

UNCLASSIFIED



DoD Public Key Enablement (PKE) Reference Guide

Configuring Citrix XenDesktop for Use with DoD PKI

Contact: dodpke@mail.mil

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

Enabling PKI Technology
for DoD users

Configuring Citrix XenDesktop for Use with DoD PKI

25 July 2012

Version 1.1

DoD PKE Team

UNCLASSIFIED

Revision History

Issue Date	Revision	Change Description
01/27/12	1.0	Initial Release
07/25/12	1.1	Updated with comments

Contents

INTRODUCTION	1
PURPOSE.....	1
SCOPE	1
GETTING STARTED	2
BASELINE	2
PREREQUISITES.....	2
CREATING A MASTER VIRTUAL MACHINE	4
CONFIGURING XENDESKTOP 5	5
MANAGEMENT OF THE VIRTUAL DESKTOP AGENT	5
ALLOCATING XENDESKTOP VIRTUAL DESKTOPS.....	5
CONFIGURING SMART CARDS FOR XENDESKTOP V5.....	6
CONFIGURING SECURE SOCKET LAYER (SSL) ON XENDESKTOP CONTROLLERS	6
CONFIGURE THE WEB INTERFACE ON THE XENDESKTOP 5 CONNECTION BROKER	6
SET THE TRUST LEVEL ON THE VDI BROKER FOR XENDESKTOP VERSION 5	6
MANAGING SMART CARD USE	6
XENDESKTOP POLICIES.....	6
CONFIGURING A SMART CARD-CAPABLE CLIENT FOR CONNECTIVITY	7
CONFIGURING SMART CARDS FOR XENAPP V6.....	8
CONFIGURING SECURE SOCKET LAYER (SSL) ON XENAPP CONTROLLERS.....	8
CONFIGURING WEB INTERFACE AND IIS SERVER	8
CONFIGURING IIS MANAGER	8
SET THE TRUST LEVEL ON THE VDI BROKER FOR XENDESKTOP VERSION 5	9
APPENDIX A: SUPPLEMENTAL INFORMATION.....	10
WEB SITE	10
TECHNICAL SUPPORT	10
APPENDIX B: ACRONYMS.....	11
APPENDIX C: REFERENCES.....	12

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 Public Key Infrastructure (PKI). The PKE Reference Guides contain procedures for enabling products and associated technologies to leverage the security services offered by the DoD PKI.

Purpose

This guide provides instructions for configuring Citrix XenDesktop for secure authentication and communications using DoD PKI. It provides details to PK-Enable the Citrix XenDesktop Environment to provision desktops for properly authenticated users.

