Enabling Smart Card Login for Linux using Centrify 2012.4

UNCLASSIFIED

Revision History

<table>
<thead>
<tr>
<th>Issue Date</th>
<th>Revision</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/14/12</td>
<td>1.0</td>
<td>Initial Document Developed</td>
</tr>
<tr>
<td>4/18/2013</td>
<td>1.1</td>
<td>Modified order of steps based on comments</td>
</tr>
<tr>
<td>2/12/2014</td>
<td>1.2</td>
<td>Updated to specify Centrify Suite 2012.4</td>
</tr>
</tbody>
</table>
# Contents

**INTRODUCTION** ........................................................................................................... 1  
- Purpose ....................................................................................................................... 1  
- Scope ......................................................................................................................... 1  
**BACKGROUND** ......................................................................................................... 2  
**PLANNING AND PREPARATION** .................................................................................. 3  
**CENTRIFY SUITE INSTALLATION** ................................................................................ 4  
- Installation of Centrify DirectManage ........................................................................ 4  
- Install DirectControl Agent on Linux System .............................................................. 5  
**CENTRIFY SUITE CONFIGURATION** .......................................................................... 6  
- Active Directory Configuration to Support Centrify .................................................... 6  
- Configuring DirectControl Administration Console .................................................. 6  
- Creating a Zone in Centrify ....................................................................................... 7  
- Creating Linux Groups ............................................................................................ 8  
- Zone Provisioning .................................................................................................... 9  
- Centrify Group Configuration .................................................................................. 10  
**JOINING LINUX SYSTEM TO DOMAIN** ................................................................... 12  
- Joining Linux System to Domain ............................................................................. 12  
- Test Linux Logon Using Active Directory Credentials ........................................... 12  
**ENABLING SMART CARD LOGON ON LINUX SYSTEMS** ........................................... 13  
- Enabling Smart Card Support on Linux Systems ..................................................... 13  
**CENTRIFY GROUP POLICY CHANGES** ..................................................................... 14  
- Setting Centrify Group Policy .................................................................................. 14  
**APPENDIX A - ENABLING SMART CARD LOGIN FOR ACTIVE DIRECTORY USER ACCOUNTS** .................................................................................................................. 15  
- User Accounts ......................................................................................................... 15  
- Manually Remapping Existing Users Who Currently Authenticate Via Username/Password .................................................................................................................. 15  
- Manually Creating New Users .................................................................................. 16  
**APPENDIX B: CENTRIFY KNOWN ISSUES** ................................................................. 18  
- Issue with Screen Saver Lockout on RHEL 5 and CentOS 5 ...................................... 18  
**APPENDIX C: ACRONYMS AND ABBREVIATIONS** ...................................................... 19  
**APPENDIX D: SUPPORT AND INFORMATION** .......................................................... 20  
- Website .................................................................................................................... 20  
- Technical Support .................................................................................................... 20  
**APPENDIX E: REFERENCES** ...................................................................................... 21
Introduction

The DoD Public Key Enablement (PKE) Reference Guides (RGs) are developed to help organizations 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 procedures in this document guide the reader in configuring Linux for Smart Card Login (SCL) using the Centrify Suite 2012.4. The information provided is a guide based on DoD best practices; however, users should consult with their organization’s PKI help desk to determine organization-specific guidelines.

Scope

This document is intended for all users of PKI technologies. No in-depth knowledge of PKI is required. Some experience installing and configuring software on Linux and Windows platforms is helpful when reading this guide. Administrative privileges will be required. It is assumed that there is already an established Active Directory domain configured for smart card logon using one of the DoD PKE guides for enabling smart card logon on Microsoft Windows Server. Please refer to the appropriate Microsoft Windows Enabling Smart Card Logon guide in the PKE A-Z section of the DoD PKE Engineering website at - http://iase.disa.mil/pki-pke.
Background

Smart card logon provides a cryptographic based logon method using DoD PKI keys and certificates. This logon method is a two factor authentication mechanism using something you have, the smart card, and something you know, the smart card PIN.

