DoD Public Key Enablement (PKE) Information Paper

DoD Root Certificate Chaining Problem

Contact: PKE_Support@disa.mil
URL: http://iase.disa.mil/pki/pke

Enabling PKI Technology for DoD users

Audience
This document is intended for DoD system administrators.

Background
Department of Defense (DoD) Public Key Enabling (PKE) and Public Key Infrastructure (PKI) Program Management Office (PMO) have received several reports from DoD services about DoD certificates chaining improperly to cross-certificates or the Common Policy Root Certification Authority (CA). When this occurs on DoD systems, PKI validation does not work properly and may result in any of the following:

a) DoD user denied access to DoD web sites
b) DoD signed emails in Outlook appear invalid
c) DoD users experience extensive delays with Outlook or Internet Explorer during validation
d) DoD users receive a prompt to install the Common Policy Root CA when opening a signed email of a DoD sender whose workstation is misconfigured

Issue
The issue is that DoD workstations are not properly configured. Due to DoD information sharing initiatives with Federal and commercial partners, cross-certificates are essential for our partners to be able to validate DoD credentials but can cause problems on DoD systems when one or more of the following conditions exist:

a) When the DoD PKI CA certificates are not installed locally in the correct locations, Microsoft CAPI will attempt to build a path to a known issuer (e.g., Common Policy) and will automatically install cross-certificates obtained during path-processing into the user trust store. In addition to an incorrect or failed path, this can also cause significant delays.
b) When Microsoft's Root Update Service is not disabled, Microsoft will automatically add the Common Policy self-signed certificates (among others) into the local computer Trusted Root store. This can pose a significant security risk and is a STIG violation.
c) When valid certificate chains exist to both the DoD Root CA 2 and Common Policy Root CA, Microsoft will prefer the path to the Common Policy Root CA.

Resolution

DoD PKE recommends the following resolution:

a) DoD Root and subordinate/intermediate certificates should be installed on all DoD systems in the appropriate locations. Administrators should either use InstallRoot or other approved method of distribution (such as GPO). This will prevent Microsoft from trying to build a path to a known issuer since all required certificates are present locally. Appendix A provides additional details on proper certificate locations.

b) Microsoft's Root Update service should be disabled on all DoD systems (through GPO when possible) which will prevent Common Policy and other certificates from being added to the local computer trusted root store through Microsoft Root Update service.

c) The following cross-certificates should be removed from the local computer and user Intermediate Certification Authorities store.
   - Common Policy → Entrust (FBCA) cross-certificate 1 (Revoked)
   - Common Policy → Entrust (FBCA) cross-certificate 2
   - Entrust (FBCA)→IRCA cross-certificate
   - IRCA→DoD Root CA 2 cross-certificate

d) The following self-signed certificates should be removed from the local computer and user Trusted Root Certification Authorities store.
   - Entrust (FBCA) self-signed certificate

* DoD PKE has developed an executable which will automatically remove the specified certificates above. Certificate details and executable information are included in Appendix B.

Appendix A: DoD Certificate Installation

DoD Administrators should ensure that:

1. Local Computer Trusted Root Certification Authorities store contains DoD self-signed certificates (DoD Root CA 2, dod ocsp ss, etc)
2. Local Computer Intermediate Certification Authorities store should contain all DoD PKI intermediate and subordinate CA certificates.

InstallRoot should be run with Administrator privileges and will add the certificates in the proper locations. InstallRoot is available from one of the following locations:

- PKE on DKO: https://www.us.army.mil/suite/page/474113 under "Downloads"
- Dodpke.com https://www.dodpke.com/installroot/

The GPO distribution Quick Reference Guide, "DoD PKE QRG-Deploying DoD PKI CA Certificates using Microsoft GPOs_v1" is available from the location below:

- PKE on DKO: https://www.us.army.mil/suite/page/474113
  under Knowledge Base→Server→Microsoft Active Directory

Appendix B: Certificates to be Removed

DoD Administrators with workstations affected by this issue should remove the certificates below either with the DoD PKE tool or some other means.

The DoD PKE "FBCA Cross-Certificate Removal Tool" is available from the following location:

- PKE on DKO: https://www.us.army.mil/suite/page/474113 under "Downloads"

The following cross-certificates should be removed from the Local Computer and User Intermediate Certification Authority store:

Common Policy → Entrust (FBCA) cross-certificate
Subject: OU=FBCA, OU=FBCA,O=U.S. Government,C=us
Issuer: OU=Common Policy,OU=FBCA,O=U.S. Government,C=us
Serial # 18 cc d6 6b 00 01 00 00 00 6f
Valid To: Thursday, April 23, 2015 9:20:26 AM

