Cross Certificate Chaining Problem – CAC Users

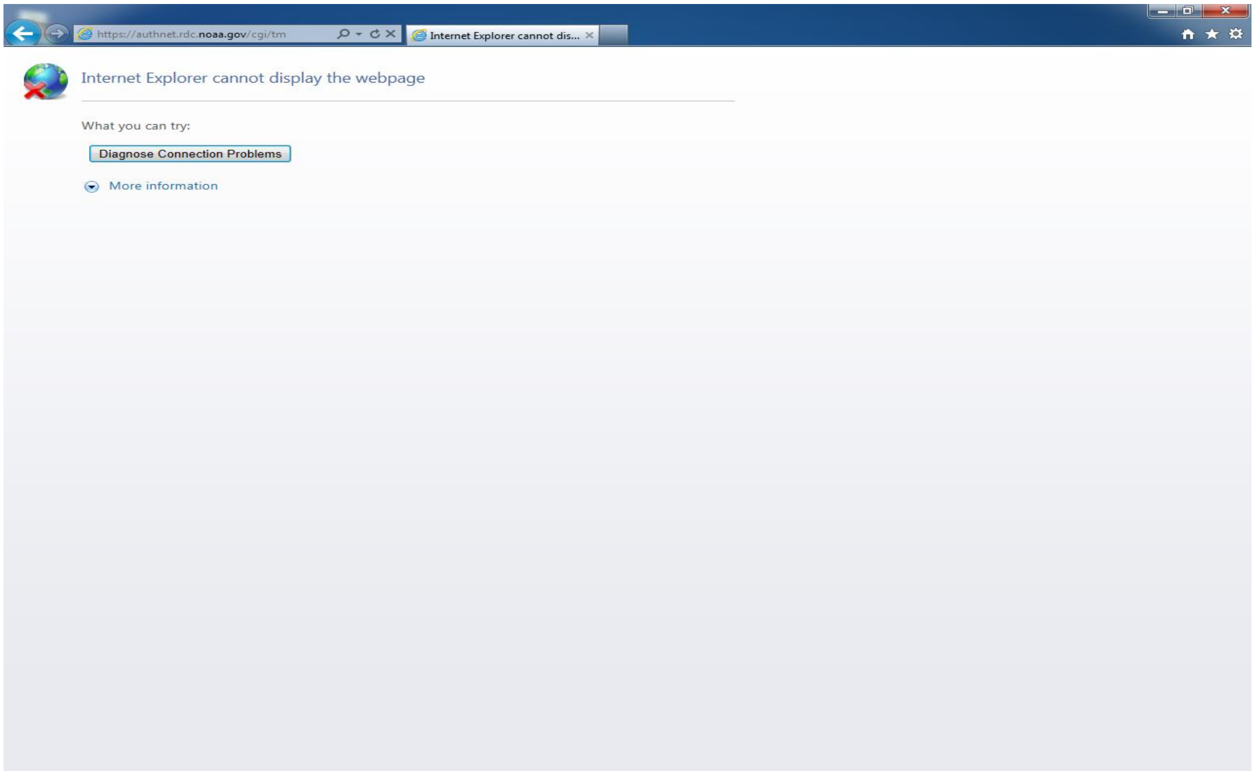
NOAA users employ CAC cards (issued by DOD) to access sites requiring Two Factor Authentication (2FA). Occasionally, Microsoft Windows Operating System (WinTel) users cannot connect to sites requiring 2FA. The underlying reason is that the DoD certificates (required for CAC card validation) are chaining improperly to cross-certificates or the Common Policy Root Certification Authority (CA).

When this occurs on NOAA (or any DoD CAC card) systems, PKI validation does not work properly and may result in any of the following:

a) NOAA Wintel user denied access to CAC enabled web sites; or

b) Users receive a prompt to install the Common Policy Root CA when opening a signed email of a DoD sender whose workstation is misconfigured.

Example: “*Internet Explorer cannot display the web page*”



https://authnet.rdc.noaa.gov/cgi/tm
Internet Explorer cannot dis...

