SafeNet Authentication Client

Integration Guide

Using SAC with Putty-CAC

THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012549-001, Rev. A
Release Date	April 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Public key authentication provides a highly secure means of identifying a user to a login server, and is an alternative to the less secure method of entering a password. PuTTY-CAC is an SSH client for Windows, based on PuTTY SC, but adds the capability to extract public keys from certificates on a smart card if the public key is not available as a distinct object. SSH (Secure Shell) is a high-security protocol that uses strong cryptography to protect your connection against eavesdropping, hijacking, and other attacks.

This document provides guidance for integrating PuTTY-CAC with the SafeNet eToken. The integration aims at enabling the user to securely authenticate to their Linux servers using a certificate on the eToken instead of entering a password. This document provides configuration steps for creating SSH (PKCS11 and CAPI) connections to the Linux server.

Prerequisites

- SafeNet Authentication Client (on the Windows machine)
- PuTTY-CAC installed on the Windows machine
- The user has a token with valid, enrolled certificate
- It is assumed that the user has access to the Linux server

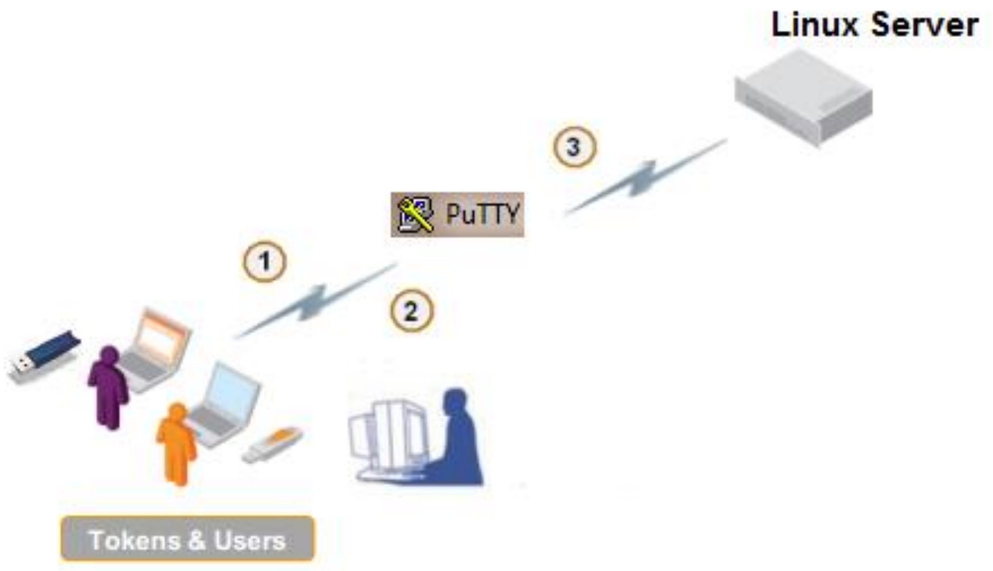
NOTE: In order for the instructions provided in this guide to succeed, the following programs must be installed and configured:

- SafeNet Authentication Client x64 Version 8.3
- PuTTY-CAC (0.62 and above) installed on Windows2K8_r2_x64
- SafeNet eToken authenticator
- Linux server (CentOS 6.5_x64)

Authentication Flow

The image below illustrates the data flow for authenticating to a Linux server through PuTTY-CAC using a certificate on an eToken.

1. The Windows user enters the login name of Linux user in the PuTTY login window.
2. The PuTTY login window asks for the eToken passphrase instead of the Linux user password.
3. Successful authentication is performed using the private key on the token. The user is logged in to the Linux server without providing his/her password.