As part of the DoD Instruction (DoDI) 8520.02 requirement to properly secure DoD information systems and networks, the enterprise must public key enable network access. This requires that all local and remote access be authenticated using approved DoD PKI credentials. This may require deployment of new hardware and software, and requires special configuration of Active Directory and other remote access technologies such as Virtual Private Networks (VPNs), if deployed.

The Centrify Suite provides capabilities for smart card-based cryptographic logon for Linux systems. However, implementing Common Access Card (CAC)-based and Secure Internet Protocol Router Network (SIPRNet) hardware token-based authentication using DoD PKI will require additional planning and poses additional challenges during both the implementation and following maintenance phases.
Planning and Preparation

Centrify has several versions of their product, but the free Express version does not support smart card logon. The standard version or higher is required for Linux smart card logon and should be obtained through your local procurement office. This guide was written using Centrify Suite 2012.4, which is the first version of the Suite to support smart card logon. Note, during testing of the 2012.5 version of the Suite it was noticed there is an issue preventing smart card logon from working with this version. For this reason it is recommended to use the 2012.4 version and not 2012.5. The Centrify Suite of software requires the Active Directory domain controller to be running Windows Server 2003 R2 or later. This is required because the Active Directory domain controller must support IETF RFC 2307ii, which was first introduced in Windows Server 2003 R2. The Centrify software will require new containers be created in Active Directory for storing items such as licenses, zone information, and separating Linux computers and users from Windows. Please see the Centrify Suite Admin Guideiii for more information on new containers and for an explanation of zones. Proper planning of the Organizational Unit (OU) structure required should be done before starting installation. For more information visit http://www.centrify.com.

This document is written with general Linux instructions but not all versions of Linux may be supported by Centrify. Please refer to guidance from Centrify for a complete list of support Linux distributions.

On Windows Server 2012 Active Directory domain controllers please install the .NET Framework 3.5 Features through Add Roles and Features before proceeding with this guide.
Centrify Suite Installation

The first step in installing the Centrify Suite is to install the DirectManage tool. This is a utility that must be installed on a Windows system. DirectManage can be installed on a domain controller or a separate Windows workstation used for management tasks. Due to its interaction with the domain controller installing DirectManage on the domain controller is the recommended way to proceed. After DirectManage is installed then the DirectControl agent needs to be installed on the Linux system.

Installation of Centrify DirectManage

These steps should be performed on the Windows system where DirectManage will be installed.

1) Obtain the Centrify Suite Enterprise Edition 32-bit or 64-bit installer depending on the Windows system you are installing it on. If the installer is in a zip format, extract everything from the zip file.

2) Execute the autorun.exe file by double clicking it. For Windows Vista or 7 right-click the installation file and click Run as Administrator. Enter logon credentials if prompted.

3) In the Centrify window under Install Centrify Suite Enterprise Edition, double click Centrify DirectManage.

4) In the Centrify DirectManage Installation window, click Next to proceed.

5) On the Review License Agreement screen, select the I agree to these terms radio button and then click Next to proceed.

6) On the User Registration screen, enter your Name and Company Name, then click Next to proceed.

7) On the Select Components screen, click the check boxes next to the components you want to install to highlight them. Centrify recommends selecting all the components. Click Next to proceed.

8) On the Choose Destination Folder screen, leave the default value or select a different location if required, then click Next to proceed.

9) On the Disable Publisher Evidence Verification screen, it is recommended to uncheck the disable verification box and click Next to proceed. Note, that having publisher evidence verification enabled could slow down startup especially on systems which are not connected to the internet.

10) On the Confirm Installation Settings screen, verify the settings, then click Next to proceed.