Common Policy → Entrust (FBCA) cross-certificate (Revoked)
Subject: OU=FBCA, OU=FBCA,O=U.S. Government,C=us
Issuer: OU=Common Policy,OU=FBCA,O=U.S. Government,C=us
Serial # 62 fa 21 6f 00 01 00 00 00 56
Valid To: Friday, March 21, 2014 12:25:49 PM

Entrust (FBCA)→IRCA cross-certificate
Subject: CN=DoD Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Issuer: OU=Entrust,OU=FBCA,O=U.S. Government,C=US
Serial # 45 1d e5 23
Valid To: Friday, December 31, 2010 12:00:00 AM

IRCA→DoD Root CA 2 cross-certificate
Subject: CN=DoD Root CA 2, OU=PKI,OU=DoD,O=U.S. Government,C=US
Issuer: CN=DoD Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial # 0C
Valid To: Thursday, March 03, 2011 10:22:43 AM

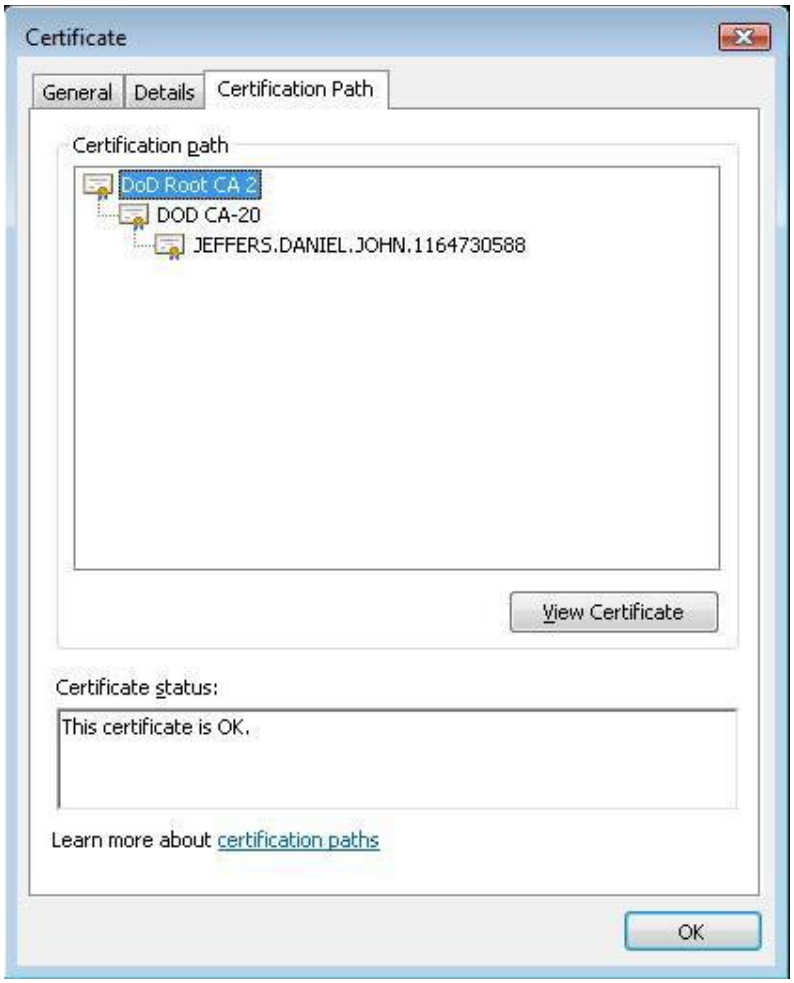
The following self-signed certificate(s) should be removed from the Local Computer and User Trusted Root Certification Authority store:

Entrust (FBCA) self-signed certificate
Subject: OU=Entrust,OU=FBCA,O=U.S. Government,C=US
Issuer: OU=Entrust,OU=FBCA,O=U.S. Government,C=US

