DoD Public Key Enablement (PKE) Reference Guide

Configuring HP ThinPro Thin Clients for Use with the SIPRNet Token

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

Enabling PKI Technology for DoD users

Configuring HP ThinPro Thin Clients for Use with the SIPRNet Token

17 December 2013

Version 1.0

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
12/17/13	1.0	Initial release

Contents

INTRODUCTION **1**

PURPOSE 1
SCOPE 1

GETTING STARTED **2**

BASELINE ENVIRONMENT 2
PREREQUISITES 2
Smart Card Logon *2*
Microsoft Remote Desktop Services (RDS) Environment *2*

CONFIGURING HP THINPRO ZERO CLIENTS WITH THE SIPRNET HARDWARE TOKEN **4**

CONNECTING TO A VMWARE VIEW VDI ENVIRONMENT 4
CONNECTING TO A CITRIX XENDESKTOP VDI ENVIRONMENT 5

APPENDIX A: SUPPORT INFORMATION **7**

WEBSITE 7
TECHNICAL SUPPORT 7
ACRONYMS 7

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 thin clients that utilize the HP ThinPro operating system. This guide details how to configure the HP ThinPro to function with the Secret Internet Protocol Routing Network (SIPRNet) hardware token and how to perform smart card logon (SCL) to a Microsoft Remote Desktop Protocol (RDP) backend environment, a VMWare View backend environment, and a Citrix XenDesktop backend environment.

Scope

This document provides instructions for configuring HP thin clients that leverage the proprietary HP ThinPro operating system. It is intended for users possessing some experience with installing and configuring software on HP thin client platforms. Familiarity with thin client technology is useful. Administrative privileges will be required.

Getting Started

At present, hardware and software zero clients are in use and growing in popularity throughout the DoD community. These devices enable easy maintenance, management, and securing of the computing environment without many of the vulnerabilities of a personal computer. Significant efforts are underway to enable these thin and zero clients for use with the new SIPRNet hardware token. This configuration guide details how to enable the thin clients to read and perform SCL with the SIPRNet hardware token.

Baseline Environment

The instructions in this guide were developed using the following environment configuration:

- HP T510 with HP Smart Zero 4.2 build 19 or later
- Windows RDS version 7.0 on a Windows Server 2008 R2 server farm in a Windows 2008 R2 domain
- VMWare ESX and View 5
- Citrix XenDesktop 5

Prerequisites

Smart Card Logon

Smart card logon has been configured for the domain. For details on configuration, refer to the appropriate version of the *Microsoft Enabling Smart Card Logon* guides available from the DoD PKE site at http://iase.disa.mil/pki-pke under *For Administrators, Integrators, and Developers* > *Network Configuration.*

Microsoft Remote Desktop Services (RDS) Environment

A Microsoft Remote Desktop Services (RDS) environment has been set up to provision desktops to thin and zero clients and enabled for SCL. Reference the DoD PKE *Microsoft Remote Desktop Services: Configuring Secure Authentication* guide located at http://iase.disa.mil/pki-pke under *For Administrators, Integrators, and Developers* > *Thin Clients and Virtualization* for proper implementation.

Citrix XenDesktop Environment

A XenDesktop environment has been PK-enabled according to the *Configuring Citrix XenDesktop for Use with DoD PKI,* located at http://iase.disa.mil/pki-pke under *For Administrators, Integrators, and Developers* > *Thin Clients and Virtualization*. The XenDesktop servers are configured as VDI brokers and the XenDesktop virtual

desktops have the proper middleware installed (90 Meter SCM) and patched to the most recent version.

VMWare View Environment

A VMWare environment has been PK-enabled according to *Configuring VMware View for Use with DoD PKI* located at http://iase.disa.mil/pki-pke under *For Administrators, Integrators, and Developers* > *Thin Clients and Virtualization*. The View servers are configured as VDI brokers and the VMWare virtual desktops have the proper middleware installed (90Meter SCM) and patched to the most recent version.

Configuring HP ThinPro Zero Clients with the SIPRNet Hardware Token

Perform the following steps to configure the HP ThinPro thin client to function with the SIPRNet hardware token.

