

## Removing the Federal Bridge cross certification certificates.

These instructions are intended to help you remove the Federal Bridge certificates from the Microsoft Certificate store on your computer. The objective of the Federal Bridge is to 'cross certify' the different certificate policies of all the federal agencies. The Federal Bridge has succeeded in getting Microsoft to include the Federal Bridge certificates in the Microsoft Certificate Store through initial operating system installation (it comes from the factory that way) and/or software updates.

Unfortunately, cross certification does not always work well in implementation. If you are trying to connect to a server (for instance, JPAS) and the server is not configured to account for the efforts of the Federal Bridge (perhaps because it is an old server), then it could cause an SSL Transaction (certificate log-on) to fail.

The DoD has produced a tool to remove these certificates. These instructions are written to show you how to use this tool. As an alternative, if you have problems running this tool, you can remove the FBCA Certificates manually by following the instructions found here:

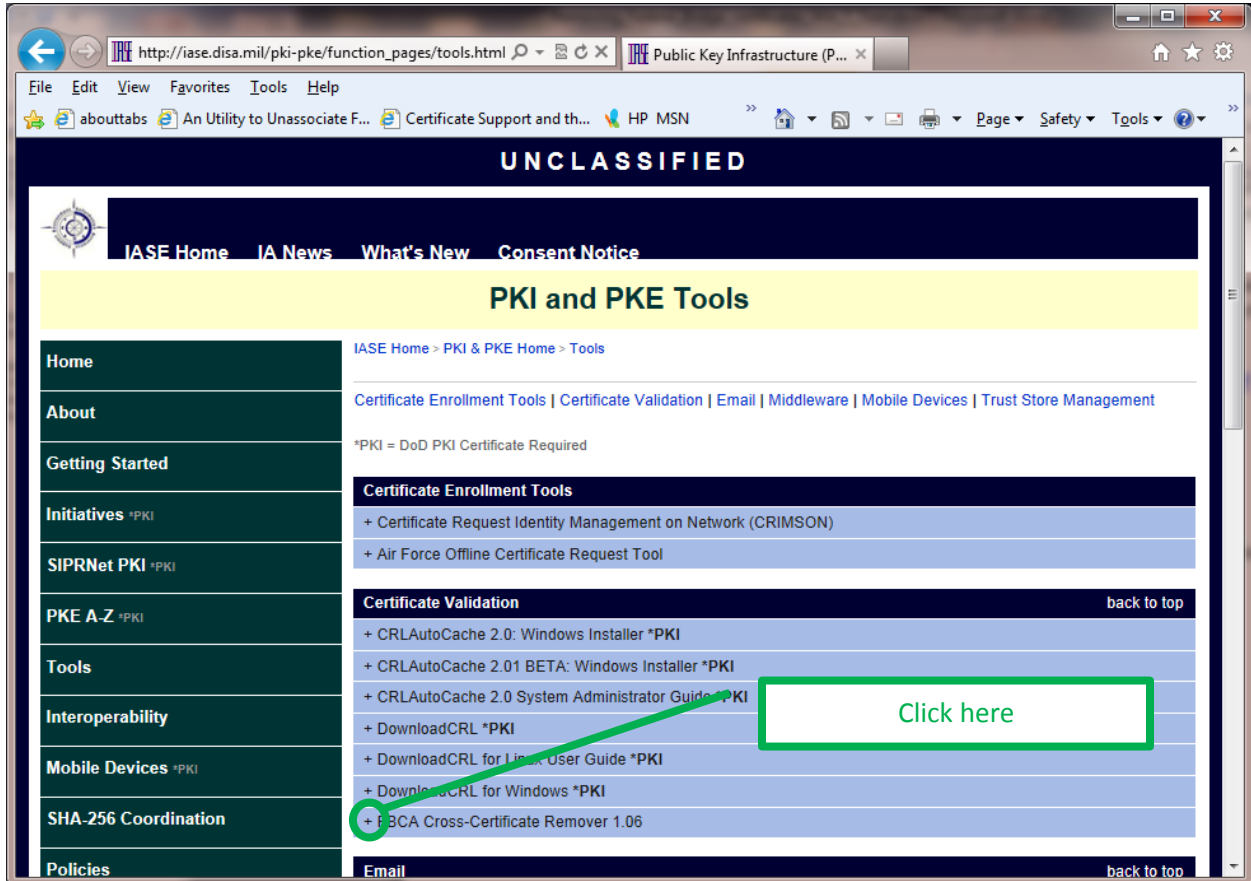
[http://eca.orc.com/wp-content/uploads/ECA\\_Docs/Removing\\_Federal\\_Bridge\\_certificates.pdf](http://eca.orc.com/wp-content/uploads/ECA_Docs/Removing_Federal_Bridge_certificates.pdf)