Scope

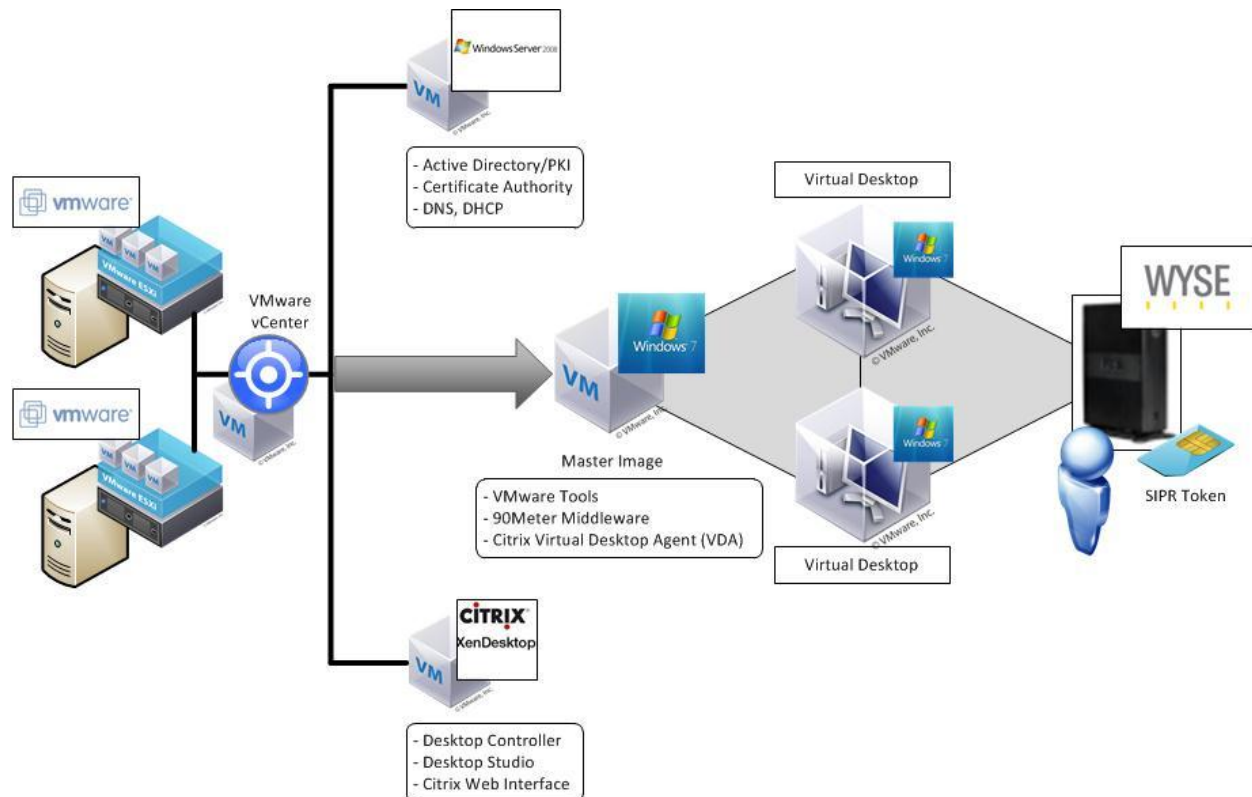
This document is intended for users of PKI technologies in a Citrix XenDesktop environment residing on a VMWare ESXI platform. Experience installing and configuring software on a Citrix XenDesktop platform is useful when reading this guide and related documentation. Experience with XenDesktop configuration is recommended.

Getting Started

Baseline

This guide was developed using Citrix XenDesktop 5.5 with IIS v7 running on VMware ESXi 5.0 serving Windows 7 desktop clients in a Windows 2008 R2 domain. This is an example architecture. There are other virtualization environments and design implementations that can be used to provide secure access to a Virtual Desktop Infrastructure (VDI) using the DoD PKI.

The following diagram represents the example architecture:



Prerequisites

This guide assumes that XenDesktop has been installed and configured for basic connectivity on a VMWare ESXi platform. For instructions on installing and configuring a Citrix XenDesktop environment, refer to the Citrix XenDesktop Administrator's Guide at <http://support.citrix.com/proddocs/topic/xendesktop/cds-library-wrapper-rho.html>. Ensure that the following components are installed and configured as discussed in *Citrix Support Article 129096: How to Configure Smart Cards with the Latest Version of Web Interface and XenApp*:

- The windows domain is configured for Smart Card Logon with DoD PKI credentials. Refer to the *Microsoft Windows Server 2008: Enabling Smart Card Logon* guide and the *Microsoft Windows Server 2003: Enabling Smart Card Logon* guide available from the DoD PKE site at <http://iase.disa.mil/pki-pke> under *For Administrators, Integrators, and Developers > Network Configuration* for detailed instructions.
- The XenDesktop servers acting as VDI brokers and the XenDesktop virtual desktops have the proper middleware installed and patched to the most recent version.
- The latest hotfix or hotfix rollup pack on all XenDesktop servers in the farm is installed.
- The latest version of Web Interface is installed. Refer to the Downloads page of the Citrix website to download the latest version of Web Interface.
- The XenDesktop VDI broker and Web Interface Server (can be the same server or different servers) is a part of the Windows Smart Card Enabled domain.
- The reader has the Administrative privileges necessary to complete the steps in this guide.

Creating a Master Virtual Machine

This section is intended for administrators who are delivering desktops through virtual machines (VMs). In this example architecture, this section is to be performed on the ESXI platform. It describes how to build a base desktop VM.

