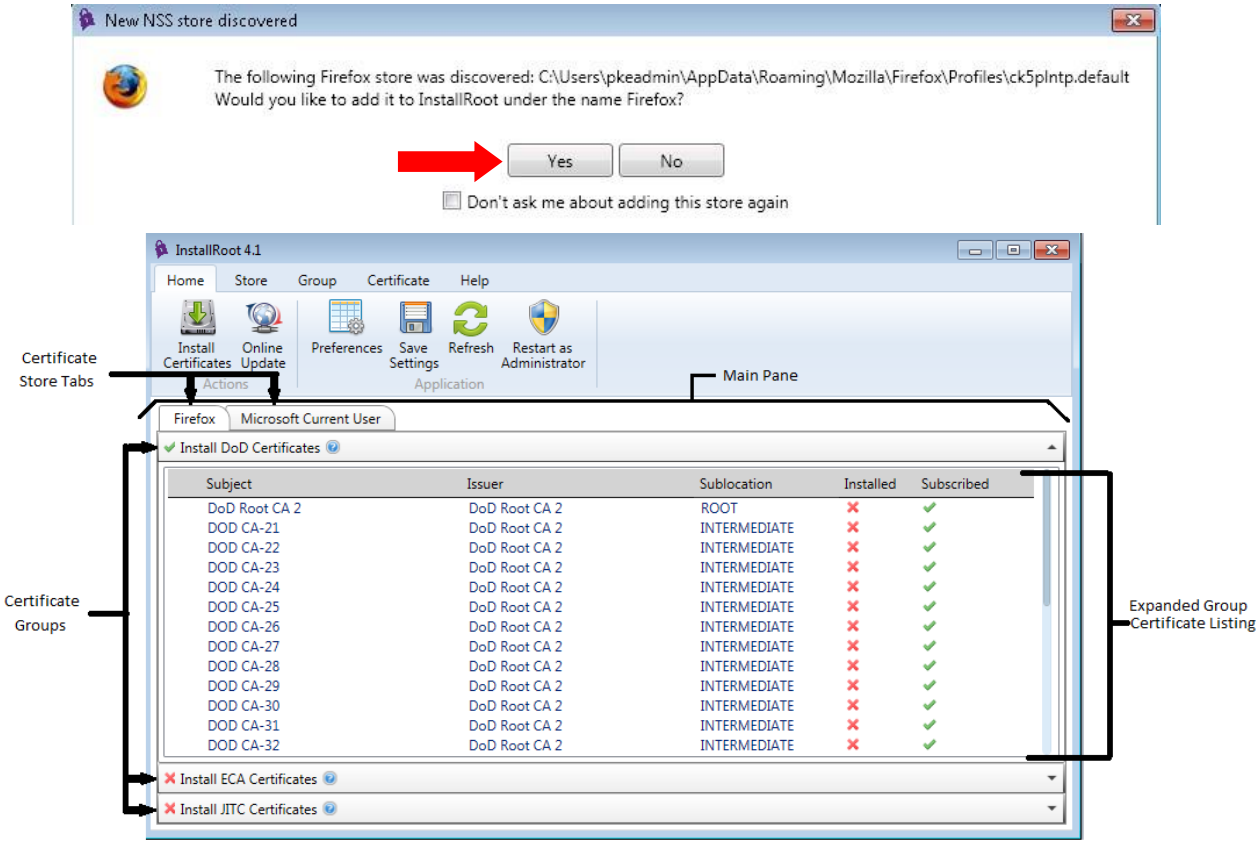


Figure 4 - Key InstallRoot options

- **Also note**: you will have to make your middleware and certificate hardware recognizable to Firefox as these devices are not included in the browser by default. Figure 5 shows the location within Firefox options for this configuration item

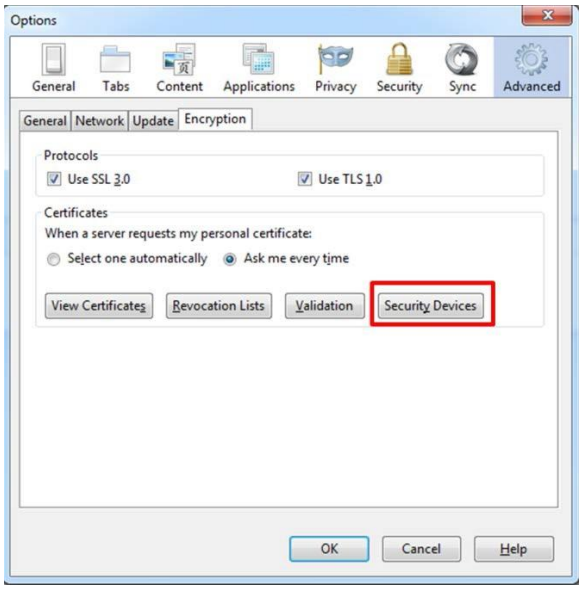


Figure 5 - Firefox Security Devices

- Each middleware will have a different file that your browser can utilize to read your certificates. Please work with your specific PKI/middleware vendor to identify this configuration item (Figure 6)
- ActivClient configuration instructions are available at the following link: http://militarycac.com/files/Tech_Note_Firefox_CAC_Authentication.pdf

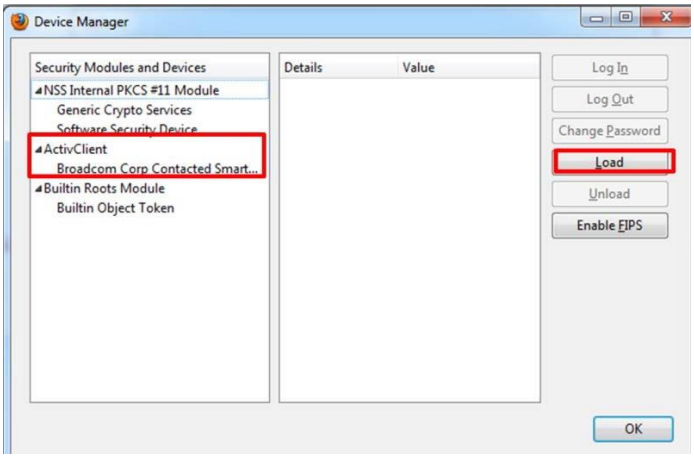


Figure 6 - Loading Middleware into Firefox

1.5. Verify JPAS/SWFT/DCII server credentials are properly configured (Proxy)

Visit one of the following sites, depending on the application you plan to access:
https://JPASapp.dmdc.osd.mil/JPAS/JPASDisclosure,
https://dcii.dmdc.osd.mil/dciiweb/login/login.jsp,
https://swft.dmdc.mil/

- Click the **Padlock** button on the end of the URL address bar
- Select the **View Certificates** button
- Select the **Certification Path** tab

- Verify the trust chain of jpasapp.dmdc.osd.mil → **DoD Root CA 3** → **DoD ID SW CA-37** (Figure 7 below)
    - If there are any other certificates in the path above **DoD Root CA 3**, please see Section 2.1.2 and specifically Figure 14 & Figure 15
    - If you notice that the JPAS/SWFT/DCII app certificate is issued by anything other than a Department of Defense Certification Authority, you will need to work with your Network administrators to ensure that you do **NOT** have a proxy server enabled
    - Software server certificates are re-issued generally every 3 years, as a result, the issuing certification authority will not be consistent, but it will always be a DoD CA

Figure 7 – Proper JPAS/SWFT/DCII server certificate

1.6. Verify you have the correct assurance level credential

- JPAS/SWFT/DCII requires the equivalent of FBCA **Medium Hardware** that only come on one of two form factors:
    i. Smartcards
    ii. FIPS 140-2 Compliant USB Tokens
- **SOFTWARE CERTIFICATES ARE NOT ACCEPTABLE BY POLICY.** Your PKI credential always needs to be on a **physical** FIPS 140-2 compliant device, such as a smartcard or a UBS token. If you do not have one of these devices, you will not be able to access your JPAS/SWFT/DCII account.
- This information can be inferred from the "certificate policy" field from a user's X.509 certificate:

i. Older DoD CACs should have a certificate policy OID of: 2.16.840.1.101.2.1.11.9 (id-US-dod-mediumhardware)

ii. Newer DoD CACs with certificates issued from CA-41+ may also have certificate policy OID of: 2.16.840.1.101.2.1.11.19 (id-US-dod-mediumHardware-2048), 2.16.840.1.101.2.1.11.42 (id-US-dod-mediumHardware-112), and/or 2.16.840.1.101.2.1.11.43 (id-US-dod-mediumHardware-128)

iii. ECA certificates can have one of two acceptable OIDs:
   - 2.16.840.1.101.3.2.1.12.2 id-eca-medium-hardware (Figure 8)
   - 2.16.840.1.101.3.2.1.12.3 id-eca-medium-token

iv. Federal PIV Authentication Certs should have a policy OID of: 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

v. Other DoD Approved credentials will have various policy OIDs that have been mapped by the DoD and the list is too extensive to re-publish here. The general rule of thumb is that they have to be on FIPS 140-2 compliant hardware (i.e. USB drive, or smartcard)