You will need to run the tool twice: once under your user profile and once as the Administrator. *Please see your local IT support if you are not an Administrator.*

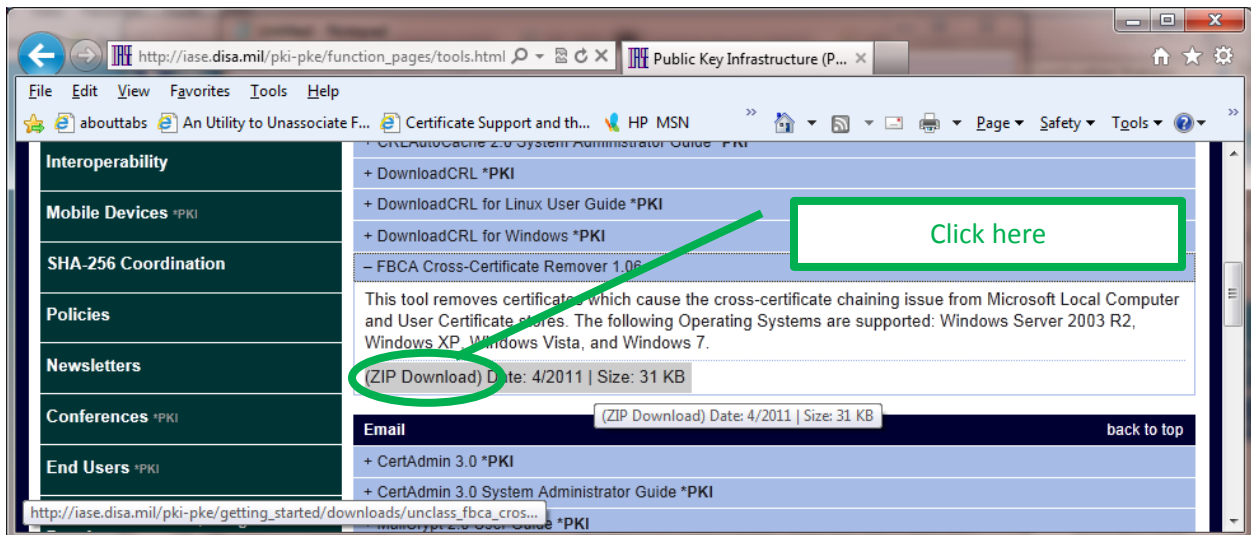
To obtain the DoD FBCA Cross-Certificate Remover tool go here:

[http://iase.disa.mil/pki-pke/function\\_pages/tools.html](http://iase.disa.mil/pki-pke/function_pages/tools.html)