11) On the Setup Complete screen, click Finish to end the installation.
Install DirectControl Agent on Linux System

These steps will outline the procedure to install the DirectControl agent on the Linux system. The procedure documented is the manual installation method, Centrify also has a Deployment Manager installation method which can identify Linux machines on the network and push the DirectControl agent to them. The Deployment Manager method might be a better choice if there are many systems that require the agent. See the Centrify Suite Admin Guide, available in the Centrify Support site at [http://www.centrify.com/](http://www.centrify.com/), for more information on the Deployment Manager installation method. Before executing these steps, the Linux system should have its network configuration completed and be able to access the DNS server and domain controller.

1) Obtain the Centrify DirectControl Agent for the Linux operating system being used and copy to Linux system. If necessary extract the installation package (ex: tar xzvf <package-name>.tgz).

2) In a Linux Terminal, change to the directory where the installation package was extracted and then execute the installation script by running /bin/sh ./install.sh as the root user.

3) The Centrify DirectControl Agent installation will execute the Centrify adcheck utility which verifies the system is ready for DirectControl installation. If there are any failures from adcheck they should be addressed before proceeding with installation. When prompted to proceed with installation, type E to proceed with Enterprise installation and press Enter if there are no failures to address.

4) When prompted to run adcheck, type Y and press Enter.

5) When prompted to enter the Active Directory domain to check, type the name of your domain (ex: pke.mil) and press Enter.

6) When prompted to join and Active Directory domain type N and press Enter.

   NOTE: The Linux system will be joined to the domain later in the process and should not be joined at this time.

7) The installation script will let you verify the choices you selected. If everything is correct type Y and press Enter to continue.

8) The installation script will now attempt to install the DirectControl agent. It should state that Install.sh completed successfully if installation was successful.

   NOTE: You may see a warning that adcheck exited with warning(s) which can happen and should not impact installation. If adcheck exits with failures that will impact installation and should be investigated.

9) The Linux system should now be rebooted.
Centrify Suite Configuration

Active Directory Configuration to support Centrify

These steps will be executed on the domain controller to prepare for the Linux systems and users. It is recommended to create a separate container (OU) for Linux systems, groups, and users. These steps will be different depending on the domain configuration for your environment. Please ensure proper planning is done before proceeding.

1) Launch Active Directory Users and Groups, navigate to Start > Programs > Administrative Tools > Active Directory Users and Computers.

2) Expand the domain and create new OUs as required by your organization. A new OU can be created by right-clicking the domain and selecting New > Organizational Unit. Then enter the name of the new OU in the New Object window and click OK to create the new OU. Repeat as required to create additional OUs for your environment.

An example setup might be to create an OU named “Linux” and under that OU create OUs for Service Accounts, Linux Groups, and Linux Servers.

Configuring DirectControl Administration Console

These steps will be performed on the Windows machine where the Centrify DirectManage software was installed earlier in the installation section.

1) Open the DirectControl Administration Console, click Start > All Programs > Centrify > DirectControl > Centrify DirectControl.

2) At the Connect to Forest window, specify the domain controller. If you are not logged in as an administrator, click the Connect as another user check box and enter the user name and password for a domain admin account. If you are logged in as an administrator, do not click the Connect as another user check box. Click OK.

3) At the Welcome to the Centrify DirectControl Setup Wizard screen, click Next to proceed.

4) If the User Credentials screen appears, leave use currently connected user credentials selected and click Next.

5) At the Install Licenses screen, you must specify where Centrify should create the Active Directory container to store licenses. Click Browse to find a location. It is recommended you choose a location under the new OU container you created in the previous section. In the Browse for Container window, select the previously created OU (ex: Linux) and then click Create. In the Create New Object screen, leave the Type as container and in the Name field enter a name for the new container (ex: Licenses). Then click OK to create the new container. Back at the
Browse for Container window, select the newly created container (ex: Licenses) and then click OK. Back at the Install Licenses window, verify the License container location (ex: pke.mil\Linux\Licenses)and click Next to proceed.

6) You may see a window the states All the user accounts in this AD forest will be granted Read properties permission on container … Click Yes to continue.