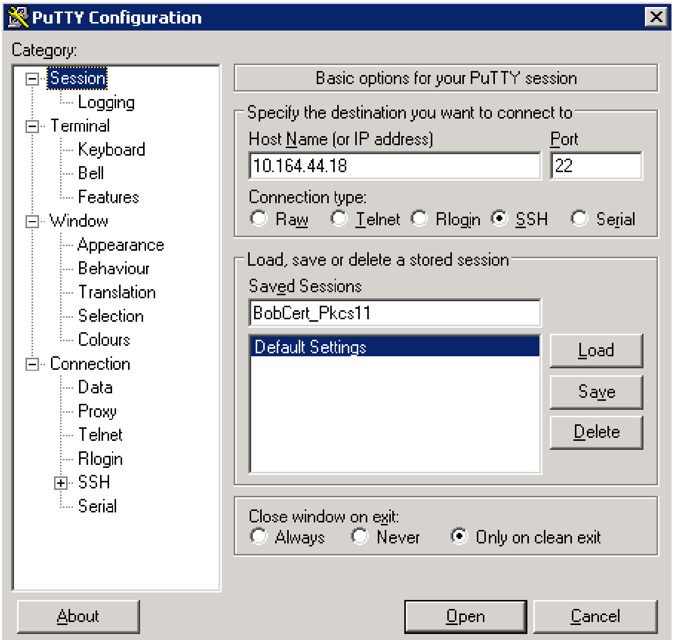


Configurations

Configuring PuTTY-CAC for PKCS11 Connection

1. Open PuTTY-CAC.
2. In the left pane, click **Session**.
3. Complete the **Basic Options for your PuTTY Session** dialog box as follows:

Host Name (or IP address)	Type the host name or IP address of the Linux server.
Port	Leave this value set to 22, the default port.
Connection type	Select **SSH**.
Saved Sessions	To save these settings, type a name for this connection session (for example, BobCert_Pkcs11).

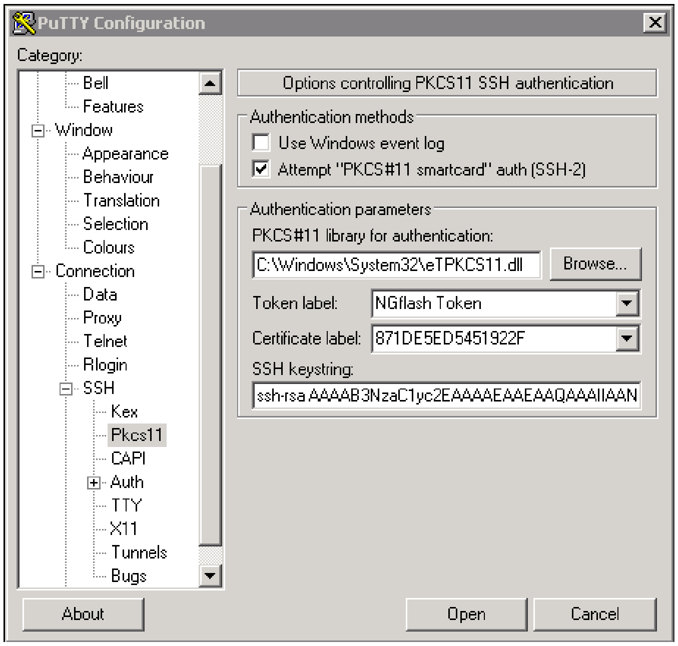


Host Name (or IP address): 10.164.44.18
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Saved Sessions: BobCert_Pkcs11
Close window on exit: ○ Always ○ Never ● Only on clean exit

4. In the left pane, select **Connection > SSH > Pkcs11**.

5. Complete the **Options controlling PKCS11 SSH authentication** dialog box as follows:

Authentication Methods	Select **Attempt "PKCS#11 smartcard" auth (SSH-2)**.
Authentication Parameters	
PKCS#11 library for authentication	Click the **Browse** button and then select **eTPKCS11.dll** (installed with SAC). The default location for this file is **C:\Windows\System32\eTPKCS11.dll**.
Token label	Select the token that contains your certificate.
Certificate label	Select the appropriate certificate label.
SSH keystring	The keystring is generated automatically based on the authentication settings above.



