DoD Public Key Enablement (PKE) Reference Guide

Enabling Smart Card Logon for Mac OS X Using Centrify Suite 2012.4

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

Enabling Smart Card Logon for Mac OS X Using Centrify Suite 2012.4

12 February 2014

Version 1.2

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
12/24/12	1.0	Initial document developed
4/18/2013	1.1	Modified order of steps based on comments
2/12/2014	1.2	Updated to specify Centrify Suite 2012.4

Contents

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 Mac OS X for Smart Card Logon (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 Mac OS X 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[i] 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 Mac OS X 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 pose 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 Mac smart card logon and should be obtained through your local procurement office. This guide was written using Centrify Suite 2012.4. 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 2307[ii], 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 Mac OS X computers and users from Windows. Please see the Centrify Suite Admin Guide[iii] 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 Mac OS X instructions but not all versions of OS X may be supported by Centrify. Centrify documentation currently states that OS X 10.4 and later are supported.

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, the DirectControl agent needs to be installed on the Mac OS X 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: 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.

Installation of DirectControl Agent on Mac OS X System

These steps will outline the procedure to install the DirectControl agent on the Mac OS X system. The procedure documented is the manual installation method, Centrify also has a Deployment Manager installation method which can identify Mac OS X 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/, for more information on the Deployment Manager installation method. Before executing these steps, the Mac OS X system should have it's network configuration completed and be able to access the DNS server and domain controller. If the Apple Active Directory plugin is currently in use on the Mac OS X system it should be disabled before proceeding.

1) Obtain the Centrify DirectControl Agent in .dmg format for the Mac OS X operating system being used and copy to the Mac system.
2) Open the OS X Finder application and navigate to the location where the .dmg file was saved to in the previous step. Double-click the **Centrify DirectControl .dmg** file.
3) The Centrify DirectControl window will open. Double-click **ADCheck** to execute the ADCheck utility.
4) In the ADCheck window, enter the **name of the domain** in the AD Domain field and click the **AD Check** button.
5) The ADCheck utility will perform checks to verify the system and domain are setup correctly for Centrify to work. If the ADCheck output shows any failures, they should be addressed before proceeding. It is not required to address warnings at this time. Click the **Quit** button.
6) At the Centrify DirectControl window, double-click the **package** icon under Install.
7) The Install CentrifyDC window will appear. If you see a prompt stating *This package will run a program to determine if the software can be installed*, click the **Continue** button to proceed.
8) At the Welcome to the CentrifyDC Installer screen, click **Continue** to proceed.
9) At the Software License Agreement screen, click the **Continue** button and then click the **Agree** button to accept the license agreement.
10) If the Select a Destination screen appears, select the disk where you would like the Centrify software installed and click the **Continue** button to proceed.

11) At the Standard Install on "<*drive_name*>" screen, click the **Install** button. If a custom installation location is required, click the **Change Install Location** button and select the location for installation then click the **Install** button.

12) At this point you may be prompted for administrator userid and password. If this occurs, enter the userid and password then click the **Install Software** button.

13) At the Centrify ADJoin window, click the **Quit** button. The Mac system will be joined to the domain later in this guide.

14) At the installation was completed successfully screen, click the **Close** button.

15) Close the Centrify DirectControl widow by clicking the **red x** in the upper left corner.

Centrify Suite Configuration

Active Directory Configuration to support Centrify

These steps will be executed on the domain controller to prepare for the Mac OS X systems and users. It is recommended to create a separate container (OU) for Mac OS X 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 on 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 “Mac” and under that OU create OUs for Service Accounts, Mac Groups, and Mac Systems.

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 then click the **Connect as another user** check box. Enter the user name and password for a domain admin account. Click **OK**.

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

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

5) At the Install Licenses screen you must specifiy 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: Mac) 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/Mac/Licenses)and click **Next** to proceed.