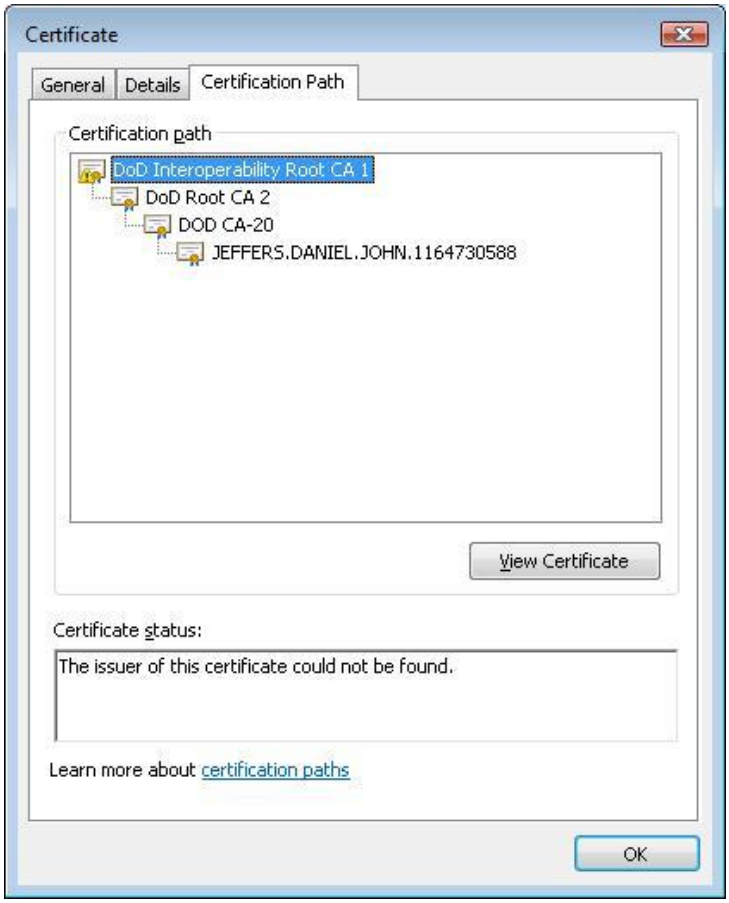
Serial # 45 1d e1 72
Valid To: Tuesday, December 31, 2013 11:04:51 AM