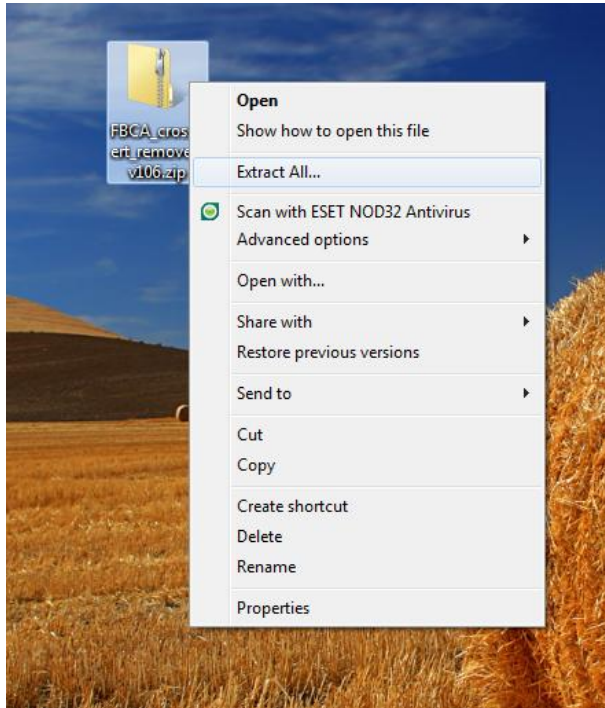
On the DISA IASE **PKI and PKE Tools** page look for the “FBCA Cross-Certificate Remover” link and click the “+” symbol to expand. *Please note that this tool may be updated over time and the version number, date and file size may change.*



Click on the Zip Download link to download the file



Download the zip file to your Desktop. On the Desktop extract the contents of the file. *Please note: There are many type of zip file extraction tools, yours may work differently. Please see your local IT support for help in extraction the zip file.*

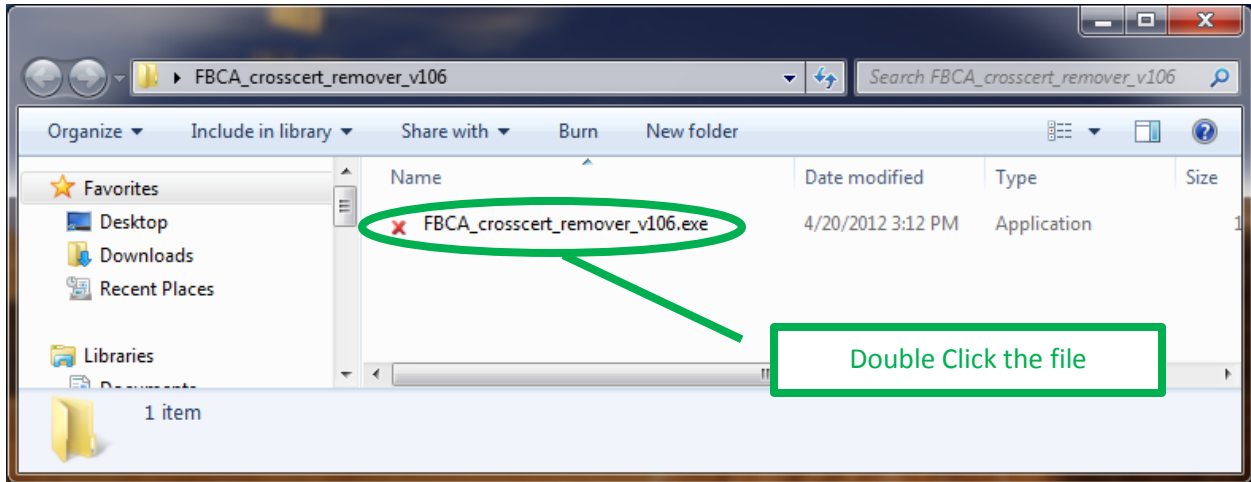


Open the extracted folder.

