DoD Public Key Enablement (PKE) Reference Guide

Public Key Enabling Firefox

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

Enabling PKI Technology for DoD users

Public Key Enabling Firefox

3 March 2010

Version 1.1

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
1/18/10	1.0	Initial Document Creation
3/5/10	1.1	Updated Document to comply with new QRG format

Contents

Introduction

The DoD Public Key Enablement (PKE) Reference Guides (RGs) are developed to help an organization augment their security posture through the use of the Public Key Infrastructure (PKI). The PKE RGs contain procedures for obtaining DoD certificates and enabling specific technologies for use with those certificates.

Purpose

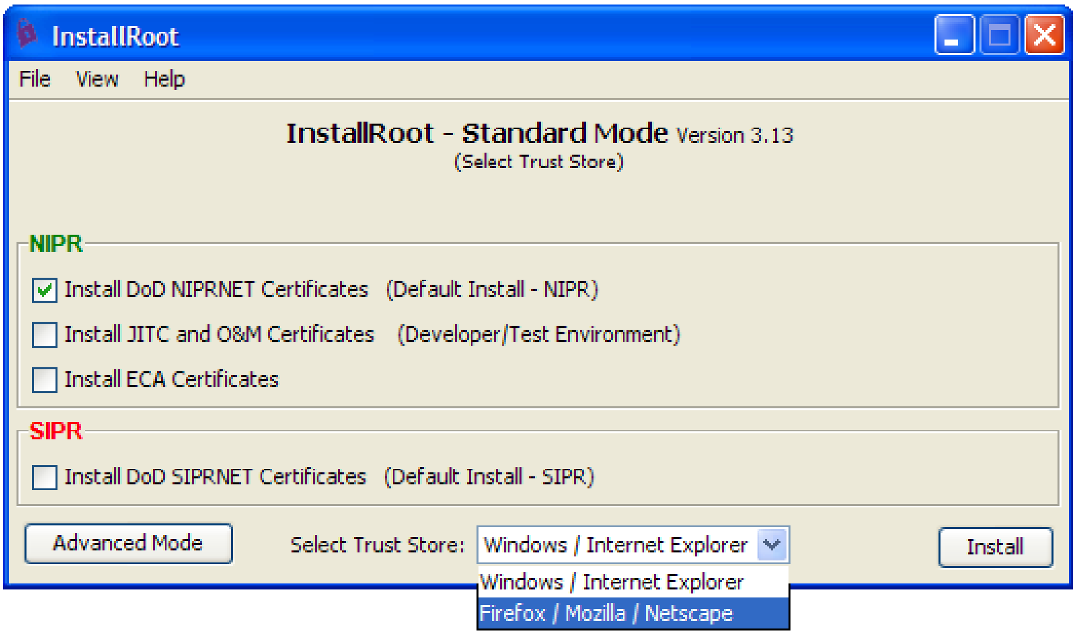
The goal of this RG is to aid in enabling Firefox for use with DoD websites. Contained in this document are instructions to install your certificate, use the CAC with Firefox, and configure certificate validation for Firefox. The overall goal is to PK-Enable Firefox.

Scope

This document is intended for all users of PKI technologies. No in depth knowledge of PKI is required, and no intimate knowledge of CACs is necessary. Some experience installing and configuring software on the Windows platforms is helpful when reading this guide.

Install Certificates from InstallRoot

1) Download and install the InstallRoot tool. Java will need to either be installed on the system, if not, the version of InstallRoot with JRE bundled will be necessary. InstallRoot may be downloaded from: https://www.dodpke.com/installroot/
2) Open the InstallRoot tool and select Firefox/Mozilla/Netscape from the tab at the bottom.
3) Be sure only the top box is checked within NIPR.



