

UNCLASSIFIED



DoD Public Key Enablement (PKE) User Guide

FBCA Cross-Certificate Remover

Contact: dodpke@mail.mil

URL: <http://iase.disa.mil/pki-pke>

Enabling PKI Technology
for DoD users

FBCA Cross-Certificate Remover 1.0.10 User Guide

23 October 2013

Version 1.4

DoD PKE Team

UNCLASSIFIED

Revision History

Issue Date	Revision	Change Description
1/18/2012	1.0	Initial Release
8/8/2012	1.1	Updated DoD PKE support email address
7/11/2013	1.2	Updated to reflect version 1.0.8 release, which incorporates untrusting the US DoD CCEB IRCA 1 > DoD Root CA 2 cross-certificate and removes functionality to proactively untrust Common Policy certification authorities (CAs) when the certificates are not found on the machine.
9/11/2013	1.3	Updated to reflect version 1.0.9 release, which incorporates the reissued DoD IRCA 1 > DoD Root CA 2 cross-certificate.
10/23/2013	1.4	Updated to reflect version 1.0.10 release, which incorporates a newly issued IRCA1>ECA Root CA 2 Cross-Certificate (Certificate Date 10.18.2013) and a reissued IRCA1>DoD Root CA (Certificate Date 10.09.2013). Also reordered the command line options to mirror the application's help file order.

Contents

OVERVIEW 1

SYSTEM REQUIREMENTS 3

 OPERATING SYSTEM 3

 REQUIRED PACKAGES 3

 USER PRIVILEGES 3

INSTALLING AND RUNNING THE TOOL 4

 PREPARATION 4

 RUNNING THE TOOL 5

 USAGE 5

 OPTIONS 6

 /SILENT 6

 /LIST 6

 /DISALLOW 6

 /NODODROOT 7

 /NOCPDISALLOW 7

 /KEEPCP 7

 /ECA 7

 /NODELETE 8

 /FORCE 8

 /DEBUG 8

APPENDIX A: SUPPLEMENTAL INFORMATION 10

 WEB SITE 10

 TECHNICAL SUPPORT 10

Overview

The Federal Bridge Certification Authority (FBCA) Cross-Certificate Remover Tool is designed to help DoD organizations address the Microsoft cross-certificate chaining issue. The issue may manifest itself in several ways:

- Users may be unable to access DoD web sites normally accessible using certificates on their Common Access Cards (CACs)
- DoD signed emails in Outlook may appear invalid
- Users may experience extensive delays with Outlook or Internet Explorer during validation
- Users' CAC certificates may appear to chain to a root beyond/other than DoD Root 2
- Users may receive a prompt to install the Common Policy Root Certification Authority (CA) or other roots cross-certified with the Federal Bridge when opening a signed email from a DoD sender whose workstation is misconfigured

The issue is due to the way Microsoft's Cryptographic Application Programming Interface (CAPI) performs its certificate path building, preferring paths with more information over paths with less, which often results in it preferring a path built through a PKI bridge (such as the Federal Bridge) to an outside trust anchor (such as Federal Common Policy) rather than a shorter path within a homogeneous PKI (such as DoD PKI). More detailed information on Microsoft's path selection algorithm can be found in their blog post at

<http://blogs.technet.com/b/pki/archive/2010/05/13/certificate-path-validation-in-bridge-ca-and-cross-certification-environments.aspx>. Additional discussion of the issue is available in *FAQ: DoD Root Certificate Chaining Problems* on the DoD PKE web site at <http://iase.disa.mil/pki-pke> under *PKE A-Z > FAQs*.

Four steps are recommended to overcome this problem:

1. The DoD root and intermediate CA certificates should be installed on all workstations and servers experiencing the issue. DoD PKE's InstallRoot tool, available from <http://iase.disa.mil/pki-pke> under *Tools > Trust Store Management*, can be used to perform this operation.
2. Microsoft's Root Update Service should be disabled in accordance with the Windows Operating System Security Technical Implementation Guides (STIGs).
3. In Microsoft Outlook Email Security settings, the "Send these certificates with signed messages" check box should be unchecked. This will cause only the end

entity signing and encryption certificates, rather than the full certificate chains, to be sent with signed messages.

4. The FBCA Cross-Certificate Remover tool should be run.

The Federal Bridge Cross-Certificate Remover tool addresses the issue by moving cross-certificates issued to DoD Root 2, including the DoD Interoperability Root CA (IRCA) 1 > DoD Root CA 2 certificate and the US DoD CCEB IRCA 1 > DoD Root 2 certificate, to Microsoft's Untrusted Certificates store on the user's workstation, causing the local machine to treat that certificate as revoked and preventing the machine from building paths from DoD end user certificates to roots outside of the DoD PKI. This will not impact the workstation's ability to build paths for and validate other Federal Bridge members' certificates. The tool can also move common roots that are installed by Microsoft's Root Update service to the Untrusted Certificates store to address instances in which machines may not properly process the cross-certificate as revoked.