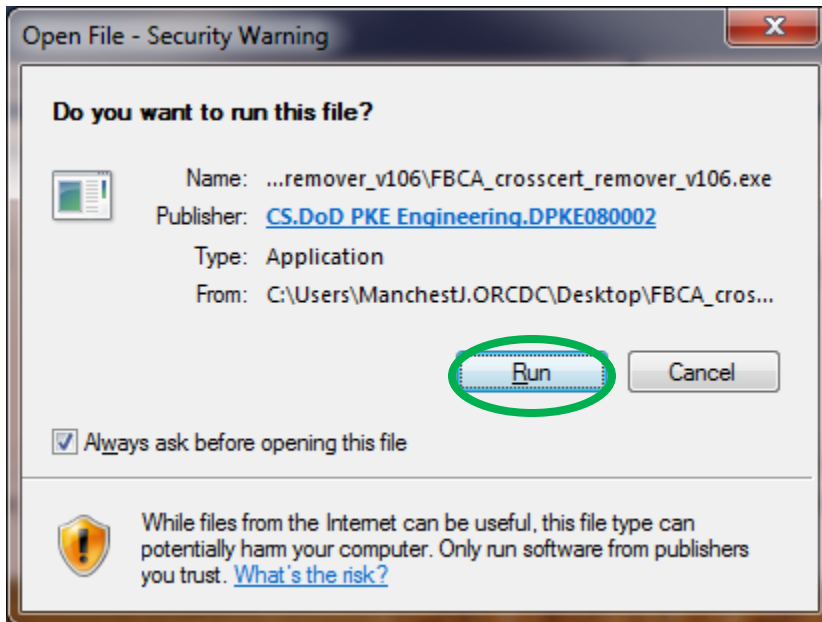


Double Click the folder

Double click to run the file.



If Windows asks, select Run



A cmd window will open. It talks about the purpose of the file and gives instructions.

```
##### FBCA cross-certificate removal tool 1.06 #####
Created by DoD PKE Engineering
Dec 2010

BACKGROUND: The DoD PKI PMO has discovered problems building certificate
chains when the DoD Root and Intermediate certificates have not been properly
installed.

PROBLEM: Administrators must install the DoD Root and latest intermediate CA
certificates on all workstations and servers.

SYMPTOMS: Users can experience delays when performing operations with DoD PKI
issued certificates. Inconsistent path building can occur where DoD PKI
certificates chain up to the Common Policy root or cross-certificates
mentioned below.

CERTIFICATES:
1) Issuer: CN=Common Policy, OU=FBCA, O=U.S. Government, C=us
   Subject: CN=Common Policy, OU=FBCA, O=U.S. Government, C=us
2) Issuer: CN=Common Policy, OU=FBCA, O=U.S. Government, C=us
   Subject: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
3) Issuer: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
   Subject: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
4) Issuer: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
   Subject: CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government, C=US
```

Scroll down



Then it has instructions

```
5) Issuer: CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government, C=US
   Subject: CN=DoD Root CA 2, OU=PKI, OU=DoD, O=U.S. Government, C=US

RESOLUTION:
* Disable the Microsoft Root Update Service (DISA STIG requirement)
* Install the DoD Root and Intermediate CA certificates which can be done by
  running the latest version of InstallRoot (as an administrator).
  InstallRoot can be obtained from https://www.dodpke.com/installroot/
* Run this tool with administrative privileges and then as the user
  experiencing the issues.

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

USAGE:
/SILENT      Silent mode - doesn't require user to hit <ENTER>.
/LIST       Only List Certificates
/DISALLOW   Disallow the certificates
/NODODROOT  Don't add the DoD Root and Intermediate CA certificates
/NOCPDISALLOW Don't disallow the certificates
/KEEPCP     Don't delete the certificates
/FORCE      Add certificates regardless if they already exist.

NOTE: Administrative privileges are required to remove certificates from
```

Scroll down



To disable Microsoft Root Update Service, you can consult Microsoft support.

To install the DOD Root and intermediate CA certificates (which you may have already done), go here:  
[http://eca.orc.com/wp-content/uploads/ECA\\_Docs/Trusting\\_DoD\\_PKIs.pdf](http://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf)

Press the Enter key

```
C:\Users\ManchestJ.ORCDC\Desktop\FBCA_crosscert_remover_v106\FBCA_crosscert_remover_v106...
* Microsoft Windows 2000 SP3 or later Operating System
* .NET Framework 2.0 or above

USAGE:
/SILENT          Silent mode - doesn't require user to hit <ENTER>.
/LIST           Only List Certificates - Don't remove them.
/DISALLOW      Disallow the certificate before deleting it.
/NOODROOT      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.
/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...
-
```