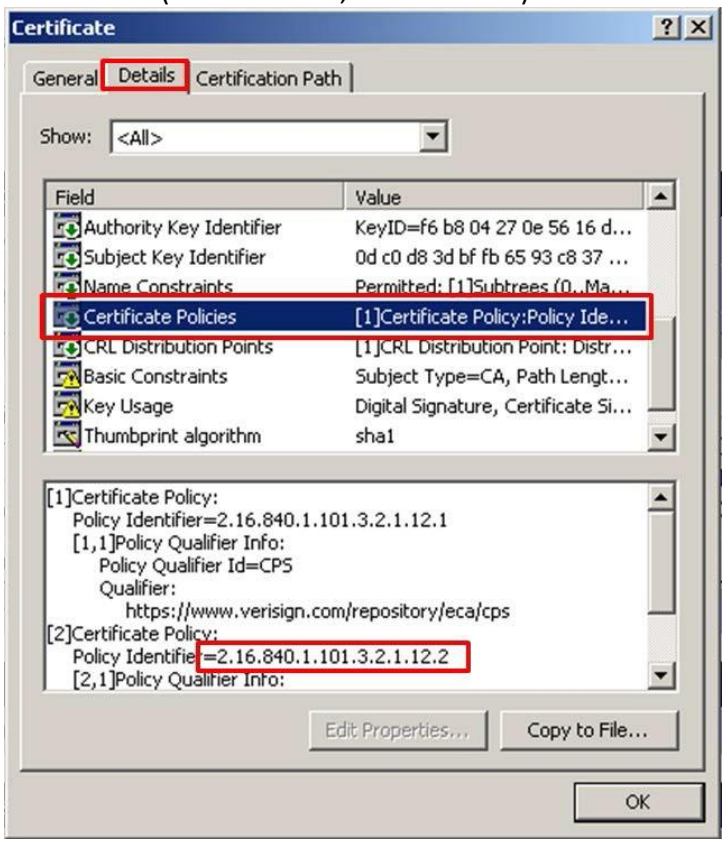


Figure 8 – ECA Certificate Policy OID Example

1.7. Test your PKI Credential

- The following site provides a PKI test for the JPAS/SWFT/DCII application logon: https://JPASpki.dmdc.osd.mil/JPAS/GetCert

  i. When prompted, please select your identity or email signing certificate (preferably your **identity certificate**)

  ii. If you are not presented with a certificate tile window (where you select

your personal credential), please clear your SSL cache as outlined above in Section 1.4, specifically Figure 2

iii. If working properly, you should see a page entitled "Request Information." See Figure 9 as an example of a positive test

- Save your results page as a PDF or copy and paste the contents into a .txt or .doc file, or make note if an error is presented. You may need the result of this step in the event that all troubleshooting steps fail and you make it to Section 5.1 of this document
- If you continue to get the "Cannot display webpage error" or a SSL handshake error, you more than likely have a cross certificate issue. Please move to section 1.8 below to test your certification path

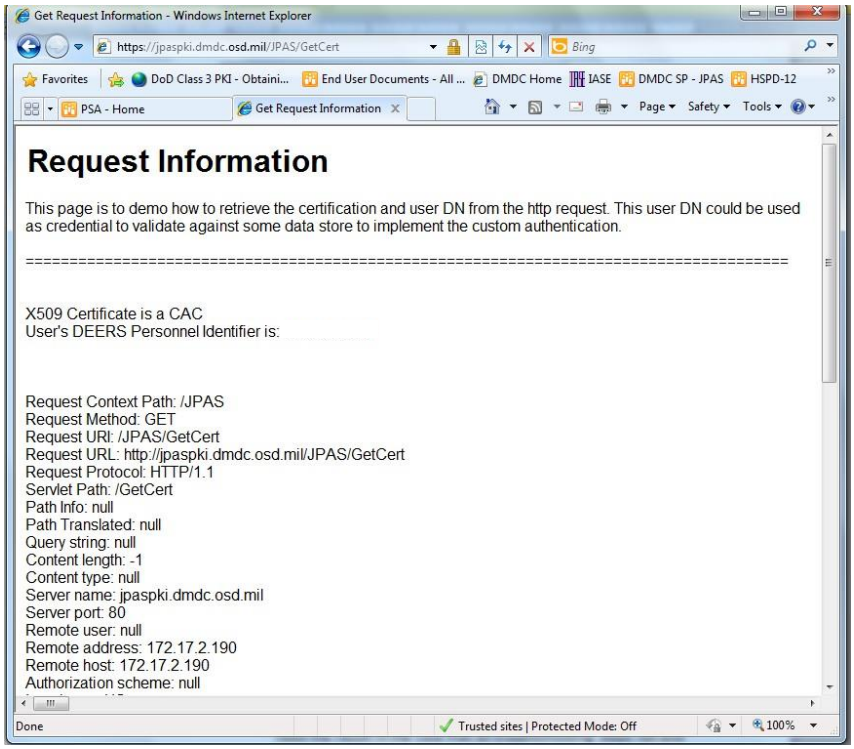


Figure 9 - Positive Credential Test

1.8. Test your Certification Path

- If you receive an "Internet Explorer cannot display webpage," error in IE or a "SSL/TLS handshake error," in Firefox, DMDC has created a page that will attempt to validate the certification path the user machine is presenting to our load balancer
- Please visit the following site to test your certification path:
  - https://check.dmdc.mil

- Provided your computer is building the proper certification path, the resulting page should look similar to Figure 10 where each certificate in your path is shown and a green check mark validates each certificate
- If the result shows red exclamation marks, as in Figure 11, you know that your trust store will need to be configured to end in a self-signed root CA as described in Sections 2.1.2, 2.2.2, 2.3.1, or 2.4.1

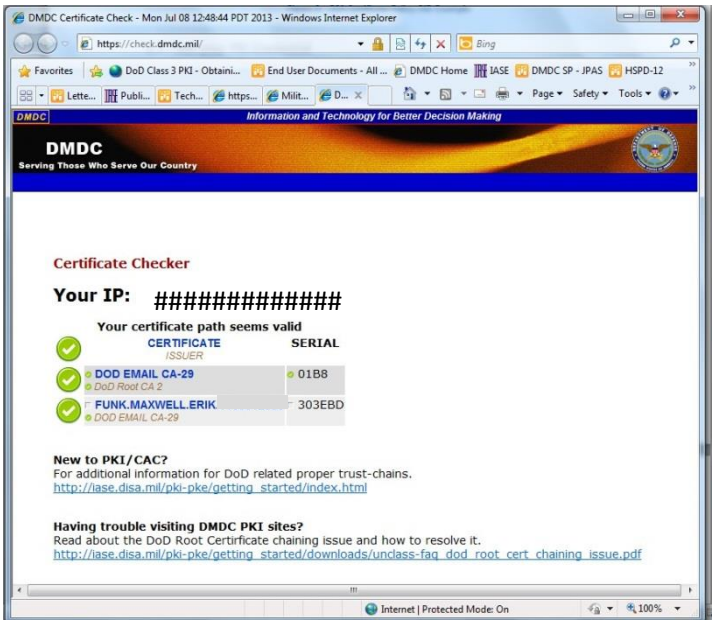


Figure 10 – Positive Certification Path Test

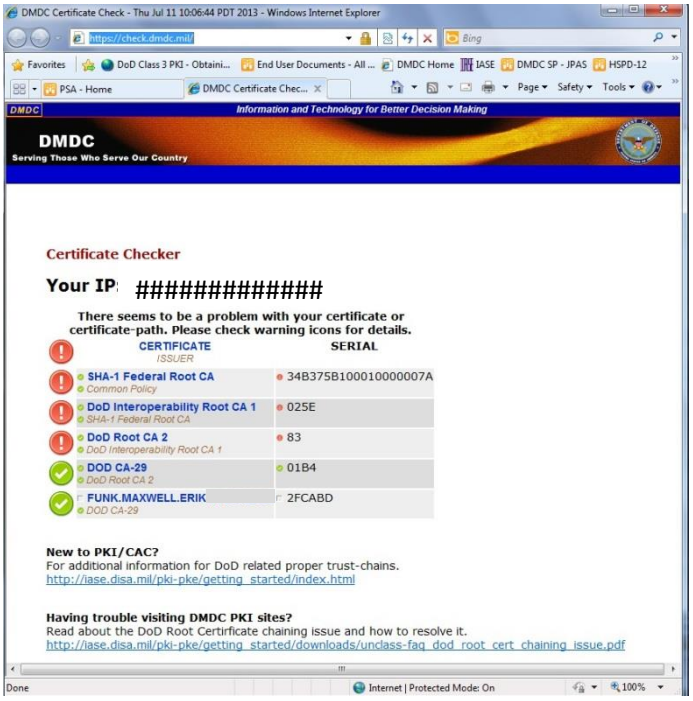


Figure 11 - Negative Certification Path Test

Before proceeding to the next section please verify the category of your PKI credential and find the corresponding section from the table of contents.

DCII users will only have either a DoD issue CAC or a Federal PIV, as a result they will only require guidance in sections 2.1 or 2.3.

2. Credential Specific Configuration Steps

2.1. DoD Common Access Card (CAC)

DMDC policy has been updated to allow CAC holders to use their identity credential for system access regardless of their role or contracting specifics, provided they have met all of the prerequisites and have been authorized a JPAS, DCII or SWFT account. For more information please see the JPAS PKI FAQ Question #35, the SWFT PKI FAQ #19, or the DCII PKI FAQ #28.

2.1.1. Ensure DoD Certificates are properly installed

- **CAC users** require the "**DoD Root CA 3"** self-signed root certificates that expires in 2029 to be in their trusted root certification authorities store
- There are two primary sources for the DoD certificate packages as listed below. Only one of them needs to be used:
  - DISA IASE Tools Site: http://iase.disa.mil/pki-pke/Pages/tools.aspx
    Under the **Trust Store** tab, download and run **InstallRoot x.x: NIPR Windows Installer** for Windows/IE users only
  - Select the For DoD PKI Only – Version x.x link and extract the Certificates_PKCS7_vX.X_DoD folder to your Desktop (or a known location)→ Open the folder, Right click on the file Certificates_PKCS7_vX.X_DoD.der.p7b and select Install Certificate → Select "Place all certificate in the following store"→ Select Browse→ Select "Trusted Root Certification Authority"→ Click Next→ Click Finish→ Select Yes to all Security Warnings pertaining to "You are about to install a certificate from a certification authority (CA) claiming to represent: DoD EMAIL CA-xx, DoD CA-xx, DoD ID SW CA-xx, and DoD ID CA-xx.