NOTE: This guide is for HP ThinPro devices that come with the HP Smart Zero 4.2 build 19 or later. OS builds prior to that are not compatible with the SIPRNet hardware token. For details on purchasing new HP thin clients, consult your HP vendor documentation.

Connecting to a Microsoft Windows RDP VDI Environment

1) Boot up the HP ThinPro device.
2) At the initial bootup screen, click the **wrench** to display the **Configuration Options**.
3) In the Configuration Options screen, click **Administrator/User Mode Switch.**
4) In the dialogue box, enter the **admin password;** this password can be acquired from your vendor documentation.
5) Click the **RDP7** button to create an RDP connection.
6) In the **Remote Connection Server** text box, enter the **server name** or **address** of the RDP session server and click **OK**.
7) Click the **Smart Card Login** check box and click **Connect**.

Connecting to a VMWare View VDI Environment

1) Boot up the HP ThinPro device.
2) At the initial bootup screen, click the **wrench** to display the **Configuration Options.**
3) In the Configuration Options screen, click **Administrator/User Mode Switch**.
4) In the dialogue box, enter the **admin password,** this can be acquired from your vendor documentation.
5) Click the **VMWare View** button to create a PCoIP connection.
6) In the **Remote Connection Server** text box, enter the **server name** or **address** of the VMWare View Connection Broker and click **OK**.
7) Click the **Smart Card Login** check box and click **Connect**.

Connecting to a Citrix XenDesktop VDI Environment

1) Boot up the HP ThinPro device.
2) At the initial bootup screen, click the **wrench** to display the **Configuration Options**.
3) In the Configuration Options screen, click **Administrator/User Mode Switch**.
4) In the dialogue box, enter the **admin password,** this can be acquired from your vendor documentation.
5) Open an **xterm**.
6) Navigate to **/home.**

   cd /home
7) Download the **firefox_4.2.0.17953 Web Browser Kit**.

   NOTE: This can be attained from your HP Vendor.
8) Copy the **KIT-WEBBROWSER.xar** to the thin client .

   cp KIT-WEBBROWSER.xar /home
9) Transfer the **KIT-WEBBROWSER.xar** to **/home**.
10) Run **xarinstall KIT-WEBBROWSER.xar**.
11) Reboot after this is completed.
12) At the initial bootup screen, click the **wrench** to display the **Configuration Options.**
13) In the Configuration Options screen, click **Administrator/User Mode Switch**.
14) In the dialogue box, enter the **admin password;** this can be acquired from your vendor documentation.
15) Open an **xterm**.
16) Move the xterm aside and create the web browser connection in the UI.
17) Run **regeditor** in the xterm.
18) Browse to **Root > ConnectionType > Firefox > Connections > [$UUID of connection]**.
19) Change **fullscreen** value from 1 to **0** and click **Save**.
20) Browse to **Root > ConnectionType > Firefox > General**.
21) Change **enableUserChanges** from 0 to **1** and click **Save**.
22) Quit regeditor .

23) Start your web browser connection.
24) Load relevant certificates into Firefox. (Every CA certificate that is required for connecting to the XenDesktop Connection Broker is required.)
25) Power off the unit completely.
26) Boot up the HP ThinPro device.
27) At the initial bootup screen, click the **Web Browser**.
28) Enter the **Web Browser server name** of the Citrix XenDesktop Connection Broker to create a connection to the VDI backend.
29) Click **Start**.
30) In the **Logon Type** drop down, click **Smart Card** and click **Logon**.
31) In the Authentication window, type the **PIN** of the smartcard.
32) At the User Identification Request box, click **OK**.
33) Click the **XenDesktop Monitor** icon.

Appendix A: Support Information

Website

Please visit the URLs below for additional information.

NIPRNet: http://iase.disa.mil/pki-pke
SIPRNet: http://iase.disa.smil.mil/pki-pke

Technical Support

Contact technical support at the email address below.
dodpke@mail.mil

Acronyms

DoD	Department of Defense
HP	Hewlett Packard
OS	Operating System
PIN	Personal Identification Number
PKE	Public Key Enablement
PKI	Public Key Infrastructure
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
SCL	Smart Card Logon
SIPRNet	Secret Internet Protocol Routing Network