The FBCA Cross-Certificate Remover tool should only be run by DoD relying parties and, to be effective, the tool should be run once as an administrator and once as the current user to perform certificate actions in both the Local Computer and Current User certificate stores.

NOTE: WEB SERVER ADMINISTRATORS WITH USERS EXPERIENCING DENIAL-OF-SERVICE DUE TO THIS ISSUE SHOULD EXPLORE OPTIONS FOR FORCING THE WEB SERVER TO DISCARD THE PRESENTED CERTIFICATE CHAIN AND ATTEMPTING TO BUILD A VALID PATH FROM THE END USER CERTIFICATE ON THE SERVER SIDE. THE TRUST ANCHOR CONSTRAINTS TOOL (TACT), AVAILABLE FROM THE DoD PKE SITE AT [HTTP://IASE.DISA.MIL/PKI-PKE](http://iase.disa.mil/pki-pke) UNDER TOOLS > CERTIFICATE VALIDATION, IS ONE SUCH OPTION.

System Requirements

Operating System

Supported operating systems include:

- Windows XP SP3
- Windows Vista
- Windows 7
- Windows Server 2003 SP2
- Windows Server 2008
- Windows Server 2008 R2

Required Packages

.NET 2.0 Framework or later is required to run the tool.

User Privileges

Administrative privileges are recommended to enable the tool to fully address the cross-certificate chaining issue by managing both the Local Computer and Current User certificate stores. The tool may be run by a non-privileged user; however, in that case certificate actions will only be taken on the Current User store, and the chaining issue may not be corrected.

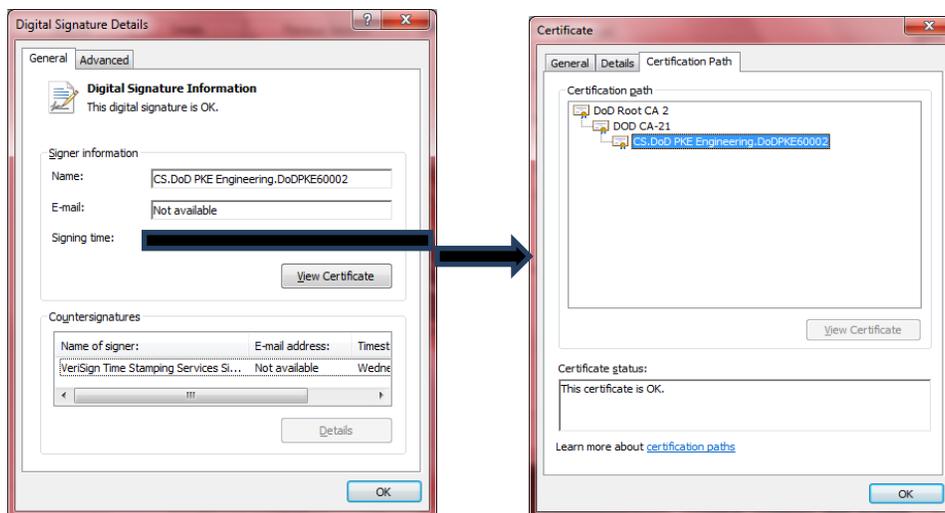
Installing and Running the Tool

The command-line utility can be run locally, from portable media, or even as a logon script.

Preparation

The command-line utilities come packaged within zip archives. No installation beyond extraction of the archive and validation of its contents is necessary.

- 1) Extract the contents of the .zip archive by right-clicking on the archive, selecting “**Extract All...**” from the pick list, entering the desired extraction location in the pop-up window and clicking **Extract**.
- 2) Verify the digital signature on the command-line executable file (.exe) that was extracted from the .zip archive.
 - a. In Windows Explorer, navigate to the directory containing the executable package.
 - b. Right-click on the executable and select **Properties** from the pop-up menu.
 - c. The Properties window opens. Click the Digital Signatures tab.
 - d. Select the certificate and click **Details**. The Digital Signature Details window opens. The message “**This digital signature is OK**” will display.
 - e. Click **View Certificate** and select the **Certification Path** tab to verify the certification path. The certification path should read “DoD Root CA 2 > DoD CA-21 > CS.DoD PKE Engineering.DoDPKE60002.”



Running the Tool

To run the utility locally or from portable media:

- 1) In a command prompt, navigate to the directory containing the command-line executable.
- 2) Enter the desired command (see Options section for available arguments) to run the tool.

NOTE: ON WINDOWS VISTA, 7, AND SERVER 2008, RUN THE COMMAND PROMPT AS AN ADMINISTRATOR TO MANAGE CERTIFICATES IN THE LOCAL COMPUTER STORE. IF THE COMMAND PROMPT IS NOT OPEN WITH ADMINISTRATIVE PRIVILEGES, ONLY CERTIFICATES IN THE CURRENT USER STORE WILL BE ADDRESSED.

Usage

There are three core commands available with the remover tool command-line utility: Manage certificates (the default behavior), list the status of certificates managed by the tool (executed using /list), and view tool help (executed using /h).