The file executes and more text appears; press the Enter key again

```
C:\Users\ManchestJ.ORCDC\Desktop\FBCA_crosscert_remover_v106\FBCA_crosscert_remover_v106...
* Adding Common Policy <2nd> to the LocalMachine Disallowed store...ACCESS DENI
ED
NOTE: This utility needs to be run with administrative privileges to perform thi
s action.

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

* Adding IRCA-DoDRootCA2 to the CurrentUser Disallowed store...ALREADY EXISTS
* Adding IRCA-DoDRootCA2 to the LocalMachine Disallowed store...ACCESS DENIED
NOTE: This utility needs to be run with administrative privileges to perform thi
s action.

Finished.

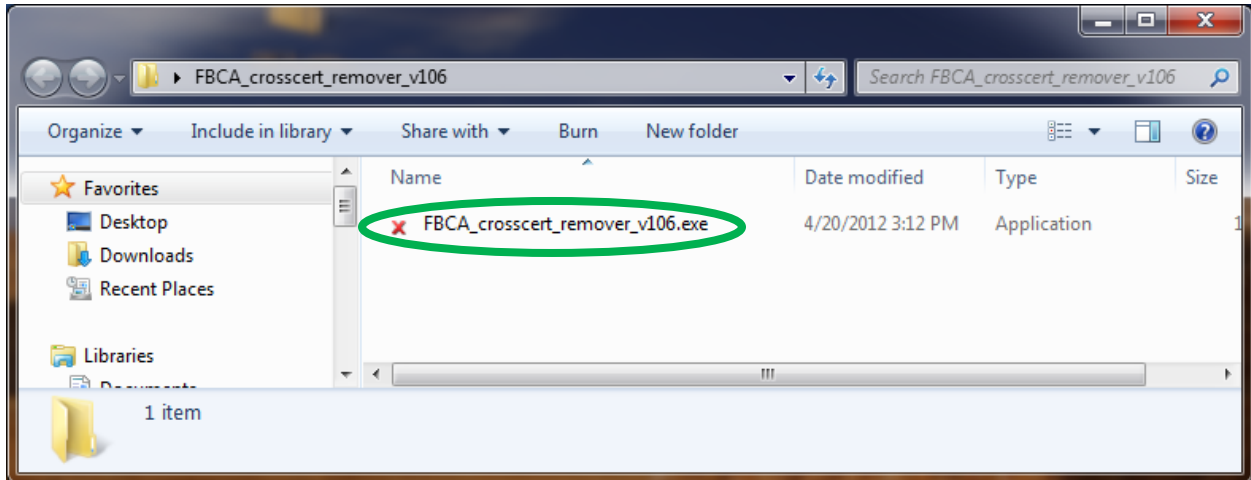
WARNING: Administrative privileges are needed to add or remove some of the
certificates on your system. Please rerun with these credentials.

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

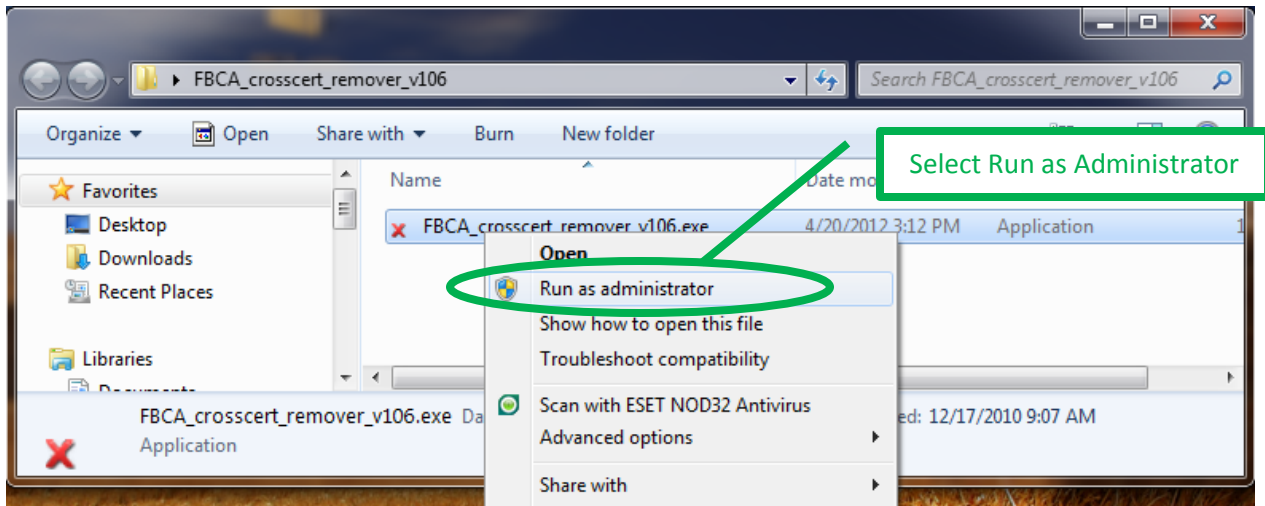
The cmd box closes.

Now run it again with Administrator privileges

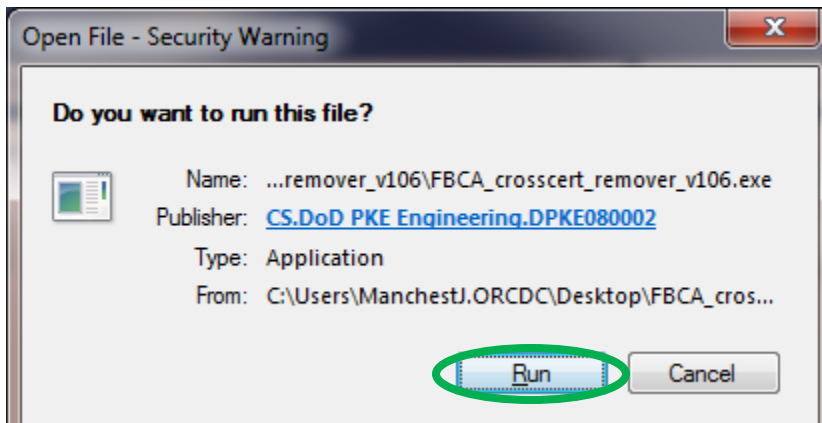
Go back to the extracted folder and right-click to run the file.



Then select Run as Administrator

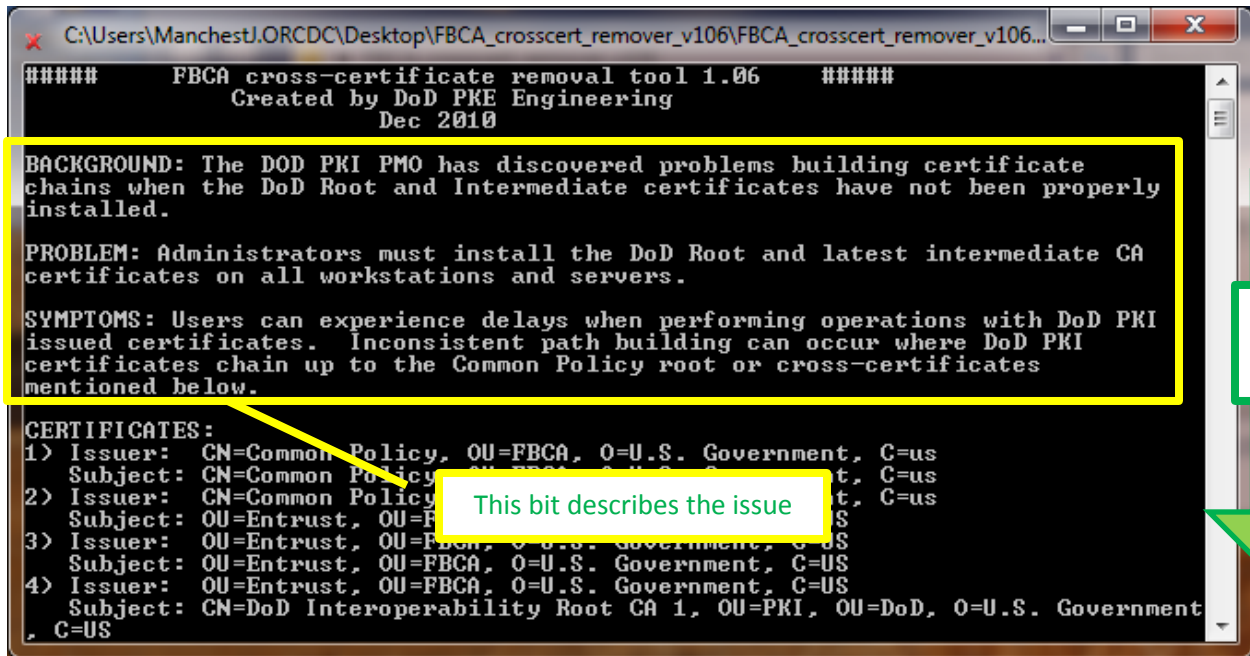


Click the Run button





A cmd window will open. It talks about the purpose of the file and gives instructions.