2.1.2. Remove any Potential DoD Cross Certificates in your Certification Path

- The majority of authentication failures are due to cross certificate errors. Please follow the directions below to ensure you have no cross certificates in your trust store. Make sure you complete or verify all steps in Section 2.1.1 before moving on to cross certificate removal.

- JPAS, SWFT, and DCII utilize the Direct Trust model for Public Key Enablement and rely on the client generated certification path. Therefore, these applications cannot process authentication requests from a browser that presents cross certificates in its path. It is recommended that CAC holders run the FBCA Cross Certificate Removal Tool provided by DISA:

  - Download and run the "FBCA Cross-Certificate Remover" available under the Certificate Validation tab at the following page: http://iase.disa.mil/pki-pke/Pages/tools.aspx
  - Once you have ran the tool, verify your certification path does not

contain cross certificates:

- From your browser select "Internet Options" → Content Tab → Certificates Button (Figure 12) → Personal Tab → Double click your identity certificate (Figure 13) → Certification Path tab (Figure 14)

Figure 12 – Internet Options, Content Tab

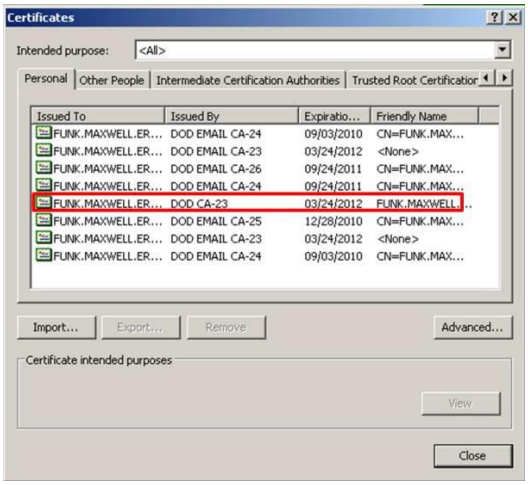


Figure 13 – Selection of an Identity (non-Email) Certificate

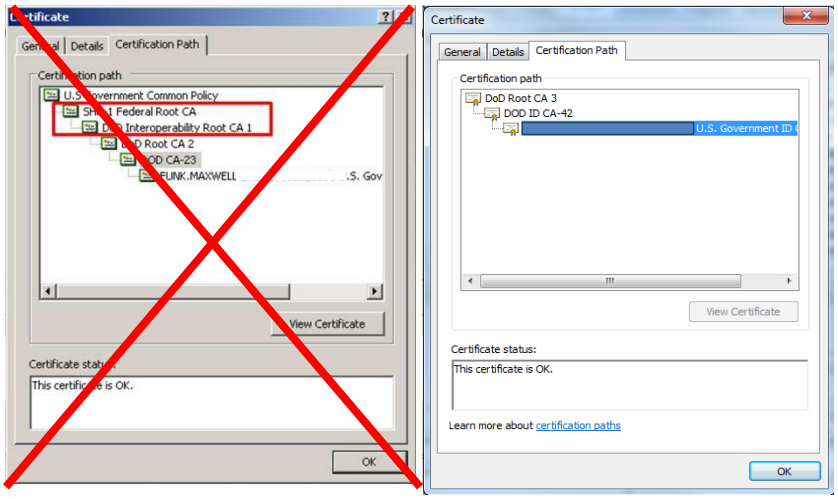


Figure 14 – Incorrect and Correct DoD CAC Certification Paths

- If the automated tool above does not work to remove the DoD cross-certs, the following are instructions for manual removal from Internet Explorer/Windows Credential Manager
  - Open Internet Explorer → Select Tools → Internet Options → Content Tab → Select the Certificates button → Select the **Intermediate Certification Authorities** Tab
  - Figure 14 shows DoD Cross Certificates that need to be removed for proper operation. These certificates are by default listed in alphabetical order by the "issued to" field
  - Select and remove the certificate issued to "DoD Root CA 2/3," as issued by the "**DoD Interoperability Root CA**" (See Figure 15)
- Additional information on cross certificates and DoD users is available at the following CAC enabled site: https://powhatan.iiie.disa.mil/pki-pke/downloads/pdf/u_dod_root_certificate_chaining_problem_v1.0_15mar2010.pdf

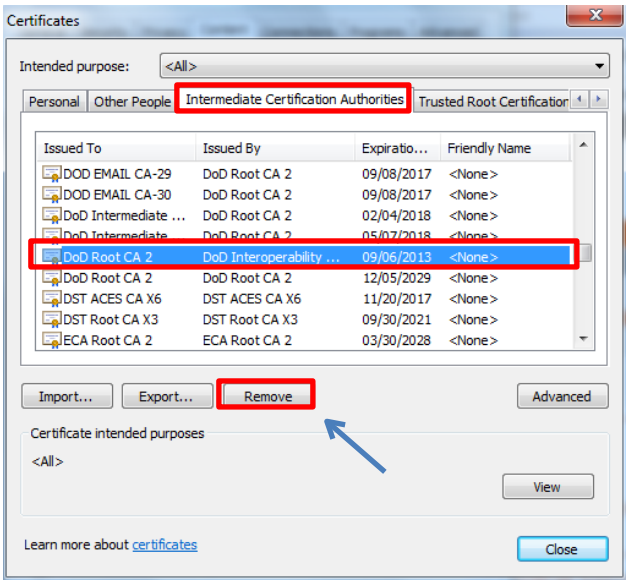
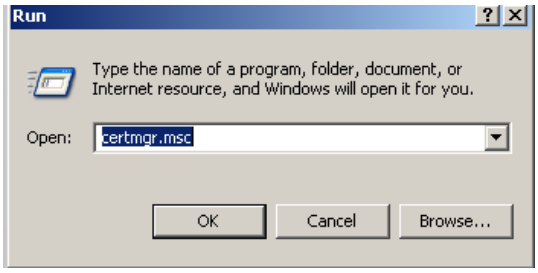


Figure 15 – DoD Cross Certificate for Manual Removal

2.1.3. Cross Certificate Re-Population Fixes

- If you maintain an operating system of Windows XP or more current, the Microsoft Root Certificate Program has the potential to automatically install non-DoD approved CAs onto your machine via Windows Updater
- If you are having difficulty keeping the DoD cross certificates out of your Intermediate CA trust store, you can simply import or move the cross certificates to the "Untrusted Certificates" store, as this takes precedence over the other stores/folders
    - The most efficient way to do this is by using the Windows Certificate Manager to drag and drop the cross certs in your intermediate trust store into the Untrusted Certificate folder (see Figure 16)
    - To do this, open the Windows Run Command from your Accessories folder or use the hotkey [Windows Key+r]
    - Type "certmgr.msc" into the prompt and hit OK
    - In the new window expand the "Intermediate Certification Authorities" folder as well as the "Untrusted Certificates" Folder in the left pane and then select the "Certificates" sub folder under Intermediate Certification Authorities
    - This will populate a list of certs on the right pane. Find the "DoD Root CA 2/3" certificate issued by the "DoD **Interoperability** Root CA" and drag and drop that certificate into the certificate sub folder under "Untrusted Certificates" on the left pane



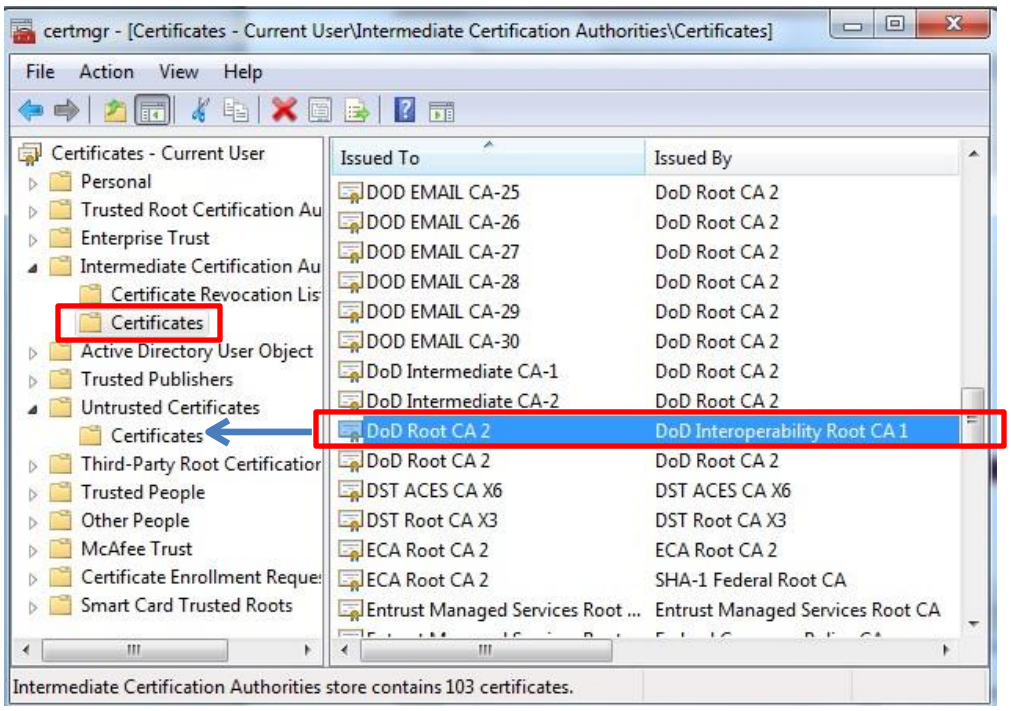


Figure 16 - Windows Certificate Manager

2.2. External Certification Authority (ECA)

External PKI holders will have to self-register their certificates once they have completed authentication. Please coordinate with your account manager/organization administrator or the DMDC Contact Center to receive your account username and temporary password that will be used in the registration process. Also note that this registration password is completely separate and distinct from the password that you may have self-generated for your smartcard or token.