7) At the Install License Key screen, if you have a license from Centrify enter the license key and click the Add button, or click the Import button and find the license file then click Open. Click Next to proceed.

8) At the Default Container for Zones screen, ensure the Create default zone container box is checked then click the Browse button. In the Browse for Container window, select the previously created OU (ex: Linux) and then click Create. In the Create New Object screen, leave the Type as container, and in the Name field enter a name for the new container (ex: Zones). Then click OK to create the new container. Back at the Browse for Container window, select the newly created container (ex: Zones) and then click OK. Back at the Default Container for Zones window, verify the Zone container location (ex: pke.mil\Linux\Zones)and click Next to proceed.

9) At the Delegate Permission screen, it is recommended to leave the check box selected and click Next to proceed.

10) At the Register the AD Administrative Notification Handler screen, it is recommended to click the check box to select it and click Next to proceed. This will allow the system to automatically maintain the integrity of the data stored in the Centrify Unix profiles.

11) At the Setup Property Pages screen, it is recommended to leave the box unchecked and click Next to proceed. Without this activated, the DirectControl property pages will still be available in AD Users and Computers. If you want the property pages available from all AD administration screens, check the box to enable the profile property pages.

12) At the Summary screen, click Next to proceed.

13) At the Completing the Centrify DirectControl Setup Wizard screen, click Finish.

Creating a Zone in Centrify

Centrify DirectControl requires that either at least one zone be created manually or that Auto Zone be used. Because Auto Zone allows every AD user and group to become valid users and groups for the joined Linux system, Auto Zone is not recommended for most environments. The zone layout should be planned ahead of time before software installation. Please see the Centrify Suite Admin guide for an explanation of zones. These steps contain the general procedures for creating a zone.
1) Open the Centrify DirectControl Administartion Console if it is not already open. Click Start > All Programs > Centrify > DirectControl > Centrify DirectControl.

2) At the Connect to Forest window, specify the domain controller then click the Connect as another user check box. Enter the user name and password for a domain admin account. Click OK.

3) Expand Console Root > Centrify DirectControl and right-click Zones. Select Create New Zone.

4) At the Specify Zone Properties window, complete the Zone name and Description fields and leave Container as the selected Object Type. The Domain controller field can be completed with the master domain controller for this zone to avoid UID and GID conflicts later on by using different domain controllers to add users and groups to a zone. Click Next to proceed.

5) At the Agent Compatibility screen, leave I want a hierarchical zone option selected and click Next to proceed.

6) At the Specify Zone Storage Model screen, leave the Standard zone option selected and click Next to proceed.

7) At the Finish Add Zone screen, click Finish to proceed.

8) Create additional zones as required.

Creating Linux Groups

This section will create a group for Linux users and add members to the group. It is recommend this group be created under the OU container created in the Active Directory Configuration to Support Centrify section. An example location for this new group is pke.mil\Linux\Linux Groups.


2) Expand the domain and find the OU created for the Linux data. Under that OU, find the OU for Linux groups (ex: pke.mil\Linux\Linux Groups). Right-click the OU for the Linux groups and select New > Group.

3) Enter a name for the group (ex: Linux Users) in the Group name field. The other fields can be left at the default values. Click OK to create the new group.

4) In the right-hand pane of the Active Directory Users and Computers window, select the newly created group. Then right-click and select Properties.

5) Click the Members tab of the group properties window and add members to the group. When done adding members click OK.
Zone Provisioning

These steps will perform zone provisioning for the desired zone created previously. This section is only necessary if auto provisioning will be used. If all accounts will be configured manually or in some other way, these steps will not be required. See the Centrify Admin Guide for more information.

1) In the Centrify DirectControl Administration Console, expand **Console Root > Centrify DirectControl > Zones**. Right-click the zone where you want to add the Linux users and select **Properties**.

2) In the zone properties window, select the **Provisioning** tab.