Options controlling PKCS11 SSH authentication

Authentication methods

□ Use Windows event log

☑ Attempt "PKCS#11 smartcard" auth (SSH-2)

Authentication parameters

PKCS#11 library for authentication: C:\Windows\System32\eTPKCS11.dll

Token label: NGflash Token

Certificate label: 871DE5ED5451922F

SSH keystring: ssh-rsa AAAAB3NzaC1yc2EAAAAEAAEAAQAAAIIAAN

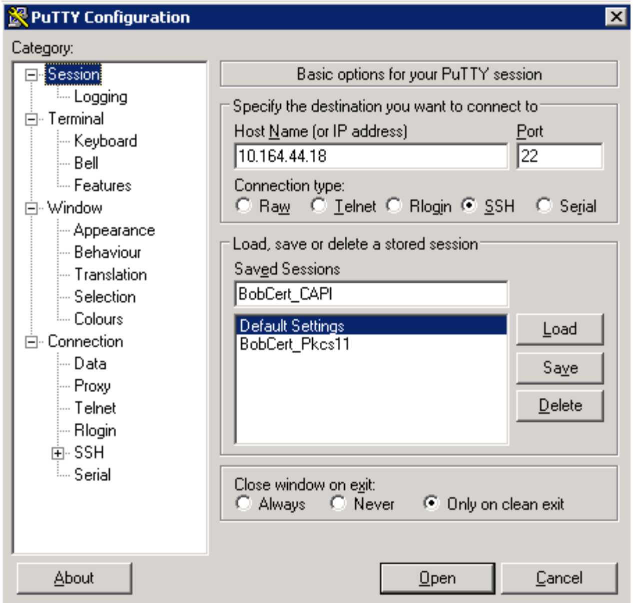
6. In the left pane, click **Session**.

7. In the right pane, click **Save**.

Configuring PuTTY-CAC for MS-CAPI Connection

1. Open PuTTY-CAC.
2. In the left pane, select **Session**.
3. Complete the **Basic Options for your PuTTY Session** dialog box as follows:

Host Name (or IP address)	Type the host name or IP address of the Linux server.
Port	Leave this value set to 22, the default port.
Connection type	Select **SSH**.
Saved Sessions	To save these settings, type a name for this connection session (for example, BobCert_Pkcs11).


PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.164.44.18

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

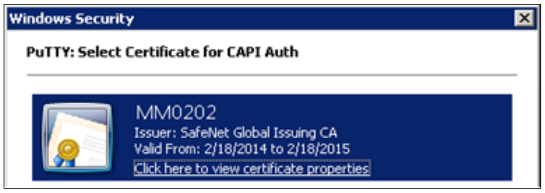
Saved Sessions: BobCert_CAPI

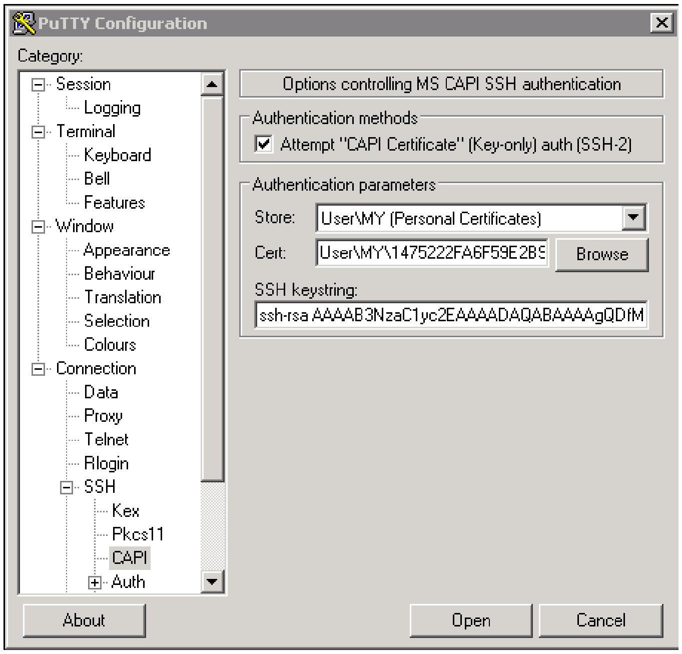
Default Settings
BobCert_Pkcs11

Close window on exit: ○ Always ○ Never ● Only on clean exit

4. In the left pane, click **Connection > SSH > CAPI**.

5. Complete the **Options controlling MS CAPI SSH authentication** dialog box as follows:

Authentication Methods	Select **Attempt "CAPI Certificate" (Key-only) auth (SSH-2)**.
Authentication parameters	
Store	Select the store that contains your certificate
Cert	Click the **Browse** button. A **Windows Security** message box is displayed. Select the appropriate certificate, and then click **OK**.  Windows Security PuTTY: Select Certificate for CAPI Auth MM0202 Issuer: SafeNet Global Issuing CA Valid From: 2/18/2014 to 2/18/2015 Click here to view certificate properties
SSH keystring	The keystring is generated automatically based on the authentication settings above.



Options controlling MS CAPI SSH authentication

Authentication methods

☑ Attempt "CAPI Certificate" (Key-only) auth (SSH-2)

Authentication parameters

Store: User\MY (Personal Certificates)

Cert: User\MY\1475222FA6F59E2B

SSH keystring:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDfM

6. In the left pane, click **Session.**

7. In the right pane, click **Save**.

Configuring the authorized_keys File on the Linux Server

In order to authenticate the user to the Linux server, the public key must be present in the server. To achieve this, perform the following steps:

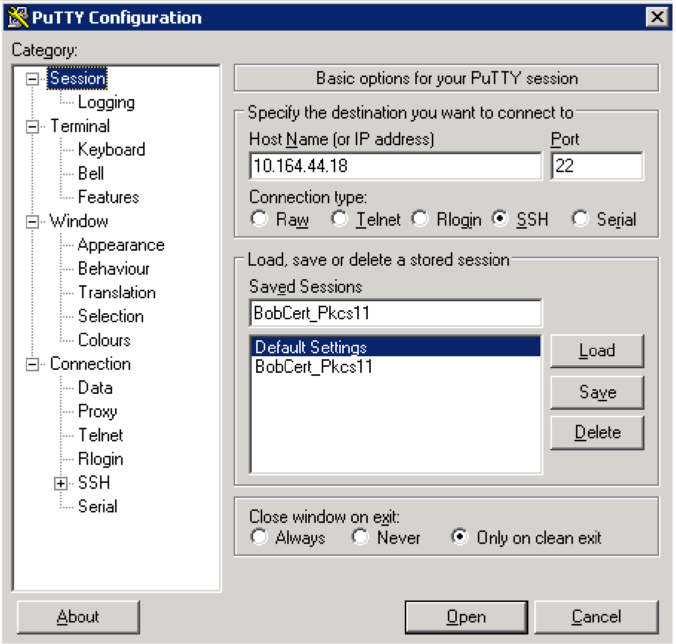
1. Log in to the Linux server.
2. Change the working directory to **$HOME/.ssh**.
3. Edit the **authorized_keys** file. You will need to create this file if it does not exist.
4. Do one of the following:
    - **For a PKCS11 connection:** Copy and paste the **SSH keystring** from step 5 on page 7.
    - **For an MS-CAPI connection:** Copy and paste the **SSH keystring** from step 5 on page 9.
5. Save the file.

Running the Solution

Once the session configuration for either the PKCS11 or CAPI connection are saved on PuTTY, and the **authorized_keys** file on the Linux server has the proper SSH keystring defined, you are ready to authenticate to the Linux server using the certificate on the token attached to the Windows machine instead of providing the password of the Linux user.

PKCS11 Scenario

1. Open PuTTY.
2. In the **Saved Sessions** list, click your previously saved session.



Specify the destination you want to connect to

Host Name (or IP address): 10.164.44.18 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