2.2.1. Ensure ECA Root Certificates are properly installed

- **ECA users** require the "ECA Root CA 4" self-signed root certificate that expires in 2029 to be in their Trusted Root Certification Authorities store
- If you are an ECA holder, root certificates can be located and installed from one of the two following locations (publicly available sites):
  - DISA IASE Tools Site: http://iase.disa.mil/pki-pke/Pages/tools.aspx
    Under the **Trust Store** tab, download and run **InstallRoot x.x: NIPR Windows Installer** for Windows/IE users only
  - Select the Download External Certificate Authority (ECA) Root CA 4 Certificate link and save to your desktop (or a known location) → Right

click on the file and select Install Certificate → Select "Place all certificate in the following store" → Click Browse → Select Trusted Root Certification Authority → Click Next → Click Finish

- Select the For ECA PKI Only – Version x.x link and extract the Certificates_PKCS7_vX.X_ECA folder to your Desktop (or known location)→ Open the folder, Right click on the file Certificates_PKCS7_vX.X_ECA.der.p7b and select Install Certificate → Select "Place all certificate in the following store"→ Select Browse→ Select "Trusted Root Certification Authority"→ Click Next→ Click Finish→ Select Yes to all Security Warnings pertaining to "You are about to install a certificate from a certification authority (CA) claiming to represent: VeriSign Client External Certification Authority – G3, IdenTrust ECA x, ORC ECA SW x, ORC ECA HW x, ORC ECA 6 and Symantec Client External Certification Authority – G4.
  - Firefox users please see Section 1.4.3 for certificate installation instruction for that browser

2.2.2. Remove any Potential ECA Cross Certificates in your Certification Path

- The majority of authentication failures are due to cross certification errors. Please ensure you follow the directions below to ensure you have no cross certificates in your trust store. Make sure you complete or verify all steps in Section 2.2.1 before moving onto cross certificate removal.
- JPAS/SWFT/DCII utilizes the Direct Trust model for Public Key Enablement and relies on the client generated certification path and therefore cannot process authentication requests from a browser that presents cross certificates in its path, it is recommended that CAC holders run the FBCA Cross Certificate Removal Tool provided by DISA:
  - Download and run the "FBCA Cross-Certificate Remover" available under the Certification Validation tab at the following page: http://iase.disa.mil/pki-pke/Pages/tools.aspx
  - Once you have ran the tool, verify your certification path does not contain cross certificates:
    - From your browser select "Internet Options" → Content Tab → Certificates Button (Figure 12) → Personal Tab → Double click your identity certificate (Figure 13) → Certification Path tab (Figure 17)

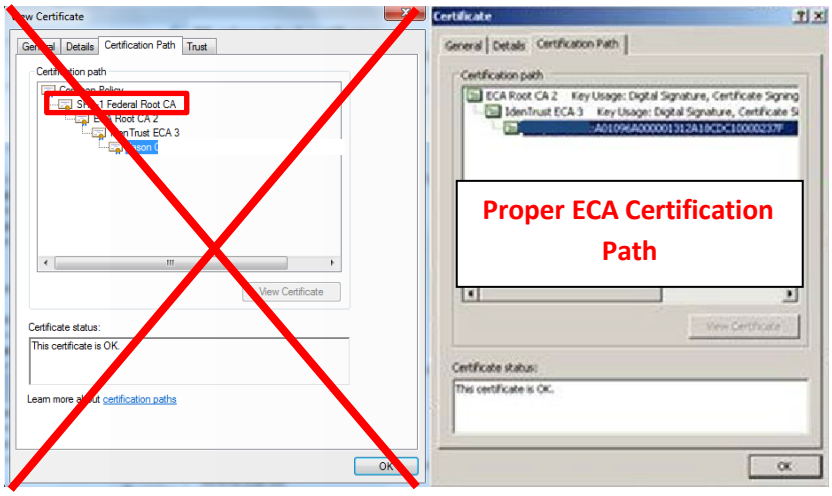


Figure 17 – Incorrect and Correct ECA Certification Path

- If the automated tool above does not work to remove the ECA cross certs, the following are instructions for manual removal of ECA cross certificates from Internet Explorer/Windows Credential Manager
  - Open Internet Explorer → Select Tools → Internet Options → Content Tab → Select the Certificates button → Select the **Intermediate Certification Authorities** Tab
  - Figure 18 shows the ECA Cross Certificate that will need to be removed for proper operation with ECA issued certificates. These certificates are defaulted to be listed in alphabetical order by the "issued to" field
  - Select and remove the certificate issued to "ECA Root CA 2," as issued by the "SHA1 Federal Root CA" which has an expiration of December 2013 or January 2014 (this is now an outdated/expired certificate)
  - Also select and remove the certificate issued to "ECA Root CA 2," as issued by the "DoD Interoperability Root CA" which has an expiration of December 2016

2.2.3. Cross Certificate Re-Population Fixes

- If you maintain an operating system of Windows XP or more current, the Microsoft Root Certificate Program has the potential to automatically install non-DoD approved CAs onto your machine via Windows Updater
- If you are having difficulty keeping the ECA cross certificate out of your Intermediate CA trust store, you can simply import or move the cross certificate to the "Untrusted Certificates" store, as this takes precedence over the other stores/folders.
- See the instructions in Section 2.1.3 for exactly how to do this. The only difference between the DoD CAC instructions and that of the ECA is the specific certificate to be moved. Please see Figure 18 for the exact certificate.

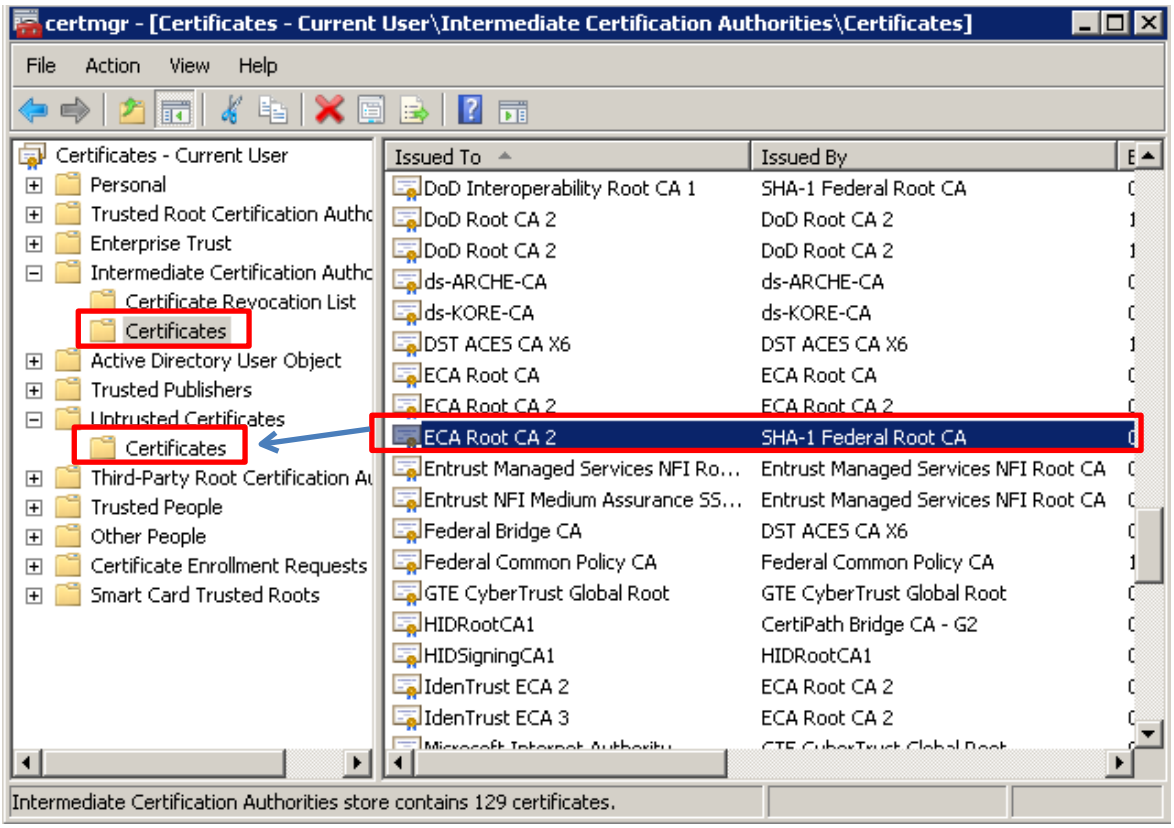


Figure 18 - ECA Cross Certificates for Removal

2.3. Federally issued Personal Identity Verification (PIV)

Federally issued PIVs are considered a "Category I" PKI credential on the DoD Approved External PKI list, and they have been deemed acceptable for use with JPAS/SWFT/DCII.

External PKI holders (which include PIV holders) will have to self-register their certificates once they have completed authentication. Please coordinate with your account manager/organization administrator or the DMDC Contact Center to receive your account username and temporary password that will be used in the registration process. Also note that this registration password is completely separate and distinct from the PIN that you may have self-generated for your smartcard.