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems
More information

See the DOD Root Certificate Chaining Problem document listed below for specifics.

https://militarycac.com/files/DoD_Root_Certificate_Chaining_Problem_v1.0_15Mar2010.pdf

To correct the Cross Certificate Chaining problem, download and run (administrator privileges required):

FBCA Cross-Certificate Remover 1.12

This tool removes certificates which cause the cross-certificate chaining issue for NOAA (and optionally DoD enabled) users from Microsoft Local Computer and User Certificate stores. The following Microsoft Operating Systems are supported: Windows XP, Windows Vista, **Windows 7**, **Windows 8, and Windows 8.1**. (ZIP Download) Size: 37 KB

To download the FBCA Cross-Certificate Remover 1.12, connect to:

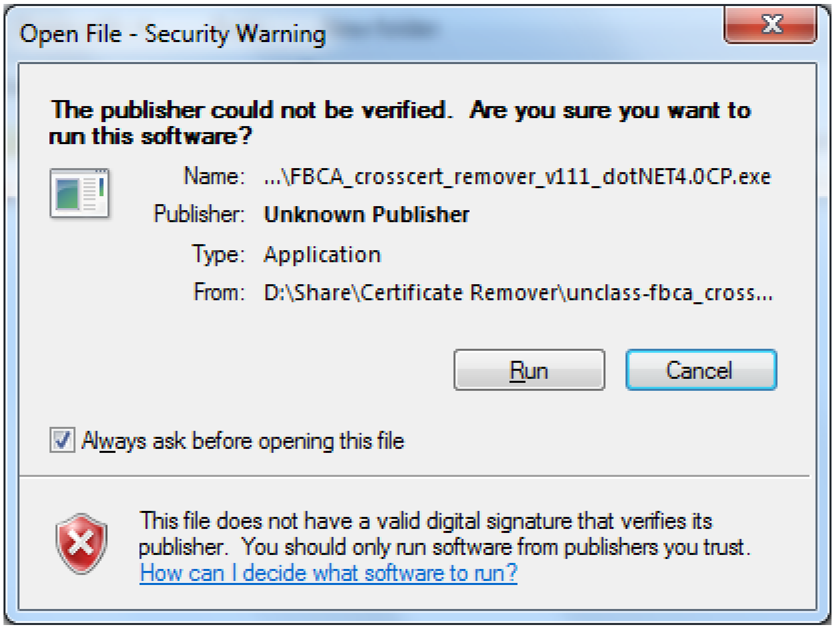
http://iase.disa.mil/pki-pke/Pages/tools.aspx

Click the Certificate Validation Tab, scroll to last two items on page.

FBCA Cross-Certificate Remover 1.12

FBCA Cross-Certificate Remover 1.12 User Guide

Example:



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...\FBCA_crosscert_remover_v111_dotNET4.0CP.exe

Publisher: **Unknown Publisher**

Type: Application

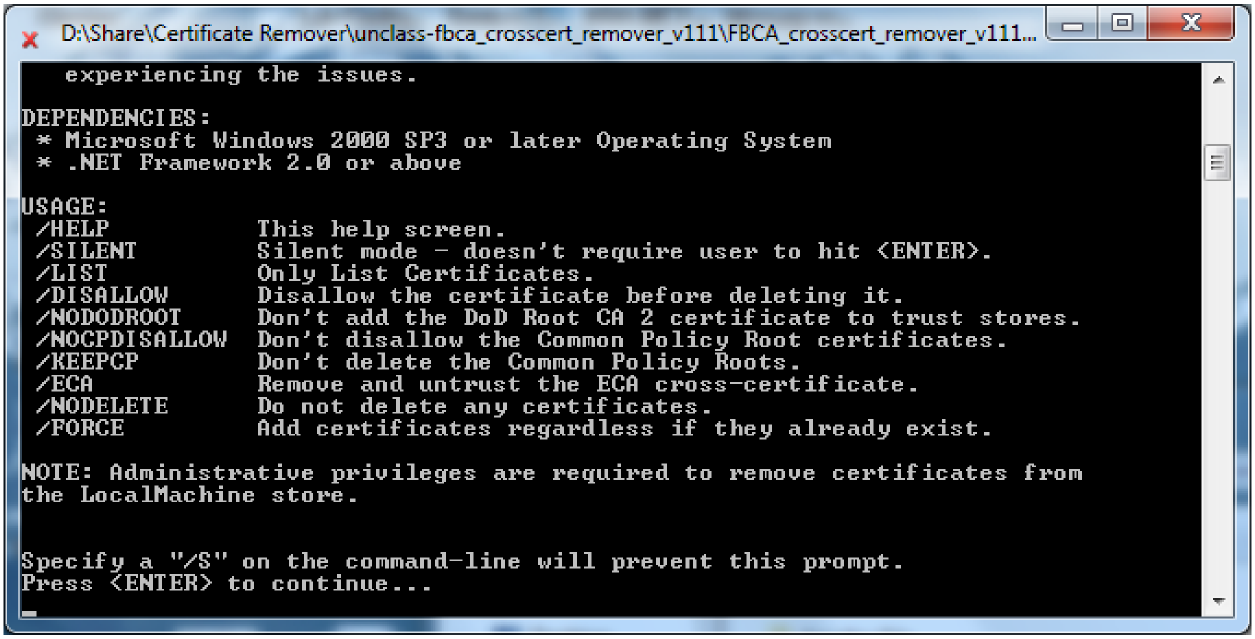
From: D:\Share\Certificate Remover\unclass-fbca_cross...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