InstallRoot - Standard Mode Version 3.13
(Select Trust Store)

NIPR

☑ Install DoD NIPRNET Certificates (Default Install - NIPR)

□ Install JITC and O&M Certificates (Developer/Test Environment)

□ Install ECA Certificates

SIPR

□ Install DoD SIPRNET Certificates (Default Install - SIPR)

Select Trust Store: Windows / Internet Explorer

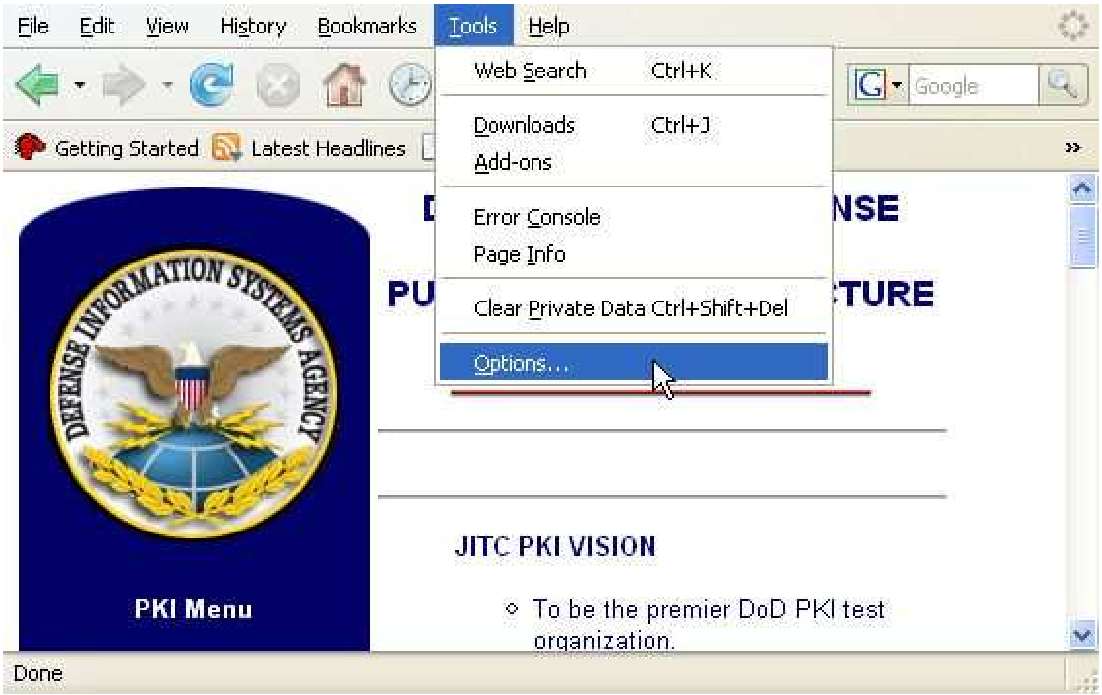
4) Click the 'Install' button and wait for the installation to complete. Please wait until you see a confirmation dialog indicating the tool is finished.
NOTE: If possible, when using the InstallRoot tool, be sure your CAC is not in the systems card reader.

Using Common Access Card (CAC) certificates in Firefox

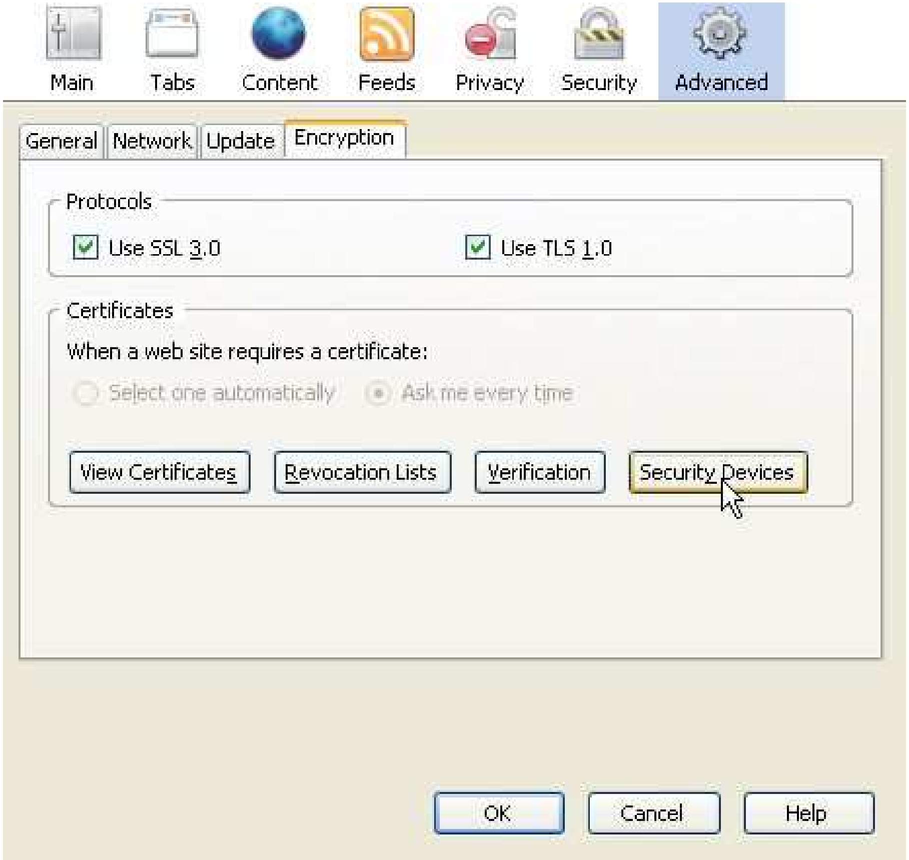
These instructions will enable ActivIdentity's ActivClient software to work within Firefox. Before proceeding, try to ensure the latest version of ActivClient is installed by going to the ActivClient website to check the latest version. Before installing the latest version, please uninstall any previous versions of ActivClient.

As of version 6.2, ActivClient by default configures Firefox to accept the CAC certificates without any additional configuration. You may use the following instructions to verify that it has been installed properly. If using an older version of ActivClient, these instructions will assist with proper configuration.

1) Open Firefox
2) Click on Tools -> Options in the menu bar.



3) In the Options window, go to Advanced -> Encryption -> Security Devices.



Protocols

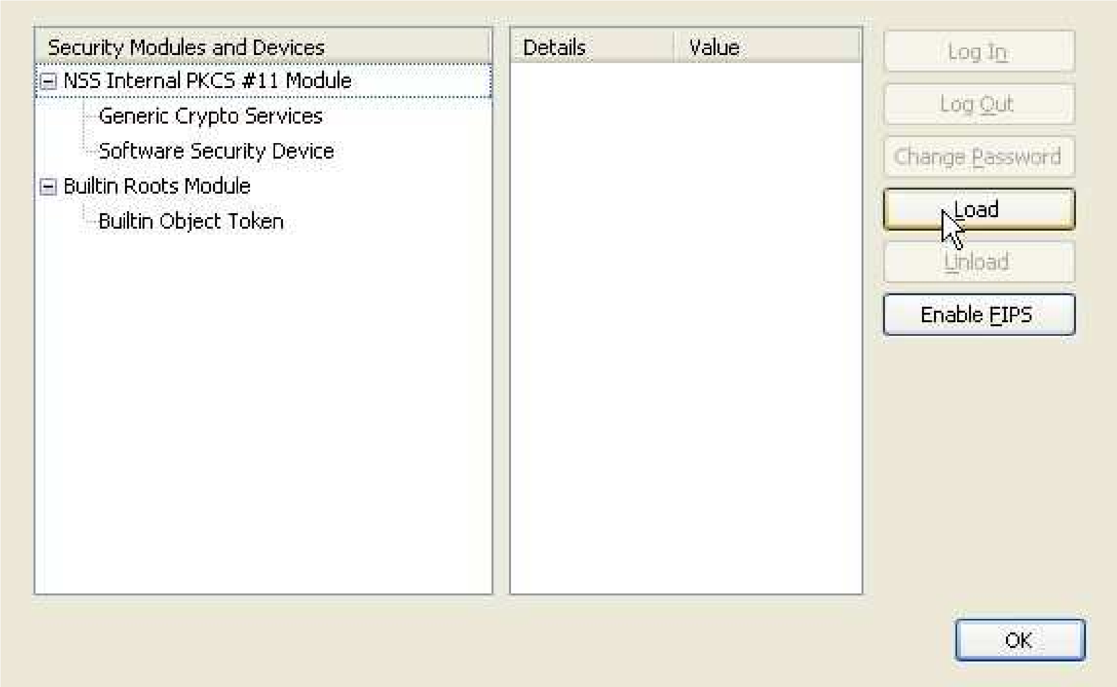
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

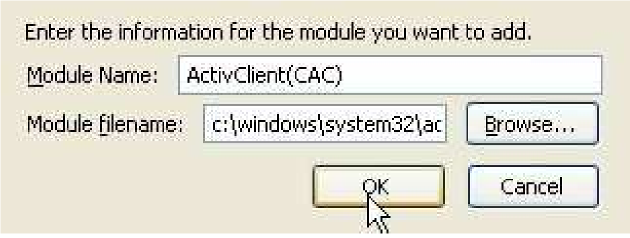
When a web site requires a certificate:

○ Select one automatically ● Ask me every time

4) In the new window, click on Load.



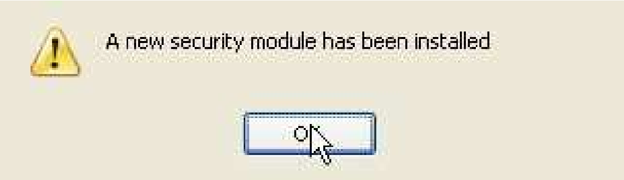
5) Enter "ActivClient(CAC)" for the Module Name and "c:\windows\system32\acpkcs201-ns.dll" for Module Filename and click OK, and then OK again in the confirmation window.


Enter the information for the module you want to add.

Module Name: ActivClient(CAC)

Module filename: c:\windows\system32\ac

6) The confirmation message will show that the security device (CAC) was loaded. CAC certificates can now be used with the browser.

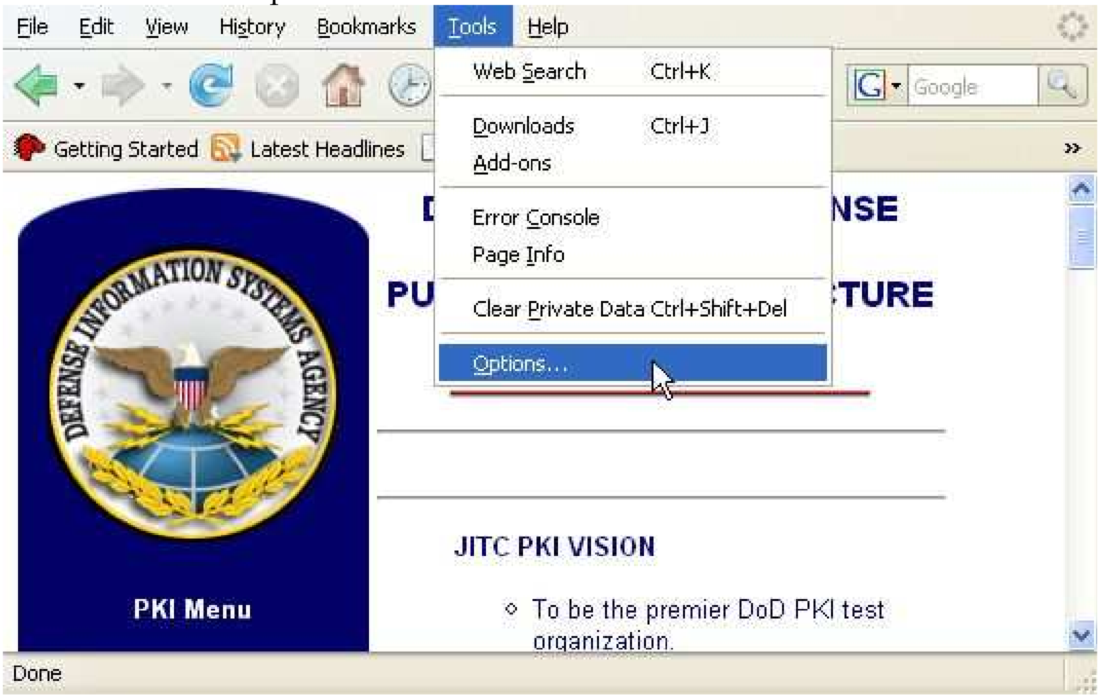


A new security module has been installed

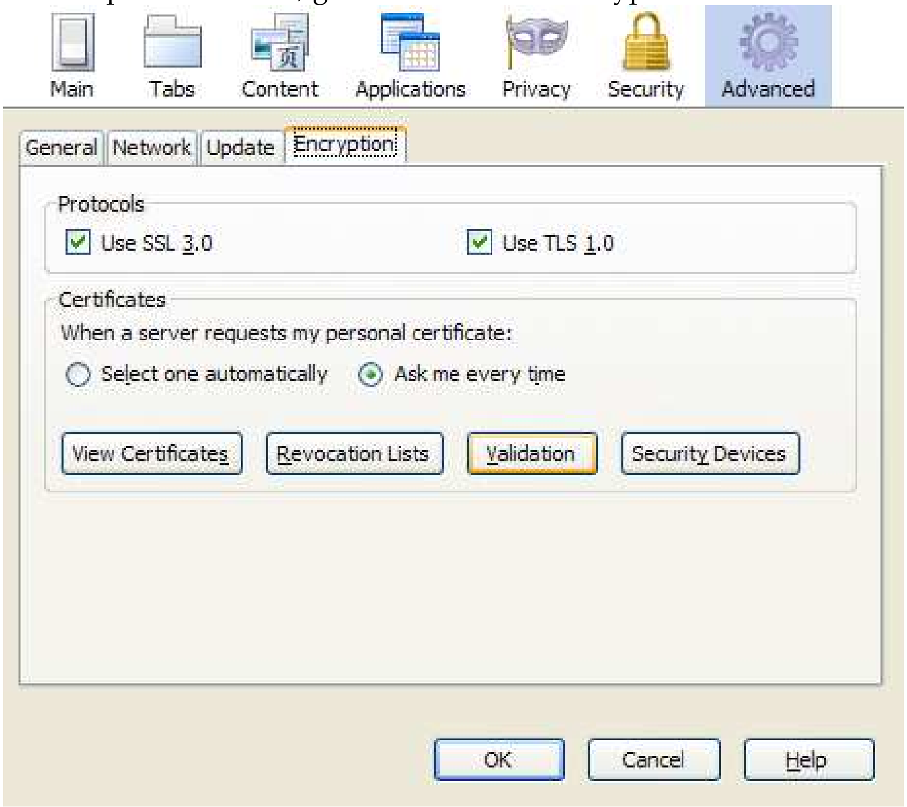
Ensure Online Certificate Status Protocol (OCSP) is Confirming Certificate Validity

With any versions of ActivClient later than 6.2, these settings will be automatically configured. However, these instructions can be used to confirm proper configuration for older versions of ActivClient.

1) Open Firefox
2) Click on Tools -> Options in the menu bar.



3) In the Options window, go to Advanced -> Encryption -> Validation.



Protocols

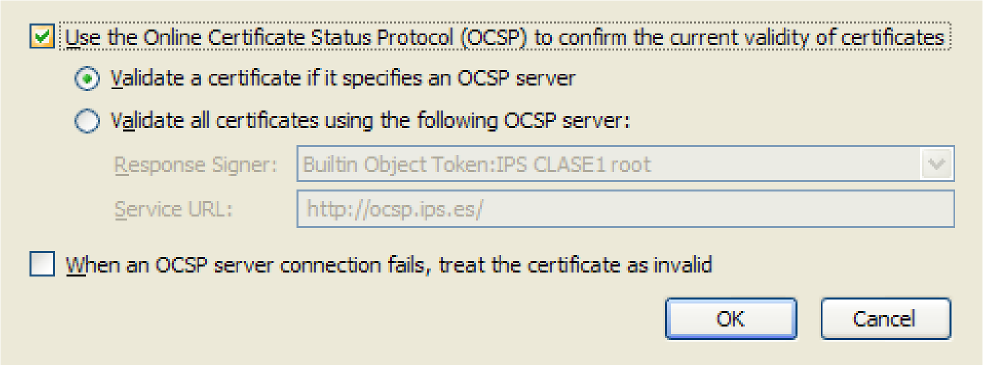
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

4) Ensure the option "Use the OCSP to confirm the current validity of certificates" is checked. If checked, Firefox is now properly OCSP enabled.



☑ Use the Online Certificate Status Protocol (OCSP) to confirm the current validity of certificates

● Validate a certificate if it specifies an OCSP server

○ Validate all certificates using the following OCSP server:

Response Signer: Builtin Object Token:IPS CLASE1 root

Service URL: http://ocsp.ips.es/

□ When an OCSP server connection fails, treat the certificate as invalid

Appendix A: Supplemental Information

Website

Please visit the URL below for additional information
www.iase.disa.mil/pki/pke

Technical Support

Contact technical support
PKE_Support@disa.mil

Acronyms

AIA	Authority Information Access
CA	Certificate Authority
CRLDP	Certificate Revocation List Distribution Point
DV	Desktop Validator
LDAP	Lightweight Directory Access Protocol
MSCAPI	Microsoft Crypto API
OCSP	Online Certificate Status Protocol
PKE	Public Key Enablement
RCVS	Robust Certificate Validation Service
VA	Validation Authority