```
##### FBCA cross-certificate removal tool 1.06 #####
Created by DoD PKE Engineering
Dec 2010

BACKGROUND: The DoD PKI PMO has discovered problems building certificate
chains when the DoD Root and Intermediate certificates have not been properly
installed.

PROBLEM: Administrators must install the DoD Root and latest intermediate CA
certificates on all workstations and servers.

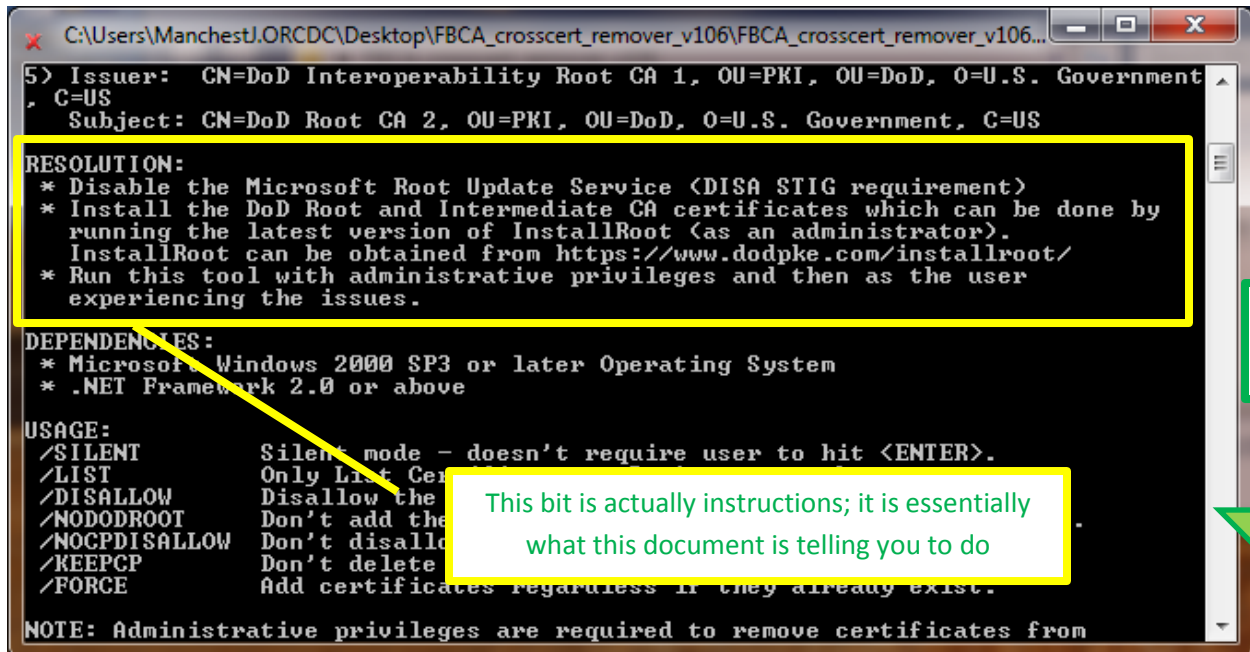
SYMPTOMS: Users can experience delays when performing operations with DoD PKI
issued certificates. Inconsistent path building can occur where DoD PKI
certificates chain up to the Common Policy root or cross-certificates
mentioned below.