- 1) In **VMware vCenter**, create a New Virtual Machine and install a **Windows Vista** or **Windows 7** operating system for the **Master Image** for XenDesktop.
- 2) After the installation of the operating system is complete, run **Windows Update** and install all applicable updates on the **New Master Image** for the operating system.
- 3) Install **VMware Tools** onto the **New Master Image**.
- 4) Install **SmartCard** middleware onto the **New Master Image**.
- 5) Install the **Citrix Virtual Desktop Agent (VDA)** onto the **New Master Image**.
- 6) Shutdown the New Master Image. The Master Image will be referenced as the template to deploy XenDesktop virtual desktops.

NOTE: Refer to vendor documentation for individual installation specifics for other vendors and implementation models.

Configuring XenDesktop 5

Management of the Virtual Desktop Agent

Please refer to the section entitled “Active Directory-based Controller Discovery” in the Citrix XenDesktop 5 documentation located in the Citrix eDocs libraryⁱⁱ for further details.

Allocating XenDesktop Virtual Desktops

Please refer to the section entitled “*Creating and Updating Desktop Groups*” in the *Citrix XenDesktop 5 Admin Guide*ⁱⁱⁱ.

NOTE: This will register the virtual desktops (Catalog) with its associated Desktop Group.

Configuring Smart Cards for XenDesktop v5

The following steps leverage the Citrix support article titled “*How to Configure Smart Cards with the Latest Version of Web Interface and XenApp*”ⁱ but are tailored for the DoD PKI.

Configuring Secure Socket Layer (SSL) on XenDesktop Controllers

Refer to the *Citrix XenDesktop 5* documentation referencing *Configuring SSL on XenDesktop* located in the Citrix eDocs Library for additional information.

Configure the Web Interface on the XenDesktop 5 Connection Broker

- 1) Perform the steps in the Microsoft IIS 7.0: Public Key Enabling guide available from the DoD PKE website at <http://iase.disa.mil/pki-pke> under *For Administrators, Integrators and Developers > Web Servers* to PK-enable the IIS instance hosting the Virtual Desktop Broker web interface.
- 2) Create a XenApp Web Site and ensure that you select the option **At Web Interface** to indicate where the user authentication takes place. For XenApp Services Site, the authentication is always done using the Web Interface.

Set the trust level on the VDI Broker for XenDesktop Version 5

For XenDesktop Version 5 perform these steps on the Virtual Desktop Broker:

- 1) Open PowerShell on the DDC (this is the server configured as the Connection or Virtual Desktop Broker).
- 2) Run the command:

```
Add-PSSnapin Citrix.*
```

to add the Citrix modules.
- 3) Run the command:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Managing Smart Card Use

Refer to the Citrix XenDesktop 5 documentation located in the Citrix eDocs library for additional information on managing smart card use.

XenDesktop Policies

- 1) In the Desktop Controller, launch Desktop Studio and select **Access** in the left pane. Expand **Access**, then expand **Citrix Web Interface**.

- 2) Select **XenApp Web Sites** in the left pane and select the **Site name** (e.g. Internal Site) in the right pane which corresponds to the Desktop Web services (https://<FQDN>/Citrix/DesktopWeb).
- 3) Right-click on the site and select **Authentication Methods**.
- 4) In Configure Authentication Methods, select check boxes **Pass-through with smart card** and **Smart card**. Click **OK**.
- 5) In left pane, select **XenApp Services Sites** and select Site name **PNAgent Site**.
- 6) Right-click on the site and select **Authentication Methods**.
- 7) In Configure Authentication Methods, select check boxes **Pass-through with smart card** and **Smart card**. Click **OK**.