6) You may see a window that 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. 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: Mac) 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. 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/Mac/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 Mac 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 procedure 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, 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 the **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 Mac Groups

This section will create a group for Mac users add members to it. 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/Mac/Mac Groups.

1) On the Domain Controller, click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers.**
2) Expand the domain and find the OU created for the Mac data. Under that OU, find the OU for Mac groups (ex: pke.mil/Mac/Mac Groups). Right-click the **OU** for the Mac groups and select **New > Group.**
3) Enter a **name** for the group (ex: Mac Users) in the **Group name** field. The other fields can remain at the default values. Click **OK** to create the new group.
4) In the right side pane of the Active Directory Users and Computers window, select the newly created group. Right-click **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 Centrify Admin Guide for more information.

1) In the Centrify DirectControl Administation Console, expand **Console Root > Centrify DirectControl > Zones.** Right-click the **zone** that you want to add the Mac users in and select **Properties**.

2) In the zone properties windows, 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** within which the Mac user 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. 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 **Apply** and then click **Start**. Click **Close**.

Centrify Group Configuration

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

1) On the Windows system with Centrify DirectControl Adminstration Console, open the console and click **Start > All Programs > Centrify > DirectControl > Centrify DirectControl.** If prompted, enter the user ID 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 Mac 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 Mac Group ID for this group. Click the **check box** beside **UNIX group name** and enter a name that will be used as the Mac group name for this group. Click **OK.**

6) Back at the Centrify DirectControl Adminstration Console screen, expand **Console Root > Centrify DirectControl > Zones > <** *zone name* > > **Authorization**.

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

8) In the **Name** field, type the **name of the group** previously created in step 3 of the **Creating Mac 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. Click the **login role** and click **OK.** Then click **OK** again.

Joining Mac OS X System to Domain

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

Joining Mac OS X System to Domain

These steps should be performed on the Mac OS X system.

1) Open the OS X Finder application and navigate to **Applications > Utilities > Centrify** and double-click **ADJoin**.
2) If the **Auto-Zone** and **Join this Zone** radio buttons are not displayed, click **Enable Licensed Features**. If prompted, enter an administrator user id and password.
3) Enter the name of the domain in the Active Directory Domain field. Click **Join this Zone** radio button and type the **name of the zone** created earlier in the guide.
4) Click the arrow next to **Show advanced options** and click the check box next to **Container DN.** In the field, enter the **location of the OU** created earlier to hold the Mac OS X systems (ex: pke.mil/Mac/Mac Systems). You may also click the **Browse** button to search for the container.
5) Click the **Join Domain** button. When prompted, enter the credentials of a domain administrator with permissions to add a system to the domain and click **OK**. If prompted, enter the user id and password for an administrator on the Mac OS X system and click **OK.**
6) If the join was successful, you should see: “This machine is joined to the Active Directory Domain.” Click **Quit** to close the ADJoin window.

Test Mac Logon Using Active Directory Credentials

These steps will test logging on to the Mac OS X system using a user id 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 Mac Username login prompt, enter the username for an Active Directory user account that was added to the Mac group in the section Creating and Configuring Mac Groups. Then enter the password for the same Active Directory user account and attempt to login.
2) The system should allow you to login and the user’s home directory should be **/User/<user-name>** as specified in the zone provisioning section earlier in this guide.

Enabling Smart Card Logon on Mac System

This section will go through the required steps to get smart card logon working on the Mac OS X system. 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 Mac Users group earlier in the Creating and Configuring Mac Groups section.

Enabling Smart Card Support on Mac System

These steps must be performed on the Mac OS X system to enable Centrify Smart Card support.