2.3.1. Federal PIV Certification Paths

- The way JPAS/SWFT/DCII is configured, all client machines present their own certification paths from their personal certificates up to their Trusted Root certificate (for most Federal Agencies, the Trust Anchor would generally be the Federal Bridge CA or the Federal Common Policy CA) for comparison and verification against the JPAS/SWFT/DCII trust list
    - An Approved Certification Authority (ACA) list, also called a "hint" list is provided to the client for selection of a common Root CA

- JPAS/SWFT/DCII has loaded and do trust all of the Shared Service Providers and approved subordinate CAs throughout the Federal Government (such as Entrust, ORC, State, Treasury, VeriSign, and Verizon Business)
- REGARDLESS OF CREDENTIAL TYPE (CAC, PIV, PIV-I), JPAS/SWFT/DCII DO **NOT** HAVE THE CAPABILITY TO CONSUME **CROSS CERTIFICATES** IN ONE'S CERTIFICATION PATH
    - This presents a difficulty for most Non-DoD Federal JPAS/SWFT/DCII users as they generally use cross certificates at various levels in their certification paths to create a route to the Federal Bridge CA or Common Policy. Additionally, they rarely have permissions at the user level to remove these cross certificates or change client machine settings
    - If at all feasible, please coordinate with system administrators to get a configuration waiver to remove cross certificates in one's Intermediate CA store
- If you are a JPAS, SWFT, or DCII user with a Federal PIV credential and are having difficulty accessing the application even after the general configuration steps, please:
    - Confirm your trusted root CA, see top certificate from examples in Figure 13 & Figure 14
    - Identify all cross certificates in your path; the prototype path validation tool at https://check.dmdc.mil can help you complete this task (see Section 1.8)
    - See the steps outlined in Section 2.1.3 to move the offending cross certs into your Untrusted Certificates store in order to facilitate your computer to present the JPAS/SWFT/DCII loadbalancer with the proper path
- Common Federal cross certificates installed in your intermediate CA trust store that prevent authentication to JPAS/SWFT/DCII are as follows:
    - Entrust Managed Services Root CA issued by the Federal Common Policy CA, which will affect:
        - Department of Justice (DOJ)
        - National Institute for Science and Technology (NIST)
        - Department of Energy (DOE)
    - ORC Root 2 as issued by the Federal Bridge CA, which will affect:
        - Environmental Protection Agency (EPA)
    - Department of State AD Root CA as issued by the Federal Common Policy CA, which will affect:
        - Department of State (DOS)
    - US Treasury Root CA as issued by the Federal Common Policy CA, which will affect:
        - Department of Treasury

- National Aeronautics and Space Administration (NASA)
- Department of Homeland Security (DHS)
- Social Security Administration (SSA)

- If you have removed the above cross certificates and are still having logon issues, please take the actions outlined in Section 5.1 to contact the DMDC Contact Center to assist with configuration

2.3.2. Potential Reasons for Auto-Population of Cross Certificates

- If you maintain an operating system of Windows XP or more recent, the Microsoft Root Certificate Program has the potential to automatically install non-DoD approved CAs onto your machine via Windows Updater
- Please see Section 2.1.3, specifically Figure 16 for instructions on how to access the Windows Credential Manager to move the offending cross certificate you identified in the last step, from your Intermediate CA folder to your Untrusted Certificate store

2.4. "Other" DoD Approved PKI / PIV-Interoperable

"Other" DoD approved PKI / PIV-I are considered a "Category II" PKI credential on the DoD Approved External PKI list, and those that have undergone Joint Interoperability Testing Command (JITC) testing and approval have been deemed acceptable for use with JPAS, DCII, and SWFT.

External PKI holders (which include PIV-I holders) will have to self-register their certificates once they have completed authentication. Please coordinate with your account manager/organization administrator or the DMDC Contact Center to receive your account username and temporary password that will be used in the registration process. Also note that this registration password is completely separate and distinct from the password that you may have generated for your smartcard or token.

2.4.1. PIV-I Certification Paths

- The way JPAS, SWFT, and DCII are configured, all client machines present their own certification paths from their personal certificates up to their Trusted Root certificate for comparison and verification with the DMDC trust store
  - An Approved Certification Authority (ACA) list, also called a "hint" list is provided to the client for selection of a common Root CA (aka trust anchor)
  - JPAS/SWFT/DCII have loaded and do trust all of the DoD approved external Shared Service Providers and approved subordinate CAs
  - REGARDLESS OF CREDENTIAL TYPE (CAC, PIV, PIV-I), JPAS/SWFT/DCII DO **NOT** HAVE THE CAPABILITY TO CONSUME **CROSS CERTIFICATES** IN ONE'S CERTIFICATION PATH
    - This presents a difficulty to many Industry users as they generally have cross certificates at various levels in their certification paths to create a path to a Trust Anchor

- If you are an Industry user with an "other" DoD approved / PIV-I credential and are having difficulty accessing JPAS/SWFT/DCII even after the general configuration steps, please:
  - Confirm your trusted root CA, see top certificate examples from Figure 13 & Figure 14
  - Identify all cross certificates in your certification path; the prototype path validation tool at https://check.dmdc.mil can help you identify this cross certificate (see Section 14.8)
  - See the steps outlined in Section 2.1.3 to move the offending cross certs into your Untrusted Certificates store in order to facilitate your computer to present the JPAS/SWFT/DCII loadbalancer with the proper path
- Common PIV-I/Other DoD Approved PKI cross certificates installed in your intermediate CA trust store that prevent authentication to JPAS/SWFT/DCII are as follows:
  - Boeing PCA G2 as issued by the CertiPath Bridge CA
  - Entrust Managed Services NFI Root CA as issued by the Federal Bridge CA
  - Exostar Federated Identity Service Root CA 1 as issued by the CertiPath Bridge CA
  - Lockheed Martin Root CA as issued by the CertiPath Bridge CA
  - Northrop Grumman Corporation Root CA as issued by the CertiPath Bridge CA
  - ORC Root 2 as issued by the Federal Bridge CA
  - RaytheonRoot as issued by the CertiPath Bridge CA
  - Verisign Class 3 Public Primary Certification Authority – G3 as issued by the Federal Bridge CA, which affects several direct issuers:
    - Booz Allen Hamilton
    - Computer Sciences Corporation
    - ICF International
    - Millennium Challenge Corporation
    - US Senate
  - Verisign Universal Root Certification Authority as issued by the Federal Bridge CA, which also may affect all of the companies listed under the Verisign Class 3 PP CA – G3 above
  - The Verizon Business NFI root which is called "CT-CSSP-CA-A1" as issued by the Federal Bridge CA

- If you have removed the above cross certificates and are still having logon issues, please take the actions outlined in Section 5.1 to contact the DMDC Contact Center team to assist with configuration

- We have conducted testing with several large and small businesses and Figure 19 shows a valid certification path that was confirmed to work for

JPAS/SWFT/DCII access for a CertiPath Bridge member (Raytheon in this case)

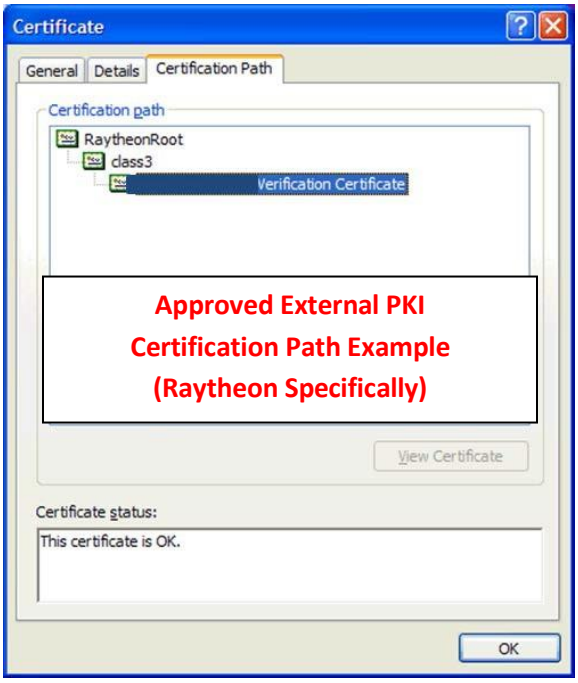


Figure 19 – Valid external PKI Certification Path

2.4.2. Potential Reasons for Auto-Population of Cross Certificates

- If you maintain an operating system of Windows XP or more recent, the Microsoft Root Certificate Program has the potential to automatically install non-DoD approved CAs onto your machine via Windows Updater
- Please see Section 2.1.3, specifically Figure 16 for instructions on how to access the Windows Credential Manager to move the offending cross certificate you identified in the last step, from your Intermediate CA folder to your Untrusted Certificate store

3. Common Logon Errors and Potential Resolution:

3.1. X.509 Certificate Cannot be Found

- Please ensure your hardware PKI token or smartcard is in the card reader or USB port
- Also, please ensure that you have followed all of the PKI provider's directions for installing the certificate and middleware onto your machine
- Occasionally, closing and re-opening your browser has been known to resolve the issue
- In addition, a temporary work-around has been developed regarding this specific error message:
    i. Select Tools → Internet Options → Content Tab → Select the "Clear SSL State" toggle button. See Figure 2 above.
    ii. After this, you should close the Options window and all IE browsers; re-open IE and logon to JPAS/SWFT/DCII as normal
- Ensure that you are properly logged onto your middleware, which is generally provided by your PKI vendor

3.2. X.509 Certificate Cannot be Read – Java.Null.Pointer.Exception

- Occasionally, closing and re-opening **ALL** of your browser windows (not just your JPAS/SWFT/DCII window) has been known to resolve the issue
- In addition, a temporary work around has been developed regarding this specific error message:
    i. Select Tools → Internet Options → Content Tab → Select the "Clear SSL State" toggle button
    ii. After this you should close the option windows and all IE browsers; re-open IE and logon to JPAS/SWFT/DCII as normal
- If neither option works, you most likely have a cross certificate error. If you are a DoD/ECA user see Section 2.1.2, if you are a Federal PIV or "other" DoD approved credential user see Section 6.1

3.3. X.509 Certificate is not DoD Approved

- See Section 1.6 for this error
- DoD has a specific approval process for use of PKI in their IT systems. This testing is conducted by Joint Interoperability Testing Command (JITC) and a list of approved external PKI providers are available at the following site:
    i. http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx
    ii. Please consider this approved PKI list when investing in credential providers
- You can find these certificate policy object identifiers (OIDs) through the internet options selection from your browser:
    i. Select Internet Tools → Content → Certificates → Personal Tab → double click your intermediate CA → select the details tab → select "Certificate Policies"
    ii. Figure 8 is a screen shot of the policy identifiers you will see for a VeriSign certificate issued through the ECA Root CA 2, note the ECA-medium-

hardware identifier, this denotes that the intermediate CA is able to issue medium hardware certificates

3.4. SSL Handshake Error

- This is generally indicative of a cross certificate error as seen in Firefox, please see Sections 1.4.3 and the relevant cross certificate section for your PKI provider

3.5. Inability to view PSQ or Signature Pages

- Ensure the "Do not save encrypted pages to disk" option is not checked
  - In Internet Explorer go to Tools → Internet Options → Advanced tab → scroll to bottom → ensure "Do not save encrypted pages to disk" option is not checked → apply changes (see Figure 3)
- If you are an Internet Explorer user, you can attempt enabling the "InPrivate," browsing option under the Safety menu option.