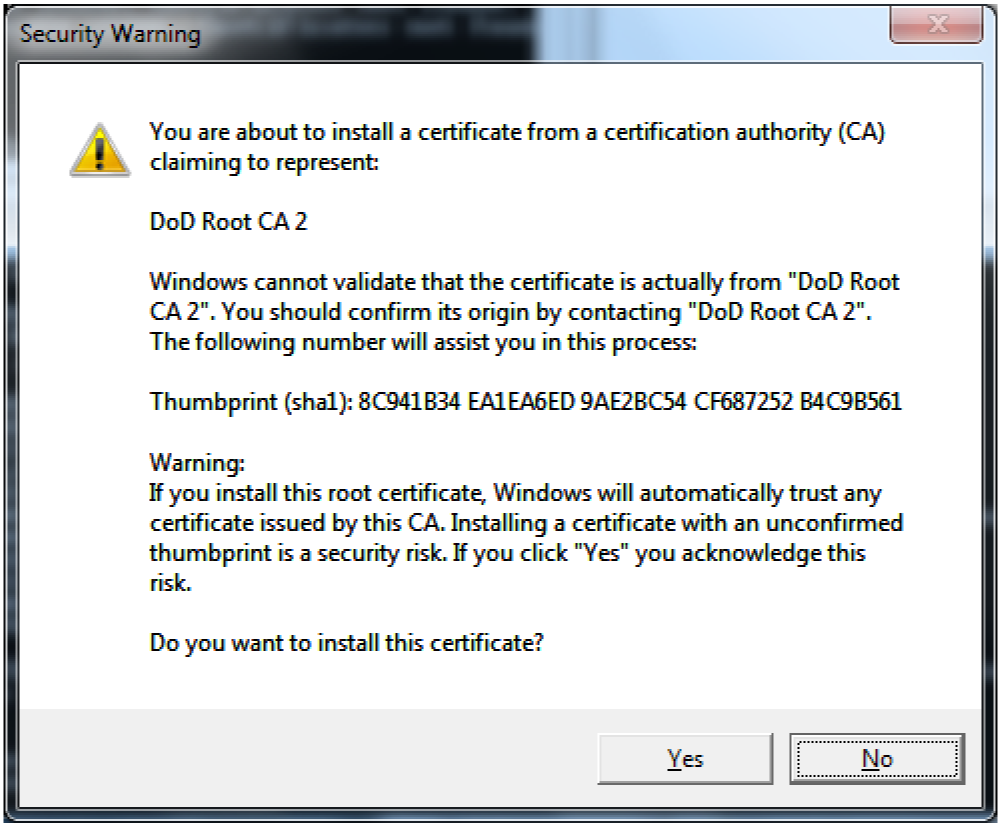
Click Run.

Note: Administrator privileges are required to run this tool.


D:\Share\Certificate Remover\unclass-fbca_crosscert_remover_v111\FBCA_crosscert_remover_v111...

```
   experiencing the issues.

DEPENDENCIES:
 * Microsoft Windows 2000 SP3 or later Operating System
 * .NET Framework 2.0 or above

USAGE:
 /HELP          This help screen.
 /SILENT        Silent mode - doesn't require user to hit <ENTER>.
 /LIST          Only List Certificates.
 /DISALLOW      Disallow the certificate before deleting it.
 /NODODROOT     Don't add the DoD Root CA 2 certificate to trust stores.
 /NOCPDISALLOW  Don't disallow the Common Policy Root certificates.
 /KEEPCP        Don't delete the Common Policy Roots.
 /ECA           Remove and untrust the ECA cross-certificate.
 /NODELETE      Do not delete any certificates.
 /FORCE         Add certificates regardless if they already exist.

NOTE: Administrative privileges are required to remove certificates from
the LocalMachine store.


Specify a "/S" on the command-line will prevent this prompt.
Press <ENTER> to continue...
_
```

Press Enter.