1) As an administrator, open the **Finder** application and navigate to **Applications > Utilities** then double-click **Terminal.**
2) Execute sctool to enable smart card support, **"sudo sctool –e"**. Enter the user password when prompted.
3) Verify smart card support was successfully enabled, **"sudo sctool –s".** Enter the user password when prompted. The command should return a message stating that smart card support is enabled.
4) Log out of the system and at the Name/password login prompt insert the CAC into the card reader. If the card is provisioned to an Active Directory user who is provisioned to the zone the machine is joined to, the login prompt should change to prompt for the PIN of the CAC. It may take several seconds for the prompt to change. The Active Directory user's account name, which corresponds to the CAC, should be displayed above the PIN prompt.
5) Type the CAC 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 Mac OS X 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. Click **Start > Administrative Tools > Group Policy Management**.
2) Find the location where you would like the GPO created (ex: Forest > Domains > pke.mil > Mac). 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 Mac 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 **Add**. 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_mac_settings.xml.
8) 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 Mac OS X 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 Mac OS X 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 logon 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.

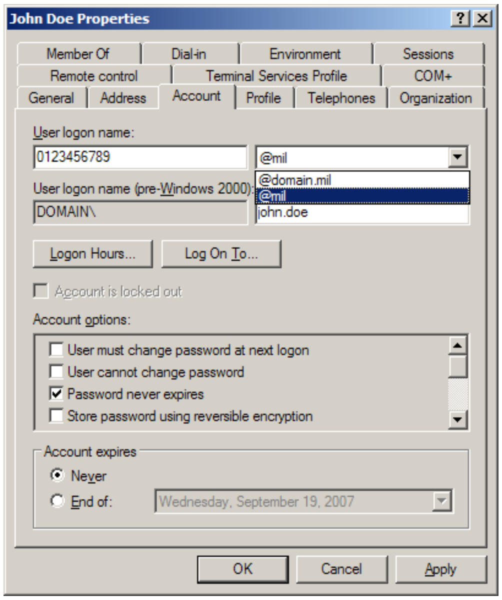
The account **User Logon Name** must be renamed to match the **Principal Name** in the certificate. Existing user accounts can be modified easily in **Active Directory Users and Computers**, and new users can be configured properly from the start using the existing new user wizard.

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) Click **Account**. 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 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.



User logon name: 0123456789 @mil

@domain.mil
@mil
john.doe

User logon name (pre-Windows 2000): DOMAIN\

□ Account is locked out

Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Wednesday, September 19, 2007

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:

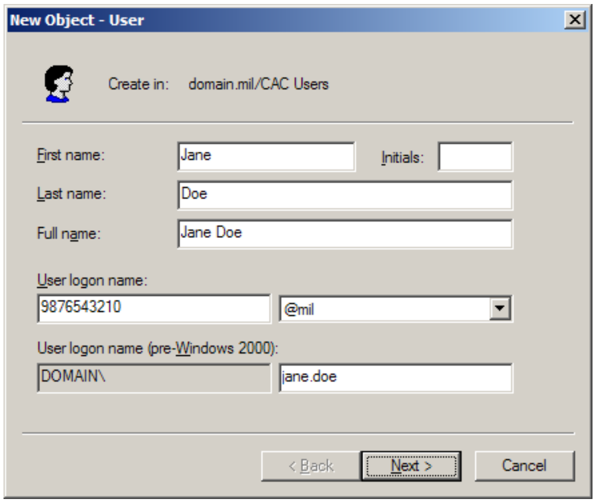
<u>**Unclassified/NIPRNet systems**</u>:

EDIPI@**mil** domain suffix

<u>**Secret/SIPRNet systems**</u>

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

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



Create in: domain.mil/CAC Users

First name: Jane

Initials:

Last name: Doe

Full name: Jane Doe

User logon name: 9876543210 @mil

User logon name (pre-Windows 2000): DOMAIN\ jane.doe

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: Acronyms and Abbreviations

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

Appendix C: 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 D: References

[i] Department of Defense Instruction (DoDI) 8520.02: Public Key Infrastructure (PKI) and Public Key (PK) Enabling, http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf.

[ii]RFC 2307: An Approach for Using LDAP as a Network Information Service, https://tools.ietf.org/html/rfc2307

[iii] Centrify Suite documentation, http://www.centrify.com/support/documentation.asp