3.6. Internet Explorer Cannot Display Webpage

- This is a ubiquitous error message that is indicative of a cross certificate error for IE users, please see sections 2.1.2, 2.2.2, 2.3.1, or 2.4.1 for instructions/guidance on the resolution
- This could also be indicative of a middleware/browser communication issue. In order to properly read your PKI card/token both the middleware and browser need to communicate on the same standard be it 32-bit or 64-bit. IE8 and 9 users can simply test another version by selecting it from the start menu. IE10 users will have to force their browsers to use 64 bit mode by going to Tools → Internet Options → Content Tab → Advanced tab, scroll toward the bottom, and under the "Security" heading you will find an options that says "Enable Enhanced Protection Mode" toggle that option, apply changes, and restart your computer to test JPAS/SWFT/DCII access in 64-bit mode.

4. Self-Registration:

Each web application/database needs to correlate your PKI credential to the account that was created in the system. SWFT, DCII and JPAS do this through a self-registration process where, after authenticating with a credential, the user provides both a User Name/Login ID and a Temporary password which they can receive from the DMDC Contact Center or their respective Account Manager/Administrator. This links the unique identifier on a PKI credential to an individual account, and as a result you will only need your PKI credential for subsequent logons. It is worth noting that this self-registration process will be required when a new credential is issued, for example, after a current credential expires.

CAC Holders Note: CAC Holders who have **activated the PIV Authentication certificate** on their CAC will be required to register their certificates in the same manner with ECA certificates for JPAS/SWFT/DCII.

JPAS Note: CAC holders utilizing their credential for access to JPAS will not be prompted to register their certificates with username/password at the self-registration screen. JPAS and DEERS have an interface in which the DoD Unique Identifier (Called an EDIPI, or DoD ID) is used to directly associate a user's digital identity to their established account. In order for the unique identifier to be transferred to JPAS, 3 fields of personally identifiable information (PII) in both repositories need to match: a user's full name, SSN and Date of Birth.

- If it is a new issue CAC (i.e. if it is the recipient's first CAC ever), the user must wait for the data synchronization to occur which takes place once a month on the day of the recipient's birth. For example if the recipient was born on the 5th of any given month, they can attempt to access JPAS on the 6th after issuance has occurred. If the user's birthday is before the CAC issuance date (i.e. the birthday is the 5th and the CAC was issued on the 15th), then they will have to wait until the 6th of the next month for the synchronization to take place.
- If the CAC was issued 60 days ago, or longer, and a user still cannot access their previously authorized JPAS account, there might be a PII mismatch between DEERS and JPAS preventing the synchronization from occurring. If this is the case, please submit your full name, date of birth, and JPAS user ID to dmdc.contactcenter@mail.mil. Please digitally sign that message with your CAC so we can reference your information in DEERS.

SWFT Note: CAC holders utilizing their credential for access to SWFT will not need to re-register their smart card on their first use after receiving a new card. All other users should go to the User Settings page in the SWFT application prior to the expiration of their current certificate. Passwords are valid for 72 hours and will only be needed on the first login with your new credential. SWFT users will need to ensure that the common name on the PKI credential matches the name on the account in order to allow access. For instance, if the name on the credential is John ODoe, and the account has the name John O'Doe, it will have to be changed to match the PKI credential.

Figure 20 - SWFT Self-Registration Screen

Figure 21 - SWFT Password Reset Screen

DCII Note: DCII requires registration in a very similar manner to SWFT. Temporary passwords for DCII users can be generated either by the DMDC Contact Center or Agency Administrators. CACs will not require additional registration if they have been reissued, but Federal PIVs are generated with new unique identifiers each time they are issued, so they will require registration upon reissuance.

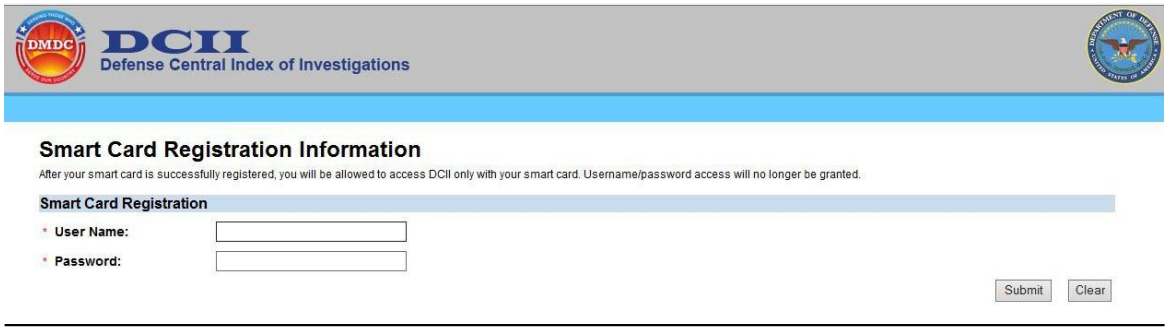


Figure 22 - DCII Smartcard Registration Screen

5. Other Possible Reasons for PKI Logon Issues:

- Smartcard or USB token is defective or requires a security upgrade
  - Work with your vendor to ensure the smartcard or USB token is properly functioning
  - You will need to call your PKI vendor to discuss
- User has not "logged onto" their middleware; some PKI translation software packages provide by vendors require logon prior to use of a Token/smartcard for PKI authentication (known examples include SafeNet Utility provided by IdenTrust)
- Computer or Network configurations are conflicting with proper operation of SSL/TLS session encryption
  - Contact your IT or Desktop Support team as some software (encryption, VPN, firewall, etc.) settings may need to be modified to ensure proper smartcard/USB token functioning, or valid certificate passage (i.e. proxy servers are turned off)
  - You can see if you are connected through a proxy server in IE by going to Tools → Internet Options → Connections Tab → LAN Settings button
    - If your LAN Settings window shows that you are using a proxy server with checkmark towards the bottom of the window, then the proxy might be interfering with the establishment of a TLS/SSL session
    - You can also check to ensure that the JPAS server certificate was issued by a DoD CA by going to the disclosure screen and viewing the security certificate. If it was issued by anything other than a DoD CA, you probably have a proxy present.
- Middleware/Browser communications issue
  - Test both 32- and 64-bit versions of your browser
  - IE8 & 9 users should be able to see both versions in the start menu under all programs
  - IE10 and IE 11 users will have to enable enhanced protection mode to switch from the default 32-bit mode to the 64-bit mode

6 If all else fails

6.1 Submit your case to the DMDC Contact Center

If you have exhausted all possibilities in this guide, please collect the following information and coordinate with the DMDC Contact Center at either (800) 467-5526 during normal operating hours (Monday-Friday; 8 AM – 8 PM ET) or via email at DMDC.ContactCenter@mail.mil:

- Your First and Last Name
- A detailed description of what you have tried using the techniques above and the errors (if any) for each technique
- Operating system and web browser(s) that are being used
- Type of certificate you are using (and its form factor: smartcard or USB token)
- The digital certificate export (see Section 6.1.1 for more information)
- A screen shot of your certification path (see Figure 14 as an example)
- A screen shot of the server SSL certification path from the JPAS/SWFT/DCII disclosure site (see Figure 7 as an example)

*Please see Appendix B for an example of the form that the Contact Center uses to troubleshoot PKI issues and the types of information they collect.

6.1.1 How to export a digital certificate from Internet Explorer:

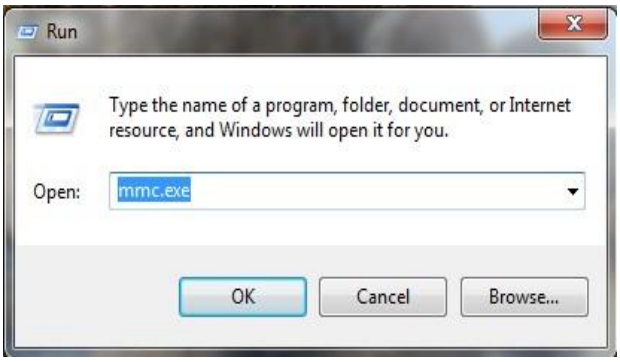
- From the Menu bar, select **Tools** > **Internet Options**
- The Internet Options dialog box appears
- Click the **Content** tab
- Click the **Certificates** button
- The Certificates dialog box appears
- Ensure the **Personal** tab is selected (this should be the default tab)
    - The tab lists your certificates and lets you choose a certificate for export
- Select the certificate to export (generally the **Identity Certificate** is preferable)
- Click the **Export** button (see Figure 13)
- The Certificate Export Wizard appears
- Select the "**No, do not export the private key**" button
- Select the "Base-64 encoded X.509 (.CER)"
- In the File name field, enter the path and filename to which you want to export the certificate
- After completing the wizard, locate the exported file and append **.txt** (i.e.: mycertificate.cer.txt) to the end of the filename
- Changing the file extension to txt allows you to e-mail the certificate without it being blocked by most government e-mail filters

Appendix A – Advanced Trust Store Management

Some users might go through this entire troubleshooting guide and find that they are still not expressing the proper certification path that the JPAS/SWFT/DCII loadbalancer is able to validate.