3) Click the **Enable auto-provisioning for user profiles** check box.

4) For Source group, click the button to find the group. In the Find groups window; in the **Name** field type the name of the group where Linux users will be included and click **Find Now**. Highlight the group at the bottom of the window and click **OK**. For the **Shell** field, enter `%{shell}`. In the **Home directory** field, enter `%{home}/%{user}`. In the **GECOS** field, enter `%{u:displayname},%{u:department},%{u:telephonenumber}`. These values can be different for each environment. The screenshot below shows the values noted in this step.

5) If a window appears stating **This zone is now auto-provisioned and any existing UNIX profiles may be deleted**, click **OK** to continue.
6) Open the Zone Provisioning Agent and click Start > All Programs > Centrify > Zone Provisioning Agent > Zone Provisioning Agent Configuration.

7) At the Centrify Zone Provisioning Agent Configuration Panel window, under Polling interval the recommended value is 10 minutes. Change to the desired value.

8) Under Event log, the recommended option is Write the UNIX profiles for the provisioned users and groups to the Event Log. Select this option using the radio button.

9) Under Service account, enter the account name and password for a delegated service account with permissions to run as a service, and create and delete UNIX profiles in the global zone.

10) Click the Apply button and then click the Start button.

11) Click the Close button.

12) Open the Services Snap-In by clicking Start > Programs > Administrative Tools > Services.

13) Verify the Centrify Zone Provisioning Agent service has a startup type of Automatic. If it is not set to Automatic double click the service and change the Startup Type to Automatic. Then click OK and close the Services Snap-In.

**Centrify Group Configuration**

This section will create the group within Centrify and configure it to allow login to the Linux system.

1) On the Windows system with Centrify DirectControl Administration Console, open the console, and click Start > All Programs > Centrify > DirectControl > Centrify DirectControl. If prompted enter the userid and password.

2) Expand Console Root > Centrify DirectControl > Zones > [zone name] > UNIX Data.

3) Right-click Groups and select Create UNIX Group.

4) In the Name field, type the name of the group previously created in step 3 of the Creating Linux Groups section and click Find Now. Highlight the group at the bottom of the screen and click OK.

5) At the Set UNIX Group Profile window, click the check box beside GID and enter a value that will be used as the Linux Group ID for this group. Click the check box beside UNIX group name and enter a name that will be used as the Linux group name for this group. Leave the Users are required to be a member of this group box unchecked. Click OK.

7) Right-click Role Assignments and select Add Group.

8) In the Name field, type the name of the group previously created in step 3 of the Creating Linux Groups section and click Find Now. Highlight the group at the bottom of the screen and click OK.

9) At the Add Access group window, click Browse beside the Role field. Select the login role and click OK. Then click OK again.
Joining Linux System to Domain

This section will join the Linux system to the domain and test to confirm userid/password login is working.

Joining Linux System to Domain

These steps should be performed on the Linux system.

1) Open a terminal window and become the root user `su -`. Enter the root user password when prompted and press `Enter`.

2) Execute the `adjoin` command to join domain, `adjoin [domain] -z [zone-name] -c [container] -u [account]`. Where `[domain]` is the name of the Active Directory domain, `[zone-name]` is the name of the Centrify zone created earlier in this guide, `[container]` is the name of the Active Directory OU created earlier to hold the Linux systems (ex: `pke.mil/Linux/Linux Servers`), and `[account]` is the Active Directory account with privileges to join a system to the domain. Example command: `adjoin pke.mil -z Global -c "pke.mil/Linux/Linux Servers" -u Administrator`. Press `Enter` to execute the `adjoin` command.

3) When prompted, enter the password for the AD user specified in the `adjoin` command from step 2. Press `Enter`.

4) The `adjoin` command should finish successfully stating you have joined the Active Directory domain.

5) Reboot the Linux system.

Test Linux Logon Using Active Directory Credentials

These steps will test logging on to the Linux system using a userid and password for an Active Directory user account. It is recommended to perform these steps from a test system using a test account when possible.