Configuring a Smart Card-Capable Client for Connectivity

To configure a client machine containing a card reader with a Smart Card inserted, complete the following procedure:

- 1) For Smart Card authentication, add the XenApp Web Site or Services site as a Trusted site.
- 2) For Pass-through with Smart Card authentication:
 - a. Add the XenApp Web Site or Services site as a Local Intranet site.
 - b. Ensure that the following components are installed on the computer:
 - Citrix Online Plugin Full (available for download from the Citrix Downloads page^{iv}).
 - The icaclient.adm template^v, configured with the following options:
 - Allow Smart card authentication
 - Use pass-through authentication for PIN

Configuring Smart Cards for XenApp v6

Prior to PK enabling XenApp, ensure the following prerequisites have been met:

- Domain configured to support Smart Card authentication
- The XenApp servers acting as XML brokers have Smart Card middleware installed
- Web Interface is installed and is part of a Windows domain

Configuring Secure Socket Layer (SSL) on XenApp Controllers

Refer to the *Citrix XenApp 6.5* documentation referencing *Configuring SSL on XenApp* located in the Citrix eDocs Library for additional information.

Configuring Web Interface and IIS Server

- 1) Install a server certificate on the IIS site hosting the XenApp Web Site for Smart Card authentication as described in the DoD PKE Public Key Enabling Microsoft IIS 7.0/7.5 Server guide^{vi}.
- 2) Install the Root and intermediate certificates on the IIS server using the DoD PKE InstallRoot utility as referenced in the InstallRoot User Guide^{vii}.
- 3) Create a XenApp Web Site and ensure that you select the option **At Web Interface** to indicate where the user authentication takes place.
- 4) Select the **Smart Card** or the **Pass-through with Smart Card** authentication method.

Configuring IIS Manager

- 1) To configure Web Server Roles, complete the following steps:
 - a. On the XenApp server, open Server Manager and navigate to the Web Server role services.
 - b. Add the role service **Client Certificate Mapping Authentication** and complete wizard.
 - c. Navigate to IIS Manager and select the **XenApp server name**.
 - d. Select the **Authentication** option.
 - e. Enable the **Active Directory Client Certificate Authentication** option and click **OK**.
- 2) To configuring Smart Card Authentication, complete the following steps:
 - a. Navigate to **IIS Manager** and select the **XenApp server name**.

- b. Select the **SSL Settings** option.
- c. In the properties page for SSL Settings, check **Require SSL** and **Accept from the Client certificates** option.

Set the trust level on the VDI Broker for XenDesktop Version 5

For XenDesktop Version 5 perform these steps on the Virtual Desktop Broker:

- 1) Open PowerShell on the DDC (this is the server configured as the Connection or Virtual Desktop Broker).
- 2) Run the command:
`Add-PSSnapin Citrix.*`
to add the Citrix modules.
- 3) Run the command:
`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`

Appendix A: Supplemental Information

Web Site

Please visit the URL below for additional information.

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

Technical Support

Contact technical support at the email address below.

dodpke@mail.mil

Appendix B: Acronyms

DDC	Desktop Delivery Controller
DoD	Department of Defense
FQDN	Fully Qualified Domain Name
IIS	Internet Information Services
PKE	Public Key Enablement
PKI	Public Key Infrastructure
SSL	Secure Socket Layer
URL	Uniform Resource Locator
VDA	Virtual Desktop Agent
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine

Appendix C: References

The resources below were used to help develop the content of this document.

-
- (i) "How to Configure Smart Cards with the Latest Version of Web Interface and XenApp," <http://support.citrix.com/article/CTX129096>.
 - (ii) "Citrix E-Docs Library," <http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-landing-page-xd5fp1.html>.
 - (iii) "Citrix XenDesktop Administrator's Guide," <http://support.citrix.com/servlet/KbServlet/download/19149-102-19637/XDAdminGuide.pdf>.
 - (iv) "Citrix Online Downloads: Online Plug-in for Windows 12.1," <http://www.citrix.com/English/ss/downloads/details.asp?downloadId=2304987&productId=186>.
 - (v) "How to Configure Version 10.x of the Presentation Server Client Using the Icaclient.adm Template," <http://support.citrix.com/article/CTX112957>.
 - (vi) "DoD Public Key Enablement (PKE) Reference GuidePublic Key Enabling Microsoft IIS 7.0/7.5 Server," https://powhatan.iie.disa.mil/pki-pke/function_pages/a-z.html.
 - (vii) "InstallRoot User Guide," http://iase.disa.mil/pki-pke/function_pages/tools.html.