As the local system's trust store might be taking precedence over the user's trust store, additional configuration steps using the Windows Mass Management Console (MMC) might be required to correct the certification path. The following steps will take you through the process to manipulate the local console trust store provided a user is logged onto their system with administrator level privileges. These steps should ONLY be performed after a user has attempted the proper configuration steps from Chapter 2 and they are still unable to access JPAS/SWFTDCII. It is also recommended that any available IT specialists assist with advanced trust store management.

- Open the run option and type "mmc.exe" in the command line, and the management console will open Figure 23



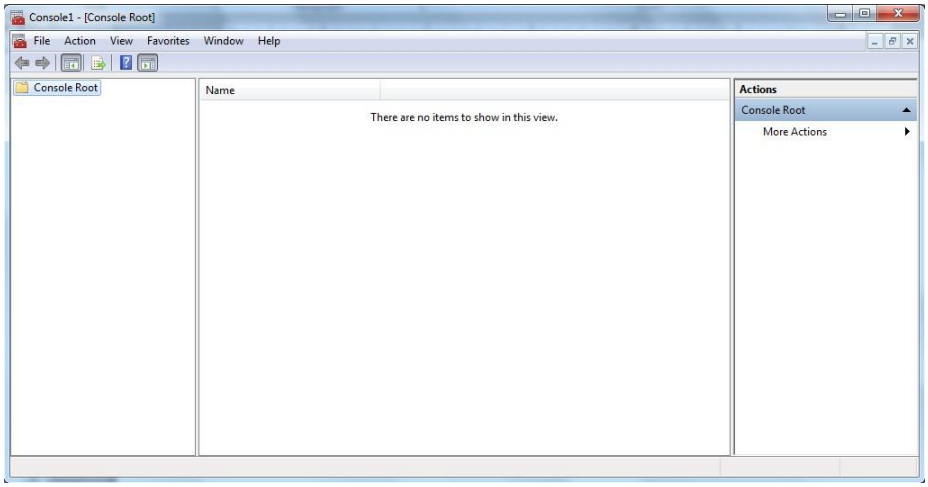


Figure 23 - Windows Mass Management Console

- Once in the management console, select the 'File' menu and then select the "add/remove snap-in" option Figure 24.

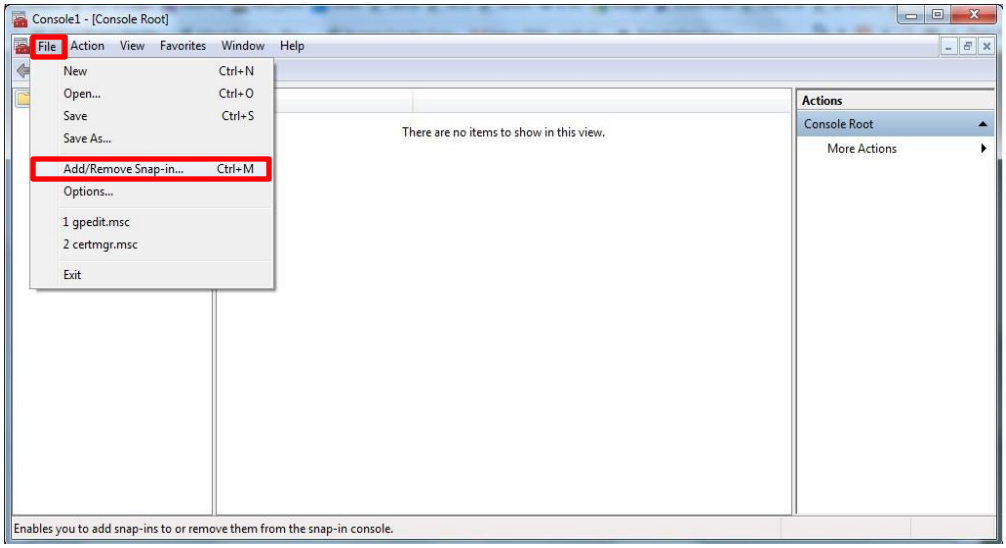


Figure 24 - MMC File Options

- In the 'add/remove snap-in' dialogue box, select the 'Certificates' snap in and then select 'add' Figure 25

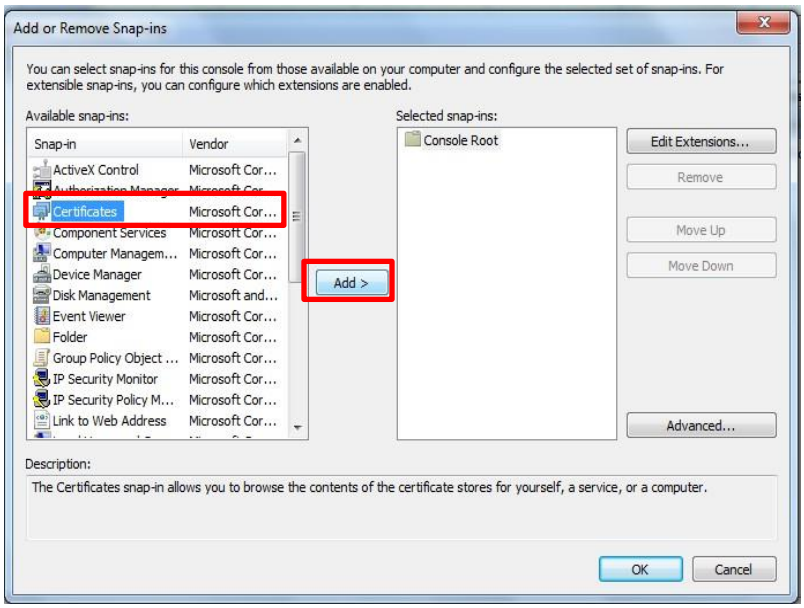


Figure 25 - MMC Certificate Snap-in

- If logged in as an administrator, you will then be prompted to select the account and the computer of the trust store you want to manipulate. Select 'computer account' and then 'local computer' respectively Figure 26

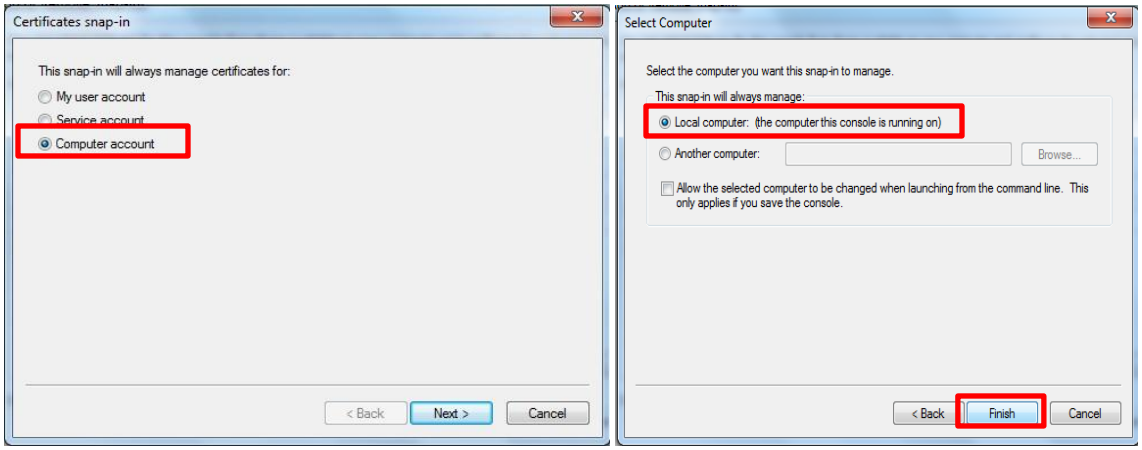


Figure 26 - Snap-in Selection

- **Once** this is complete you will be provided an interface that is very similar to the Windows credential manager as described in Chapter 2 (Figure 16) Figure 27