1) At the `Linux Username` login prompt, enter the username for an Active Directory user account that was added to the Linux group in the section `Creating and Configuring Linux Groups`. Then enter the password for the same Active Directory user account and attempt to log in.

2) The system should allow you to log in and the user’s home directory should be `/home/user` as specified in the zone provisioning section earlier in this guide.
Enabling Smart Card Logon on Linux Systems

This section will go through the required steps to get smart card logon working on the Linux system. Note that RHEL 6 will most likely need smart card packages installed prior to proceeding with enabling smart card support. This is noted in the Centrify Smart Card Configuration Guide. See the guide for more details. This section assumes that Active Directory user accounts have already been configured for smart card logon (see Appendix A) and the account that will be tested was added to the Linux Users group earlier in the Creating and Configuring Linux Groups section.

Enabling Smart Card Support on Linux Systems

These steps must be performed on the Linux system to enable Centrify Smart Card support.

1) Open a terminal window and become the root user `su -`. Enter the root user password when prompted and press `Enter`.

2) Execute `sctool` to enable smart card support, `sctool -e`.

3) Verify smart card support was successfully enabled with `sctool -s`. The command should return a message stating that smart card support is enabled.

4) Log out of the system and notice the login screen should now show a note about inserting your Smart card or entering your username. Insert the CAC into the card reader.

5) The login prompt should prompt for the Smart card PIN. Type the PIN and press `Enter`. The system login using the smart card should be successful.
Centrify Group Policy Changes

The Centrify software allows for group policy to be applied to the Linux systems. Items such as certificate revocation checking, smart card removal behavior, and login settings can be configured using group policy.

Setting Centrify Group Policy

These steps contain general instructions for creating and configuring a Group Policy Object.

1) From the Windows system where Centrify DirectManage was installed, open the Group Policy Management console and click Start > Administrative Tools > Group Policy Management.

2) Find the location where you would like the GPO created (ex: Forest > Domains > pke.mil > Linux). Right-click the location and select Create a GPO in this domain, and Link it here.

3) In the New GPO window, type a name for the GPO (ex: Centrify Linux SCL) and click OK.

4) On the right side of the Group Policy Management console, you should see the newly created GPO. Right-click the GPO and select Edit.

5) In the Group Policy Management Editor window under Computer Configuration, expand Policies > Centrify Settings.

6) Right-click Centrify Settings and select Add/Remove Templates.

7) In the Add/Remove Templates window, click the Add button. In the Open window, select all the Centrify .xml template files and click Open. If the Open window does not start at the location of the Centrify templates, they are normally located at C:\Program Files\Centrify\DirectControl\group policy\policy and have names such as centrify_linux_settings.xml.

8) Back in the Add/Remove Templates window, click OK.

9) At the Group Policy Management Editor window, a number of subfolders should now appear. Expand down to find the location of the policy you would like to set.

   NOTE: There are also Centrify Group Policy settings located under User Configuration > Policies > Centrify Settings.

10) On the right side, double-click the setting in question then make the desired changes and click Ok to save them. This completes the GPO change. The Centrify DirectControl agent running on the Linux system will pick up these changes the next time it checks in. For immediate updating of group policy, the adgpupdate command can be run from the Linux system.
Appendix A - Enabling Smart Card Login for Active Directory User Accounts

This Appendix will outline the steps required in Active Directory to make smart card login available for AD users.

**User Accounts**

To map a user’s certificate to their AD account in Windows Server 2008 using the standard method of mapping (Principal Name), the certificate must contain two things:

- An Enhanced Key Usage (EKU) of “Smart Card Logon” or a Key Usage of “Digital Signature”
- A Principal Name value in the SAN attribute of the certificate - this Principal Name must be in the form of xxxxx@domain_suffix

Their account User Logon Name must be renamed to match the Principal Name in the certificate. Existing user accounts can be modified easily in Active Directory Users and Computers, and new users can be configured properly from the start using the existing new user wizard.