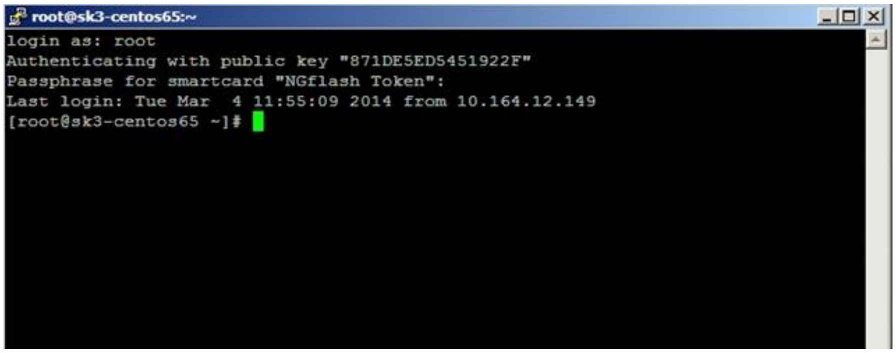
Load, save or delete a stored session

Saved Sessions: BobCert_Pkcs11

Default Settings
BobCert_Pkcs11

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Click **Load** to upload the saved settings.
4. Click **Open**.
5. The login window for the Linux machine is displayed.
6. Type the user ID of the Linux user for which you have configured the **authorized_keys** file, and then press **Enter**.
7. Type the token passphrase, and then press **Enter**.
8. Check for the successful login.

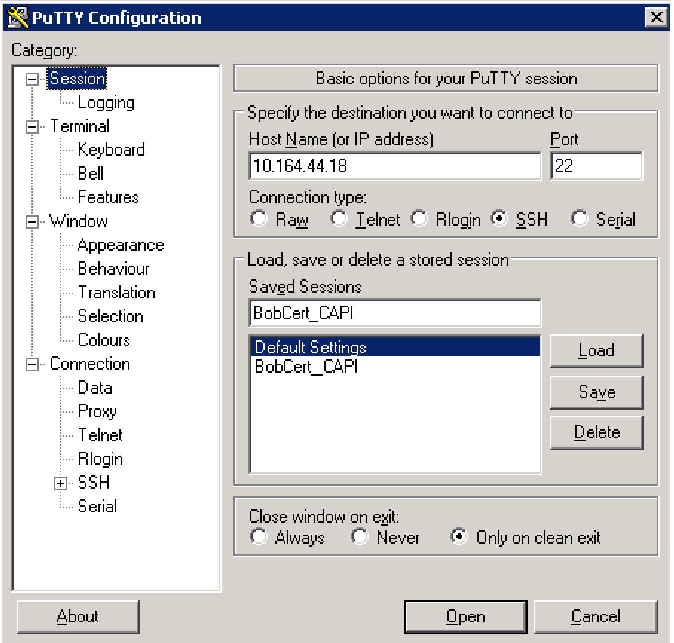


```
root@sk3-centos65:~
login as: root
Authenticating with public key "871DE5ED5451922F"
Passphrase for smartcard "NGflash Token":
Last login: Tue Mar  4 11:55:09 2014 from 10.164.12.149
[root@sk3-centos65 ~]#
```

NOTE: PuTTY will authenticate with the public key, referring to the **Certificate label**, and will prompt for the smart card passphrase (instead of the password for the user), referring to the Token Label.

MS- CAPI-based Connection

1. Open PuTTY.
2. In the **Saved Sessions** list, click your previously saved session.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.164.44.18