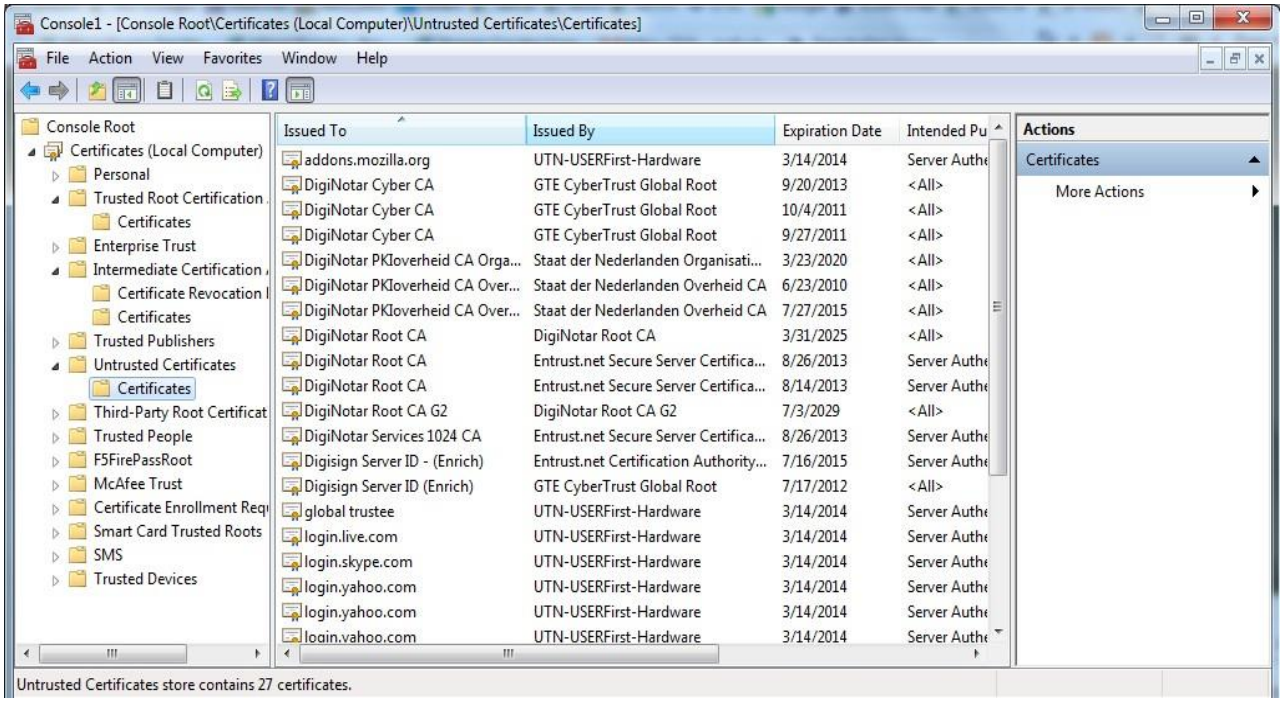


Figure 27 - Local Computer Certificate Manager

- You will need to ensure those certificates that should be in your certification path are not in the untrusted folder of your local computer trust store, you may also need to ensure that your self-signed trusted roots are installed in the Trusted Root CA folder here in order to take effect in your user profile trust store
    - To do this you will have to download the certificate packages from the following URL:
        - http://iase.disa.mil/pki-pke/Pages/tools.aspx
            - Trust Store tab
            - PKI CA Certificate Bundles: PKCS #7
            - For DoD PKI Only – Version x (ZIP Download)
                - Certificates_PKCS7_vX.XXX_DoD.der.p7b
            - For ECA PKI Only – Version x (ZIP Download)
                - Cerificates_PKCS7_vX.XXX_ECA.der.p7b

    - Then right click the "Certificates" sub-folder under "Trusted Root Certification Authorities," hover over "All Tasks", select "Import"
    - The certificate import wizard will then guide you through the installation of the cert packages you downloaded above
- Once the self-signed roots are confirmed to be in the Trusted Root Certification Authorities folder in both the local and user profile stores, cross certificates in the intermediate certification authority stores need to be untrusted. Please see sections 2.1.2, 2.2.2, 2.3.1, or 2.4.1 for lists of credential specific cross certificates.

Appendix B – DMDC Contact Center PKI Escalation Report

Tier 1: Basic System Configuration

x509 error with a DoD CAC verify that the user is selecting the PIV certificate

Step 1: System time, PKI form Factor

☐Verify system time is correct (hover over time in taskbar and ensure correct date and time) use the following http://nist.time.gov to check Date and Time

☐Verify with the user that their PKI is on a Smartcard or USB token and reader/token light is active

Step 2: Operating System

☐Verify Operating System type:

Windows	MAC
☐XP, Vista, 7	☐**(Tier II)**
☐8	
☐10	

Step 3: Internet Browser

☐Verify Web Browser **being used:**

☐Internet Explorer 8 or 9
☐Internet Explorer 10 or 11
☐Chrome
☐FireFox/WaterFox **(Tier II)**
☐Safari **(Tier II)**

Note: Windows 10 users must use IE 11 not Microsoft Edge

To find IE 11 in Windows 10; type in search bar "internet explorer" and right click on IE icon blue E with a gold halo and pin to task bar.

Note: IE11 needs "osd.mil" to be added to compatibility view (**IE Tools→ Compatibility View settings**)

Step 4: Internet Options Settings: (IE Tools→ Internet Options)

Step 4a: Delete Browsing History

☐**General Tab→ Delete Button→ Delete Browsing history: Select all (except Preserve Favorites website data, Form Data and Passwords) (History cannot be selected on a government computer)**

Step 4b: Verify Trusted Sites

☐**Security Tab→ Trusted site→ Sites** https://*.dmdc.osd.mil is added

Step 4b: Third Party Cookies Accepted

☐**Privacy Tab** → Advanced button: Verify cookies are accepted

Step 4c: Clearing SSL State

☐**Content Tab → Clear SSL State**

Step 4d: PKI Provider Identification and Cross Certificates

☐**Content Tab→** Certificates; double click personal certificate,

'General' tab see "Issued by" field; Select corresponding provider:

Public PKI Provider*	Organizationally Issued PKI*
☐IdenTrust ECA	☐DoD CAC
☐ORC ECA	☐Federal PIV
☐Symantec ECA (formerly Verisign)	☐A&D Corporate Badge*
☐Exostar (SHA256 only)	☐Other (BAH, CSC, EID, etc.)
☐Entrust	*(Boeing, Northrop Grumman, Lockheed Martin, etc.)
☐Verizon Business	
☐ORC NFI	

'Certification Path' tab are there more than 3 or 4 certificates in the path?

☐Yes (will do Step 7, if Exostar is provider, **escalate to Tier II**) ☐No

Step 4e: Browser Encryption Standards **SSLs & TLSs**

Advanced Tab (toward bottom of the Settings box)

Checked	Unchecked
☐TLS 1.0	☐Do not save encrypted pages to disk
☐TLS 1.1	☐SSL 2.0
☐TLS 1.2	☐SSL 3.0

Step 5: Identify any installed Middleware

- ☐ SafeNet (normally issued by IdenTrust)
- ☐ eToken (normally issued by Symantec/Verisign)
- ☐ ActivClient (normally issued by ORC and is installed on most DoD workstations)
- ☐ NO MIDDLEWARE INSTALLED, but has a DoD CAC or Federal PIV with a Windows 7 or 8 OS

Step 6: Test https://check.dmdc.mil with both 32-bit and 64-bit versions of IE*, what is the result?

- ☐ Internet Explorer cannot display the webpage (with PIN Prompt)*
- ☐ Internet Explorer cannot display the webpage (without PIN Prompt)*
- ☐ There seems to be an issue with the path (go to Step 6)
- ☐ The path seems fine (table with all green checks, test in JPAS application)

*IE8 & 9 users will be able to switch between versions via the Start Menu → All Programs
*IE10 & IE 11 defaults to 32-bit mode, if not working have them test in 64 by going to Tools → Internet Options → Advanced tab → Select "Enable Enhanced Protected Mode" under security → restart system and retest

Step 7: Run the DISA Federal Bridge Cross Certificate Remover and have them retest Step 5:
http://iase.disa.mil/pki-pke/Pages/tools.aspx Certificate Validation tab: FBCA Cross-Certificate Remover (the version changes so a direct link will break)

Step 8: Does issues with the path still remain?

☐ Yes (escalate to Tier II) ☐ No, have them attempt to logon to JPAS

Tier II: Trust Store, Network and Driver Troubleshooting

Provided the steps completed from Tier I, it is assumed that escalating the issue to Tier II means that they have narrowed the issue down to a Certification Path/Trust Store issue, a network (proxy server) issue, or another hardware specific issue.

Step 1a: Verify no proxy servers are enabled on customer network. Have user go to the application's DoD Notice and Consent Banner screen (the 'I Agree" page), in the URL bar, generally just to the right they will see a profile of a padlock, have them click the padlock, and then select the "view certificate" option. In the new window does the "Issued by:" fields reflect **DoD ID SW CA-37**?

- ☐ Yes (no proxy server present)
- ☐ No (have user work with their network team to disable, or have them test on open network)

Step 1b: While the server certificate window is open have them check the "Certification Path" tab, does the path only have 3 certificates in the path ending at the top at **DoD Root CA 3**?

- ☐ Yes (DoD certificates are properly installed)
- ☐ No (go to Step 2)

Step 2: Have the user download and install both the DoD Root 3 and ECA Root 4 certificate packages from the following link:
http://iase.disa.mil/pki-pke/Pages/tools.aspx

- Trust Store tab
- PKI CA Certificate Bundles: PKCS #7
- For DoD PKI Only – Version x (ZIP Download)
  - Certificates_PKCS7_vX.XXX_DoD.der.p7b
- For ECA PKI Only – Version x (ZIP Download)
  - Cerificates_PKCS7_vX.XXX_ECA.der.p7b

Then have the user, re-run the Cross Cert removal tool: http://iase.disa.mil/pki-pke/Pages/tools.html Certificate Validation tab: FBCA Cross-Certificate Remover (the version changes so the link will break)
Have the user recheck their certification path on the personal certificate (Tools → Options → Content tab → Certificates → double click their cert → Certification Path tab)…. Is his or her path now streamlined?

- ☐ Yes (Have them test logging onto JPAS)
- ☐ No (try to identify the cross certificate in the path from the PKI tech guide, go to Step 3)

Step 3: Open the windows credential manager (certmgr.msc in windows run command), have the user expand the Intermediate Certification Authorities and Untrusted Certificates folders on the left. Have the user select the certificate sub-folder under intermediate CAs. Look through the list on the right and have the user drag and drop any cross certs identified in section 2.3.1 or 2.4.1 in the technical guide into the certificate sub-folder under Untrusted Certificates. Also move the following certs if present:

Issued to:	Issued by	Expiration
DoD Root CA 2	DoD Interoperability Root CA 2	December 2016
ECA Root CA 2	DoD Interoperability Root CA 1	December 2016

Have them recheck their certification path. Is the path now streamlined?

- ☐ Yes (have them test JPAS)
- ☐ No (Escalate to Government Rep)

Step 4: If working with Windows 7/8/10 and the user has a Federal PIV or a DoD CAC, you should test with the middleware uninstalled. Additionally, you might have to have the OS reinstall the hardware drivers for the reader and the smartcard itself by uninstalling via device manager.