**Manually Remapping Existing Users who currently authenticate via username/password**

1) Navigate to Start > Programs > Administrative Tools > Active Directory Users and Computers.
2) Navigate to a user who will be migrated to smart card logon.
3) Right-click the user and select Properties.
4) Select the Account tab. Note the user’s logon name and UPN suffix.
5) Change the User Logon Name to match the Principal Name of this user.
**Unclassified/NIPRNet systems:**

Select the @mil extension from the domain suffix pull-down box to match the domain suffix in the user’s certificate Principal Name value. Do not change the User logon name (pre-Windows 2000) fields.

![Image of user account properties]

**Secret/SIPRNet systems**

Select the @smil.mil or @agency.smil extension from the domain suffix drop-down box to match the domain suffix in the user’s certificate Principal Name value. Do not change the User logon name (pre-Windows 2000) fields.

6) Scroll down to the Account options section and check **Smart card is required for interactive logon**.

7) Click OK to save the modifications.

**Manually Creating New Users**

1) Navigate to Start > Programs > Administrative Tools > Active Directory Users and Computers.

2) Navigate to the OU container that will hold the new user. Right-click the container and select New > User.

3) Enter the user’s information similar to the screen shot below – enter the user’s real name information, but for the User Logon Name enter the EDI-PI of the user with the appropriate domain suffix:

**Unclassified/NIPRNet systems:**

EDIPI@mil domain suffix
Secret/SIPRNet systems

EDIPI@smil.mil or EDIPI@agency.smil domain suffix

Form the User Logon Name (pre- Windows 2000) as it would conform to the proper username convention of your network. Click Next when done.

4) Enter the appropriate temporary password for the user, selecting the standard options for your domain. Click Next when done.

5) When done, click Finish.
Appendix B: Centrify Known Issues

This Appendix will document some known issues that could impact the use of the Centrify Suite with Linux.

Issue with Screen Saver Lockout on RHEL 5 and CentOS 5

There is a known issue on RHEL 5 and CentOS 5 systems with not being able to log back into the system with the smart card after screen saver lockout occurs. This same issue may occur with Active Directory users that login using userid/password. Centrify has this documented in their knowledge base (KB-1629) and states it is an issue with the gnome screensaver.
## Appendix C: Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>DC</td>
<td>Domain Controller</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoDI</td>
<td>DoD Instruction</td>
</tr>
<tr>
<td>EDI-PI</td>
<td>Electronic Data Interchange – Personnel Identifier</td>
</tr>
<tr>
<td>EKU</td>
<td>Enhanced Key Usage (Microsoft definition)</td>
</tr>
<tr>
<td>GID</td>
<td>Global Identifier</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
</tr>
<tr>
<td>JRE</td>
<td>Java Runtime Environment</td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft Management Console</td>
</tr>
<tr>
<td>MSI</td>
<td>Microsoft Installer file format</td>
</tr>
<tr>
<td>NIPRNet</td>
<td>Unclassified but Sensitive Internet Protocol Router Network</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSS</td>
<td>National Security Systems</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKE</td>
<td>Public Key Enablement</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RG</td>
<td>Reference Guide</td>
</tr>
<tr>
<td>SAN</td>
<td>Subject Alternative Name</td>
</tr>
<tr>
<td>SCL</td>
<td>Smart Card Logon</td>
</tr>
<tr>
<td>SIPRNet</td>
<td>Secure Internet Protocol Router Network</td>
</tr>
<tr>
<td>STIG</td>
<td>Security Technical Implementation Guide</td>
</tr>
<tr>
<td>UID</td>
<td>Unique Identifier</td>
</tr>
<tr>
<td>UPN</td>
<td>User Principal Name</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Appendix D: Support and Information

Website
Please visit the URL below for additional information.

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

Technical Support
Contact technical support.

dodpke@mail.mil
Appendix E: References