Appendix B: Certificate Chain Screen Shots

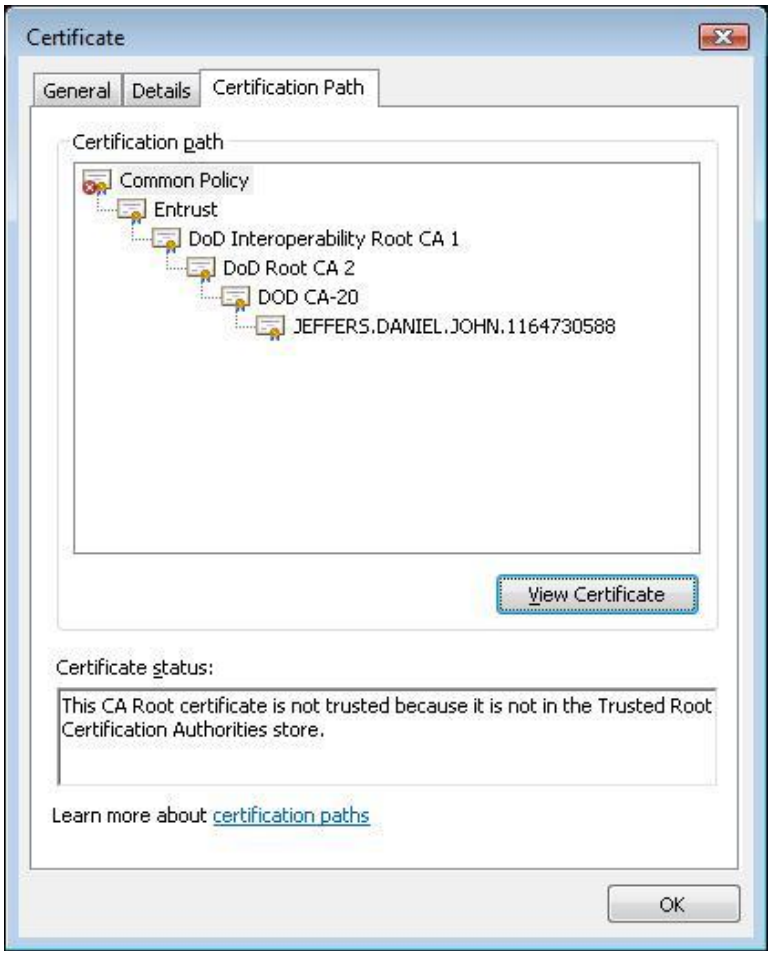
Desired Chain



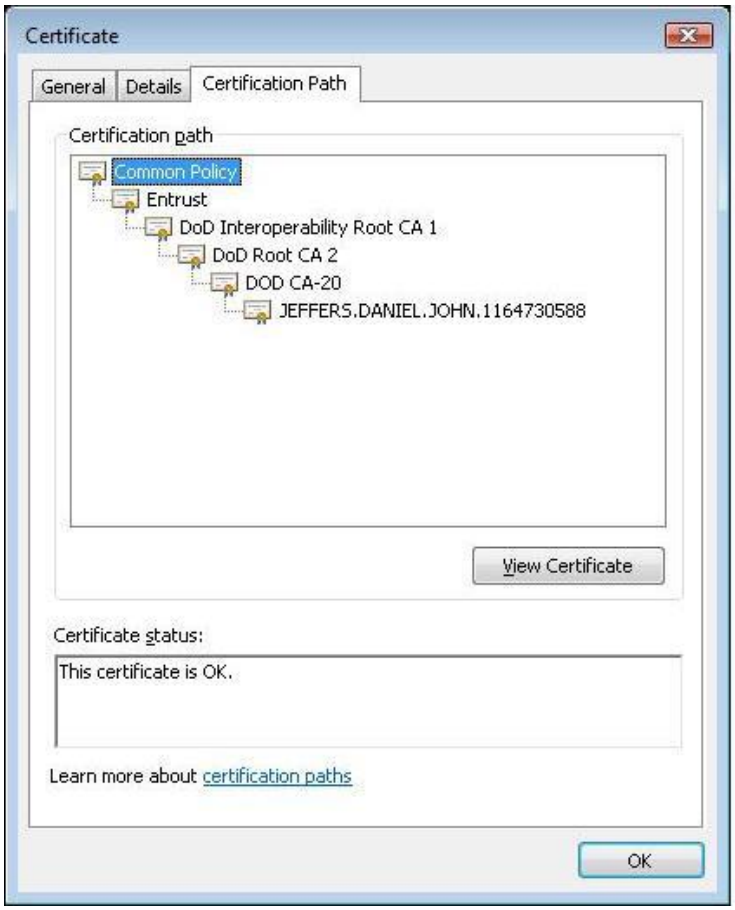
Bad Chain # 1


Certificate
General
Details
Certification Path
Certification path
DoD Interoperability Root CA 1
DoD Root CA 2
DOD CA-20
JEFFERS.DANIEL.JOHN.1164730588
View Certificate
Certificate status:
The issuer of this certificate could not be found.
Learn more about certification paths
OK

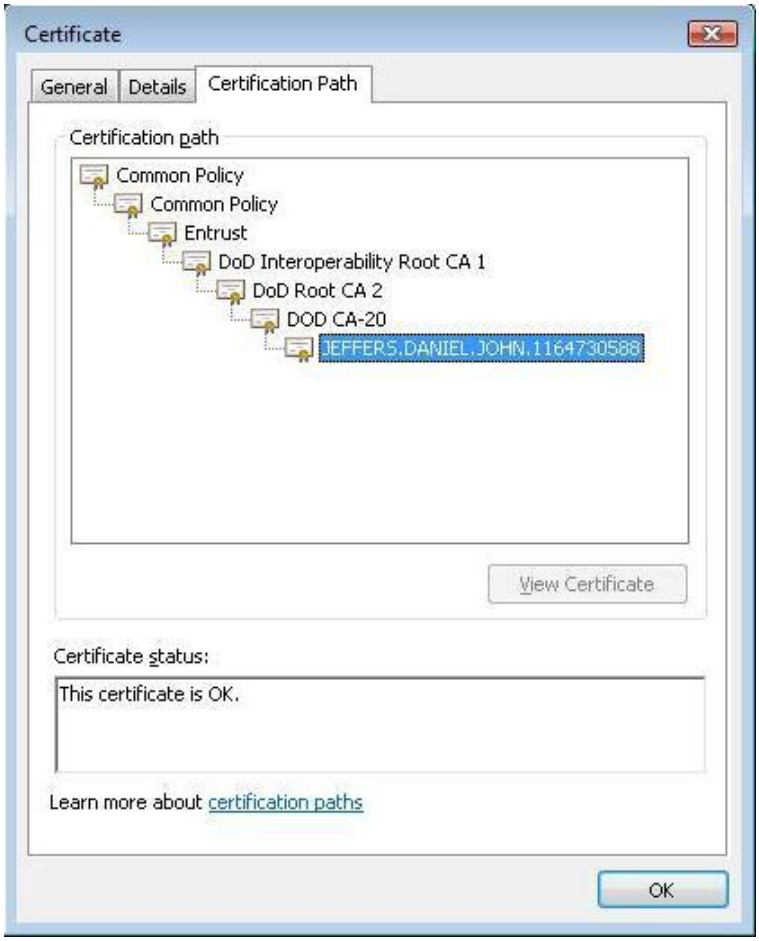
Bad Chain #2


Certificate
General
Details
Certification Path
Certification path
Common Policy
Entrust
DoD Interoperability Root CA 1
DoD Root CA 2
DOD CA-20
JEFFERS.DANIEL.JOHN.1164730588
View Certificate
Certificate status:
This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.
Learn more about certification paths
OK

Bad Chain #3


Certificate
General
Details
Certification Path
Certification path
Common Policy
Entrust
DoD Interoperability Root CA 1
DoD Root CA 2
DOD CA-20
JEFFERS.DANIEL.JOHN.1164730588
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK

Bad Chain #4


Certificate
General
Details
Certification Path
Certification path
Common Policy
Common Policy
Entrust
DoD Interoperability Root CA 1
DoD Root CA 2
DOD CA-20
JEFFERS.DANIEL.JOHN.1164730588
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK