DoD Public Key Enablement (PKE) Reference Guide

Public Key Enabling Oracle Weblogic Server

Contact: dodpke@mail.mil
URL: http://iase.disa.mil/pki-pke
URL: http://iase.disa.smil.mil/pki-pke

Enabling PKI Technology for DoD users

Public Key Enabling Oracle Weblogic Server

4 March 2015

Version 1.0

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
3/4/2015	1.0	Initial release of PKI Authentication and Certificate Revocation guide

Contents

Introduction

The DoD Public Key Enablement (PKE) reference guides are developed to help an organization augment their security posture through the use of the DoD and National Security Systems (NSS) Public Key Infrastructures (PKI). The PKE reference guides contain procedures for enabling products and associated technologies to leverage the security services offered by the DoD and NSS PKIs.

Purpose

The purpose of this reference guide is to provide guidance to the DoD user community on the process to secure and Secure Socket Layer (SSL)/Transport Layer Security (TLS)-enable an Oracle Weblogic server. This document describes how to generate a certificate request, submit a certificate request, and retrieve a PKI certificate for the server. Furthermore, it details steps for installing the server certificate, configuring Weblogic security settings, and implementing certificate validation. Server certificates raise the security posture of DoD information assets by providing identity authentication of the resource and enabling the server to use TLS to encrypt communications. Certificate-based client authentication increases the security posture even further by providing identity authentication of the user requesting access to the resource. Finally, mapping or binding of the user's certificate to a user account with associated permissions provides authorization to the resource. It is important that this document is read front to back to ensure all relevant steps are performed. Partially implementing the steps in this document can leave portions of a web server unsecure.

Scope

This document is intended for all system administrators. Administrator privileges are required to complete this guide. No in-depth knowledge of PKI is required. Experience installing and configuring software on Windows platforms is required.

Baseline

This guide was developed using Weblogic 11gR1 installed on a Windows 2008 Server R2 system. It is highly recommended that Windows 2008 operating system have the latest software updates. The command utilities used in this guide are specific to Windows systems. The system must also have the latest Security Technical Implementation Guide (STIG) settings applied. The STIGs are located at http://iase.disa.mil/stigs/. If this guide is being implemented on different operating systems, equivalent commands will need to be used to accomplish each specific task in the guide.

Planning and Preparation

As part of the DoD Instruction (DoDI) 8520.02i requirement to properly secure DoD information systems and networks, the enterprise must Public Key-enable access to web servers. This requires that all users be authenticated using DoD-approved PKI credentials.

The procedures in this guide go through PK Enabling the Weblogic Admin Server console. These same procedures may be repeated to PK Enable other Weblogic hosted applications.

Install the Certification Authorities (CA) Trust Anchors

The most current root certificates must be installed on both servers and workstations. InstallRoot is a utility that manages certificates for DoD and NSS trusted root and intermediate Certification Authorities (CAs) on Microsoft servers and workstations.

Unclassified/NIPRNet systems

Download, install and run the NIPRNet InstallRoot application.

1) Open a web browser, navigate to http://iase.disa.mil/pki-pke, and select *Tools*.
2) Download the latest Windows Installer (MSI) version of InstallRoot under the heading labeled *Trust Store Management*.
3) Execute the InstallRoot installation tool.

   NOTE: Administrative rights are required when installing the InstallRoot application under the C:*Program Files*\ location on the system.

4) Run the tool as an administrator to install the DoD NIPRNet certificates into the Windows/Internet Explorer local machine trust store.

   NOTE: Refer to the *InstallRoot User Guide* for installation and configuration instructions for InstallRoot. This guide is located on the DoD PKE website at http://iase.disa.mil/pki-pke **under *Tools* > *Trust Store Management*.**

Secret/SIPRNet systems:

Download the InstallRoot SIPR Windows Installer to install the SIPRNet/NSS root and intermediate CA certificates. The download is available on SIPRNet URL http://iase.disa.smil.mil/pki-pke/ under *Tools* > *Trust Store Management*. Additional information is available in the *InstallRoot User Guide* in the same location.

Once the tool is downloaded, execute similar steps as mentioned in the above Unclassified/NIPRNet systems section.

Configure Weblogic Trust Keystore

Configuring the Weblogic Trust Keystore requires importing each CA certificate from InstallRoot into the Weblogic Trust keystore that will be in Java Keystore (JKS) format.

1) Under [%Weblogic_HOME%]\user_projects\domains\[%YOUR_DOMAIN%], create a folder named **certstores**.

2) Export the DoD CA certificates using InstallRoot, and import each into a truststore using the following command:

   NOTE: Refer to the *InstallRoot User Guide* for instructions on how to export certificates using the InstallRoot GUI.

   keytool -importcert -file <*ca-cert.cer*> *-alias* <*ca-alias*> *-keystore "[%Weblogic_HOME%]\user_projects\domains\[%YOUR_DOMAIN%] \certstores\truststore.jks"*

   Note: The first time you run this command, keytool will create the truststore.jks file and prompt you to establish and confirm a password for it. For each subsequent import, you will be prompted to provide the file password to allow the import to succeed. When importing Root CA certificates, keytool will display details of the certificate being imported and prompt to trust this certificate. When prompted, verify the certificate information and then type *yes* and press Enter.

   Note: Throughout this guide when executing keytool commands if you receive a message *keytool is not recognized as an internal or external command, operable program or batch file* you may need to specify the full path to the keytool.exe file (e.g., "C:\Program Files\Java\Jre7\bin\keytool.exe").

Server Certificate Installation

In PKI systems, a Certificate Signing Request (CSR) is sent from an applicant to a CA in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the server (such as a distinguished name in the case of an X.509 certificate) and the public key chosen by the applicant. The corresponding private key is not included in the CSR but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the Registration Authority (RA), and the RA may contact the applicant for further information. If the request was authorized, the RA will send the applicant a link to a certificate that has been digitally signed by the CA.

Public Key Cryptography Standard #10 (PKCS#10) defines a format for encoding CSRs for use with X.509. A CSR may be represented as a Base64-encoded PKCS#10 blob, and the Base64 information contained within is part of the data needed to submit the certificate request to a DoD or NSS CA.

Generate Server Certificate Request

1) Use the following command to create the Weblogic Identity keystore:

   Unclassified/NIPRNet Systems:

   *keytool -genkey -alias weblogic -keyalg RSA -keysize 2048 -dname "cn=<server_fqdn>,ou=<org>,ou=**PKI**,ou=DoD,o=U.S. Government,c=US" -keystore "[%Weblogic_HOME%]\user_projects\domains\[%YOUR_DOMAIN%]\certstores\keystore.jks"*

   Secret/SIPRNet Systems:

   keytool -genkey -alias weblogic -keyalg RSA -keysize 2048 -dname "cn=<server_fqdn>,ou=<org>,ou=DoD,ou=NSS,o=U.S. Government,c=US" -keystore "[%Weblogic_HOME%]\user_projects\domains\[%YOUR_DOMAIN%]\certstores\keystore.jks"

   NOTE: Replace <server_fqdn> with the FQDN that will be used to access the admin server and <org> with your organizational unit code (e.g. USA, USN, USMC, USAF, DISA, etc).

2) You will be prompted to enter and confirm a password for the keystore. You will then be prompted to enter and confirm a password for the key with the alias **weblogic** that will act as the server's private key.

3) Now create the CSR using the following command:

keytool –certreq –keyalg RSA –alias weblogic –file "<CSR FILE PATH>\certreq.txt" –keystore "[%Weblogic_HOME%]\user_projects\domains\[%YOUR_DOMAIN%]\certstores\keystore.jks"

NOTE: Replace <CSR FILE PATH> with any chosen file path where you want to create the certificate request. This will create a text file which you will open, copy, and paste into the CSR form in the next section.

Submit Server Certificate Request

After the certificate request has been generated, it must be submitted to the proper CA for approval. DoD PKE has developed guidance on how to properly submit a certificate request. Refer to the DoD PKE reference guide entitled *Obtaining a PKI Certificate for a DoD Server* for guidance on submitting the Certificate Request.

The document can be found on the DoD PKE website at http://iase.disa.mil/pki-pke/(NIPRNET) or http://iase.disa.smil.mil/pki-pke/(SIPRNET) under *PKE A-Z> Guides*.

Retrieve Server Certificate

1) Once the RA has reviewed and approved the request, the requestor will be notified of the approval and provided information on certificate retrieval. Using the browser, navigate to the **CA site** provided and select the **Retrieval** tab.
2) Enter your **request number** in the **Request identifier** field. Click **Submit**.
3) The Request Status window will display information related to the entered Request ID.

   Note: Before downloading your certificate, verify the *Submitted on* date matches your request to ensure you are attempting to retrieve the correct certificate. If this information does not match, confirm the URL you are on matches the one provided for your certificate retrieval.
4) Click the **Issued certificate** (serial number) link.
5) Review the form contents for accuracy. Scroll down to the **Base 64 encoded certificate with CA certificate chain in pkcs7 format** certificate, highlight and copy the **certificate** to the clipboard (including the *-----BEGIN CERTIFICATE-----* and *-----END CERTIFICATE-----)* tags.

   Open a text editor and paste the copied certificate data. Save the file to an easily accessible location. Select **All Files** as the **Save as Type** and save the file with a **.p7b** extension. If the system used for retrieval is different from the server for which the request was generated, the retrieved certificate must be transported to the requesting server via removable media or copied via the network.

Install Server Certificate

1) Use the following command to install the new certificate:

   keytool –import –alias weblogic –file "<P7B FILE PATH>\cert.p7b" –keystore "[%Weblogic_HOME%]\user_projects\domains\[%YOUR_DOMAIN%]\certstores\keystore.jks"

   NOTE: Replace <P7B FILE PATH> with the file path where the certificate was saved in the previous section. If prompted *Install reply anyway,* type *yes* and press Enter.

Configuring Weblogic Security Settings

Once the Weblogic Trust and Identity keystores are properly created and all the required CAs and server certificates are stored; the next step is to configure the security settings inside Weblogic.

Configure Identity and Trust

1) Open Weblogic **Admin Server Console**.
2) From the Home page, click the **Servers** button in the Domain **Configurations > Environment** section**.**
3) From the grid, click **AdminServer**.
4) Under the Configuration main tab, go to the **Keystores** tab.
5) Click **Lock & Edit** from the **Change Center** area in the upper left corner of the webpage. This will enable you to make changes to the Weblogic server configurations.
6) For the **Keystores** setting, click **Change** and select **Custom Identity and Custom Trust.** Then click **Save**.
7) For the **Custom Identity Keystore** setting, enter the path of the Identity Keystore that you created during the **Generate Server Certificate Request** section of this guide. Enter *JKS* for the **Custom Identity Keystore Type** setting. For the **Custom Identity Keystore Passphrase,** enter the password you used to create the keystore in the **Generate Server Certificate Request** section of this guide. Confirm the keystore password in the **Confirm Custom Identity Keystore Passphrase** field.
8) Repeat step 7 for the **Custom Trust Keystore** settings. However, use the path and password from the trust keystore that you created during the **Configure Weblogic Trust Keystore** section of this guide. Also use **JKS** for **Custom Trust Keystore Type.**
9) Click **Save** and click **Activate Changes** from the Change Center.

Configure SSL

1) Open Weblogic **Admin Server Console**.
2) From the Home page, click the **Servers** button in the **Domain Configurations > Environment** section**.**
3) From the grid, click **AdminServer**.
4) Under the Configuration main tab, go to the **SSL** tab.

5) Click **Lock & Edit** from the **Change Center** area in the upper left corner of the webpage. This will enable you to make changes to the Weblogic server configurations.
6) For the **Identity and Trust Locations** setting, click **Change** and select **Keystores**. Then click **Save**.
7) Click the **Advanced** link to open the drop panel that contains additional settings.
8) For the **Two Way Client Cert Behavior** setting, select **Client Certs Requested and Enforced** (this will enable two way SSL). Also check and enable the **Use JSSE SSL** setting.

   NOTE: If running a newer version of Weblogic, the Use JSSE SSL check box may not exist as Weblogic uses JSSE SSL by default.
9) In the **Identity** section, enter *weblogic* (or the alias that you used when creating the server certificate in the **Generate Server Certificate Request** section of this guide) for the **Private Key Alias** setting. Enter and confirm the password you gave while creating the server certificate.
10) Click **Save** and click **Activate Changes** from the Change Center.

Configuring Weblogic Admin Server console port assignments

In order to use certificate authentication, the SSL port must be assigned and enabled for the Admin Server console. In addition, you can choose to disable standard http, and non-secure connections. This will force the users to only connect to the Admin Server console via certificate authentication.

Admin Server Console Port Settings

1) Open the Weblogic **Admin Server Console**.
2) From the Home page, click the **Domain** button in the **Domain Configurations > Domain** section.
3) Click the **Control** tab from the upper tabs group, and from the grid click **AdminServer.**
4) Click **Lock & Edit** from the **Change Center** area in the upper left corner of the webpage. This will enable you to make changes to the Weblogic server configurations.
5) Enable **SSL Listen Port Enabled** and enter a port number of choice for the **SSL Listen Port** setting.
6) If necessary, disable **Listen Port Enabled** to disable standard http connection.
7) Click **Save** and click **Activate Changes** from the Change Center. Restart the Admin Server if necessary.

Once SSL Listen Port has been enabled and assigned, Weblogic will be PK-Enabled. Log out of the admin console and use the SSL connection to test it.

Certificate Revocation Checking

Weblogic provides a default configuration which validates certificates on a domain-wide basis. Revocation checking is disabled by default and must be enabled. Once enabled, it first uses OCSP and then CRLs. Weblogic also provides the option of CA Override which allows you to configure CA-specific CRLs, OCSP, and exception settings.

Enable Default Certificate Revocation Checking

The default configuration will first use OCSP by obtaining the OCSP responder URL from the certificate. It will then create an OCSP response local cache that is provided by the OCSP responder. All certificates will be validated from the created OCSP response local cache. If the certificate has an OCSP status of unknown, Weblogic then uses the CRL local cache to determine the certificate's validity. The CRL local cache is a file-based store that is updated from CRL distribution points obtained from the certificates. If the revocation status is unknown or cannot be determined (e.g. due to network connectivity) after using OCSP and CRL checking, validation by default is considered not failed.

1) Open Weblogic **Admin Server Console**.
2) From the Home page, click the **Domain** button in the **Domain Configurations > Domain** section.
3) Click the **Security** tab from the upper tabs group, and then click the **SSL Certificate Revocation Checking** tab from the lower tabs group.
4) Click **Lock & Edit** from the **Change Center** area in the upper left corner of the webpage. This will enable you to make changes to the Weblogic server configurations.
5) Check **Enable Certificate Revocation Checking** from the **General** sub-tab.
6) Optionally **Fail on Unknown Revocation Status** can be checked to deny access when the certificate revocation status of a certificate cannot be determined. This setting will increase security but could also decrease Weblogic availability if there are issues obtaining revocation data.
7) Click the **Save** button and click **Activate Changes** from the Change Center. Restart the Admin Server if necessary.

Customizing Certificate Revocation Checking Configuration

In addition to the default certificate revocation checking features, you can customize the following settings under the **SSL Certificate Revocation Checking** tab:

- Certificate Revocation (CR) Checking method order

  - The order of CR checking method: OCSP and then CRLs or, vice-versa
- Require certificate revocation status
  - Fails certificate path validation if status is unknown or cannot be determined
- Domain-wide OCSP settings
  - Use of nonces (a random number, when included in an OCSP request, forces a fresh response) in OCSP requests and responses
  - OCSP response cache settings (i.e. capacity, refresh period)
  - OCSP response timeout interval settings
- Domain-wide CRL protocol settings
  - Use of CRL distribution points
  - CRL cache refresh frequency
  - CRL distribution point download timeout interval settings
- Certificate authority overrides.
  - Disable revocation checking for those certificates
  - Change the CR checking method order
  - Automatically fail certificate path validation if revocation status is unknown or unavailable
  - Customize OCSP or CRL settings (except for the CRL local cache settings)
  - Designate the OCSP responder URL to use
  - Designate the CRL distribution point URL to use

Certificate Credential Mapping

Weblogic Server supports mapping user certificates to Weblogic user accounts. This section discusses mapping the Common Name (CN) from the user's certificate to a Weblogic user account with the username matching that of the CN from the certificate. For example, if the certificate CN is DOE.JOHN.1234567890 the weblogic username would also need to be DOE.JOHN.1234567890. There are other ways to do certificate to user account mapping in Weblogic but most require creating a custom Java mapper class.

Configure Identity Asserter

These steps will configure the Weblogic Identity Asserter to use the certificate as the authentication token and map the certificate's CN to the user account. It is assumed the DefaultIdentityAsserter is being used.

1) Open the Weblogic **Admin Server Console.**
2) From the Home page, click the **Security Realms** button in the **Domain Configurations > Your Application's Security Settings** section.
3) Select **<Your-Realm>** from the table.
4) Click the **Providers** tab from the upper tab group, and then click the **Authentication** tab from the lower tab group.
5) Click **Lock & Edit** from the **Change Center** area in the upper left corner of the webpage. This will enable you to make changes to the Weblogic server configurations.
6) Click the **DefaultIdentityAsserter** link. In the next screen, under **Active Types** move **X.509** from the **Available** column to the **Chosen** column. Click **Save.**
7) Click the **Provider Specific** tab.
8) Select **CN** from the **Default User Name Mapper Attribute Type** drop down.
9) Check the box for **Use Default User Name Mapper**.
10) Click the **Save** button and click the **Activate Changes** button from the Change Center**.**
11) Restart the Admin Server.

Create User Accounts

Weblogic user accounts will need created with the account username matching the CN of the user's certificate (e.g., DOE.JOHN.1234567890).

1) Open the Weblogic **Admin Server Console.**

2) From the Home page, click the **Security Realms** button in the **Domain Configurations > Your Application's Security Settings** section.
3) Select **<Your-Realm>** from the table.
4) Click the **Users and Groups** tab from the upper tab group and then click the **Users** tab from the lower tab group.
5) Click the **New** button and enter the CN from the certificate in the **Name** field. Enter and confirm a password for the user.. Click the **OK** button.
6) Click the newly created user from table. Select the **Groups** tab. Add the user to the appropriate groups. Click the **Save** button.

Note: When using certificate credential mapping and logging into the Weblogic Admin Server console using a certificate, the Admin Server's Log Out link may return the user back to their home page and the user may appear to remain logged in. When the Log Out link is clicked, the user is being logged out but the user is automatically authenticated again and returned to their home page based on how the Weblogic Admin Server and the user's web browser behave. In order to properly log out, the user should close the web browser to terminate the session.

Appendix A: Supplemental Information

Website

Please visit the URL below for additional information:

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

Technical Support

Contact technical support:

dodpke@mail.mil

Acronyms

CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DoD	Department of Defense
DoDI	DoD Instruction
FQDN	Fully Qualified Domain Name
JKS	Java Keystore
NSS	National Security Systems
OCSP	Online Certificate Status Protocol
PKCS	Public Key Cryptography Standard
PKE	Public Key Enablement
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Appendix B: References

- Keytool is a JAVA key and certificate management utility. It provides keystore creation, public/private key creation, certificate importing, and various other functionality. Keytool can be found in the *[%JAVA HOME%]\jre\bin* directory. For complete description of Keytool commands and features see *Keytool – Key and Certificate Management Tool* at http://download.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html.
- More information on revocation checking capabilities for the Weblogic Server is available at http://docs.oracle.com/cd/E23943_01/web.1111/e13707/ssl.htm#autoId42