You are about to install a certificate from a certification authority (CA) claiming to represent:

DoD Root CA 2

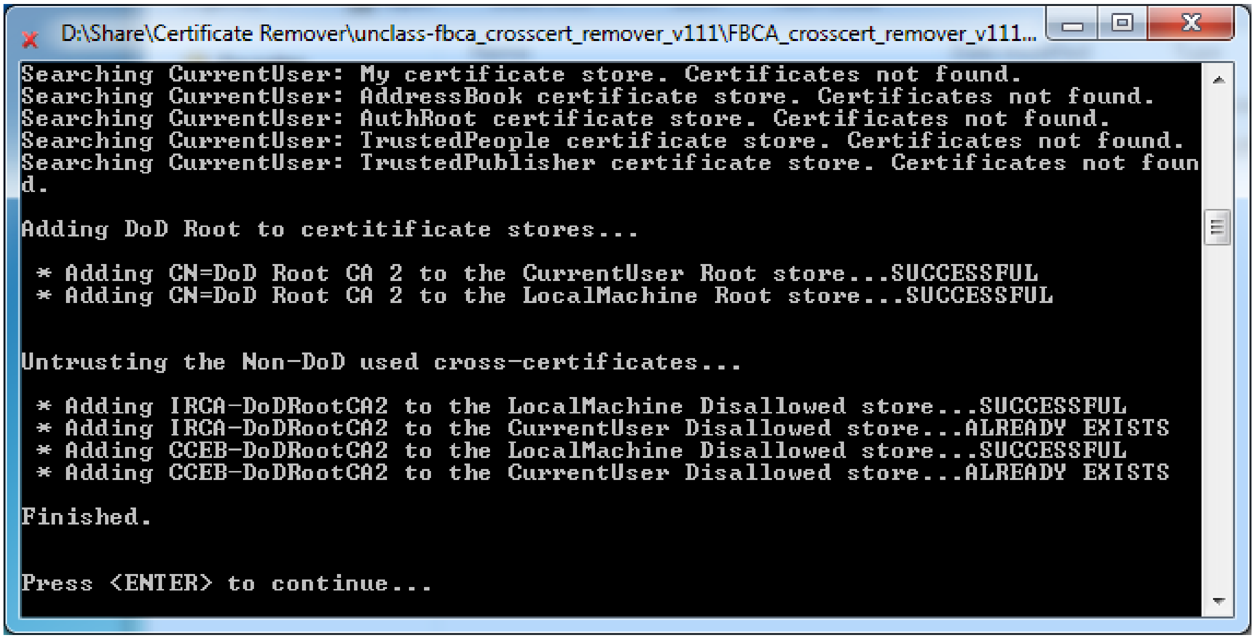
Windows cannot validate that the certificate is actually from "DoD Root CA 2". You should confirm its origin by contacting "DoD Root CA 2". The following number will assist you in this process:

Thumbprint (sha1): 8C941B34 EA1EA6ED 9AE2BC54 CF687252 B4C9B561

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Click Yes.


D:\Share\Certificate Remover\unclass-fbca_crosscert_remover_v111\FBCA_crosscert_remover_v111...

```
Searching CurrentUser: My certificate store. Certificates not found.
Searching CurrentUser: AddressBook certificate store. Certificates not found.
Searching CurrentUser: AuthRoot certificate store. Certificates not found.
Searching CurrentUser: TrustedPeople certificate store. Certificates not found.
Searching CurrentUser: TrustedPublisher certificate store. Certificates not foun
d.

Adding DoD Root to certitificate stores...

 * Adding CN=DoD Root CA 2 to the CurrentUser Root store...SUCCESSFUL
 * Adding CN=DoD Root CA 2 to the LocalMachine Root store...SUCCESSFUL


Untrusting the Non-DoD used cross-certificates...

 * Adding IRCA-DoDRootCA2 to the LocalMachine Disallowed store...SUCCESSFUL
 * Adding IRCA-DoDRootCA2 to the CurrentUser Disallowed store...ALREADY EXISTS
 * Adding CCEB-DoDRootCA2 to the LocalMachine Disallowed store...SUCCESSFUL
 * Adding CCEB-DoDRootCA2 to the CurrentUser Disallowed store...ALREADY EXISTS

Finished.


Press <ENTER> to continue...
```

Press Enter.

Screen closes.

Close all open browser connections.

Retry connecting to the ITC test website. https://itcip.rdc.noaa.gov