By default, the tool will perform the following certificate management operations:

1. List certificates that will be removed by the tool if present in the trusted certificate store. These include:
 - DoD Interoperability Root CA (IRCA) 1 > DoD Root CA 2 cross-certificate
 - Federal Bridge (Entrust) > IRCA1 cross-certificate
 - Federal Bridge (Entrust) self-signed root certificate
 - Common Policy > FBCA (Entrust) cross-certificate
 - Common Policy self-signed root certificate
2. Search for the certificates listed in step 1 in the Local Computer and Current User **Trusted** certificate stores.
3. Remove any certificates found in step 2 from the Local Computer and Current User **Trusted** certificate stores.
4. Add DoD Root CA 2 to the Local Computer and Current User **Trusted** certificate stores.
5. Add the following certificates to the Local Computer and Current User **Untrusted** certificate stores:
 - DoD IRCA 1 > DoD Root CA 2 cross-certificate (valid dates 8/27/2013 to 12/31/2013)
 - DoD IRCA 1 > DoD Root CA 2 cross-certificate (valid dates 10/10/2013 to 10/09/2016)
 - US DoD CCEB IRCA 1 > DoD Root CA 2 cross-certificate

See **Options** for a description of the behavior of optional arguments. Replace <num> with the release number of the executable you wish to run; for example, FBCA_crosscert_remover_v110. Optional arguments are displayed in square [] brackets.

To run the tool: FBCA_crosscert_remover_v<num> [/silent] [/disallow] [/nododroot] [/nocpdisallow] [/keepcp] [/eca] [/nodelete] [/force]

To list certificates: FBCA_crosscert_remover_v<num> /list

To view tool help: FBCA_crosscert_remover_v<num> /h

Options

/ HELP

This option displays help information for the tool.

Usage:
/help

Examples:
FBCA_crosscert_remover_v110 /help

/SILENT

This option causes the tool to execute without any required user intervention or console output.

Usage:
/silent

Example:
FBCA_crosscert_remover_v110 /silent

/LIST

This option searches the certificate stores for and reports on the status of certificates managed by the tool.

Usage:
/list

Example:
FBCA_crosscert_remover_v110 /list

/DISALLOW

This option moves all certificates to the untrusted store before deleting them.

Usage:
/disallow

Example:
FBCA_crosscert_removal_v110 /disallow

/NODODROOT

This option prevents the DoD Root CA 2 certificate from being installed in the **Trusted Root Certification Authorities** stores.

Usage:
/nododroot

Examples:
FBCA_crosscert_removal_v110 /nododroot

/NOCPDISALLOW

This option prevents the Common Policy root certificate from being added to the **Untrusted** certificate stores.

Usage:
/nocpdisallow

Examples:
FBCA_crosscert_removal_v110 /nocpdisallow
FBCA_crosscert_removal_v110 /nocpdisallow /silent

/KEEPCP

This option prevents the deletion of the Common Policy root certificate from the **Trusted** certificate stores.

Usage:
/keepcp

Examples:
FBCA_crosscert_removal_v110 /keepcp
FBCA_crosscert_removal_v110 /keepcp /silent

/ECA

This option removes and untrusts the SHA-1 Federal Root CA > ECA Root CA 2 and the DoD Interoperability Root CA 1 > ECA Root CA 2 cross-certificates in addition to performing the default actions. It also trusts the ECA Root CA 2

certificate. This option should only be run on machines that trust the ECA Root CA 2 and wish to prevent ECA certificates from chaining beyond that root.

Usage:

```
/eca
```

Examples:

```
FBCA_crosscert_removal_v110 /eca  
FBCA_crosscert_removal_v110 /eca /silent
```

/NODELETE

This option prevents the deletion of any certificates.

Usage:

```
/nodelete
```

Examples:

```
FBCA_crosscert_removal_v110 /nodelete  
FBCA_crosscert_removal_v110 /nodelete /silent
```

/FORCE

This option adds certificates regardless of whether they already exist in the machine's certificate store.

Usage:

```
/force
```

Examples:

```
FBCA_crosscert_removal_v110 /force  
FBCA_crosscert_removal_v110 /force /silent
```

The following command does not appear in the /help parameter:

/DEBUG

This option displays detailed output describing the steps the tool is executing as it is run.

Usage:

```
/debug
```

Example:

```
FBCA_crosscert_removal_v110 /debug
```


Appendix A: Supplemental Information

Please use the links below for additional information and support.

Web Site

Visit the URL below for the PKE website.

<http://iase.disa.mil/pki-pke>

Visit the *Tools* page to download the latest version of the FBCA Cross-Certificate Remover.

Technical Support

Contact technical support through the email address below.

dodpke@mail.mil

Acronyms

CA	Certification Authority
CAC	Common Access Card
CAPI	Cryptographic Application Programming Interface
FBCA	Federal Bridge Certification Authority
IRCA	Interoperability Root Certification Authority
PKE	Public Key Enablement
PKI	Public Key Infrastructure
SP	Service Pack
STIG	Security Technical Implementation Guide