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

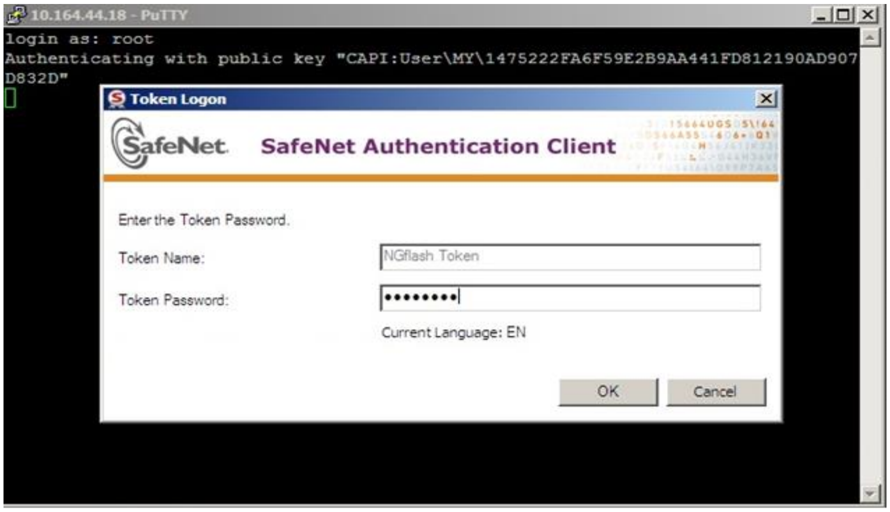
Load, save or delete a stored session

Saved Sessions: BobCert_CAPI

Default Settings
BobCert_CAPI

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Click **Load** to upload the saved settings.
4. Click **Open**.
5. The login window for the Linux machine is displayed.
6. Type the name of Linux user for which you have configured the **authorized_keys** file, and then press **Enter**.
7. On the **SAC Token Logon** dialog box, type the token password, and then click **OK**.



```
login as: root
Authenticating with public key "CAPI:User\MY\1475222FA6F59E2B9AA441FD812190AD907
D832D"
```

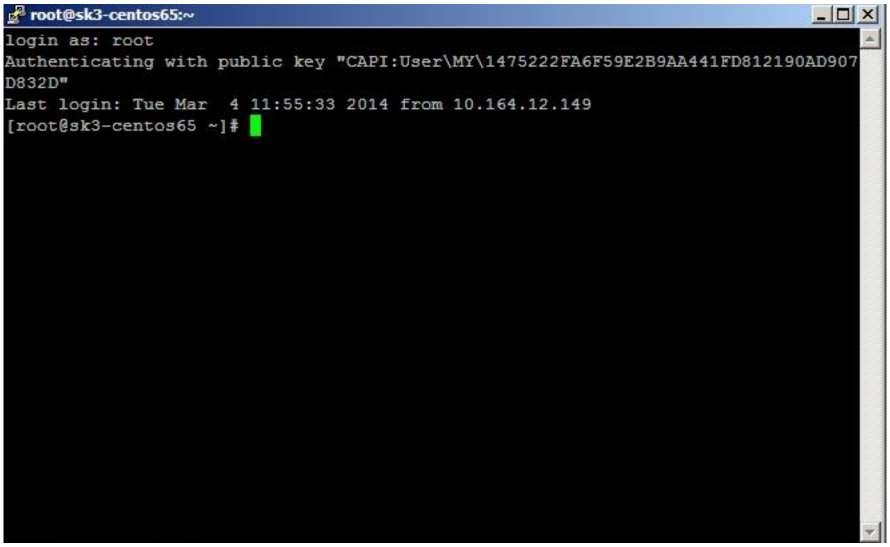
Enter the Token Password.

Token Name: NGflash Token

Token Password: ••••••••

Current Language: EN

8. Check for successful login.



```
login as: root
Authenticating with public key "CAPI:User\MY\1475222FA6F59E2B9AA441FD812190AD907
D832D"
Last login: Tue Mar  4 11:55:33 2014 from 10.164.12.149
[root@sk3-centos65 ~]#
```

Troubleshooting

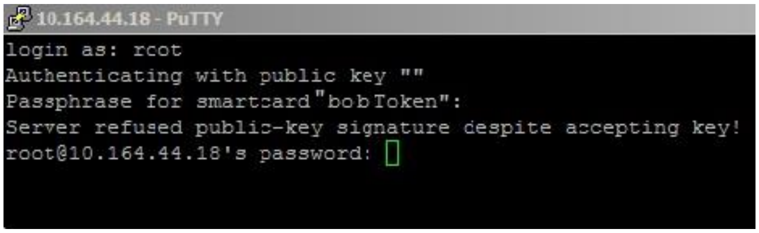
Common Errors

Error: Server refused our key

To resolve this error, ensure that the Linux user has access to the **authorized_keys** file and that the SSH keystring is correctly copied.

Error: Server refused public-key signature despite accepting key!

To resolve this issue, ensure the **authorized_keys** file in the SSH keystring is in a single line, and that there are no starting or trailing blank spaces.



```
login as: root
Authenticating with public key ""
Passphrase for smartcard "bobToken":
Server refused public-key signature despite accepting key!
root@10.164.44.18's password: 
```

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	