CERTIFICATES:
1) Issuer: CN=Common Policy, OU=FBCA, O=U.S. Government, C=us
   Subject: CN=Common Policy, OU=FBCA, O=U.S. Government, C=us
2) Issuer: CN=Common Policy, OU=FBCA, O=U.S. Government, C=US
   Subject: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
3) Issuer: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
   Subject: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
4) Issuer: OU=Entrust, OU=FBCA, O=U.S. Government, C=US
   Subject: CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government, C=US
```

This bit describes the issue



Then it has instructions



```
5) Issuer: CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government, C=US
   Subject: CN=DoD Root CA 2, OU=PKI, OU=DoD, O=U.S. Government, C=US

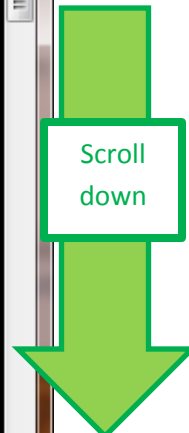
RESOLUTION:
* Disable the Microsoft Root Update Service (DISA STIG requirement)
* Install the DoD Root and Intermediate CA certificates which can be done by
  running the latest version of InstallRoot (as an administrator).
  InstallRoot can be obtained from https://www.dodpke.com/installroot/
* Run this tool with administrative privileges and then as the user
  experiencing the issues.

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

USAGE:
/SILENT      Silent mode - doesn't require user to hit <ENTER>.
/LIST       Only List Certificates
/DISALLOW   Disallow the certificates
/NODODROOT  Don't add the DoD Root and Intermediate CA certificates
/NOCPDISALLOW Don't disallow the certificates
/KEEPCP     Don't delete the certificates
/FORCE      Add certificates regardless if they already exist.

NOTE: Administrative privileges are required to remove certificates from
```

This bit is actually instructions; it is essentially what this document is telling you to do



To disable Microsoft Root Update Service, you can consult Microsoft support.

To install the DOD Root and intermediate CA certificates (which you may have already done), go here: [http://eca.orc.com/wp-content/uploads/ECA\\_Docs/Trusting\\_DoD\\_PKIs.pdf](http://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf)



Press the Enter key

```
C:\Users\ManchestJ.ORCDC\Desktop\FBCA_crosscert_remover_v106\FBCA_crosscert_remover_v106...
* Microsoft Windows 2000 SP3 or later Operating System
* .NET Framework 2.0 or above

USAGE:
/SILENT          Silent mode - doesn't require user to hit <ENTER>.
/LIST           Only List Certificates - Don't remove them.
/DISALLOW       Disallow the certificate before deleting it.
/NOODROOT       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.
/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...
-
```

The file executes and more text appears; press the Enter key again

```
C:\Users\ManchestJ.ORCDC\Desktop\FBCA_crosscert_remover_v106\FBCA_crosscert_remover_v106...
* Adding Common Policy <2nd> to the LocalMachine Disallowed store...ACCESS DENIED
NOTE: This utility needs to be run with administrative privileges to perform this action.

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

* Adding IRCA-DoDRootCA2 to the CurrentUser Disallowed store...ALREADY EXISTS
* Adding IRCA-DoDRootCA2 to the LocalMachine Disallowed store...ACCESS DENIED
NOTE: This utility needs to be run with administrative privileges to perform this action.

Finished.

WARNING: Administrative privileges are needed to add or remove some of the
certificates on your system. Please rerun with these credentials.

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

The cmd box closes.

You are now done; you may close the extracted folder.

