Technical Report

ONTAP SSH Authentication with a Common Access Card

Dan Tulledge, NetApp

September 2018 | TR-4717

Abstract

This technical report describes configuring and testing third-party SSH clients, in conjunction with ActivClient software, to authenticate an ONTAP storage administrator via the public key stored on a common access card (CAC) when it is configured in ONTAP.

Version History

Version	Date	Document Version History
Version 1.0	September 2018	Dan Tulledge: Initial commit.

TABLE OF CONTENTS

1 Overview

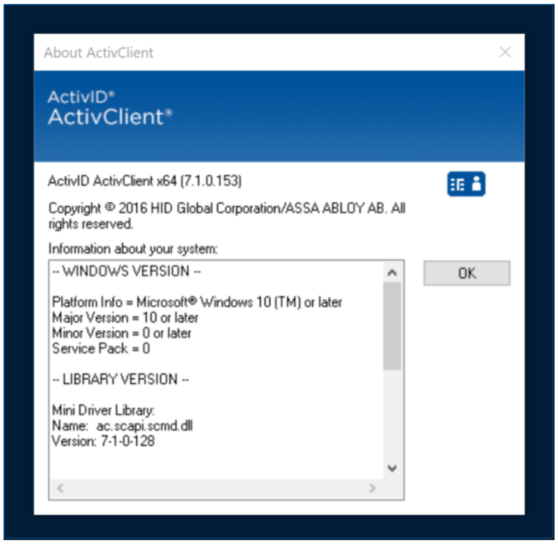
A common access card (CAC) is a “smart” identity card for active-duty military personnel, Selected Reserve members, DoD civilian employees, and eligible contractor personnel. The CAC stores X.509 certificates that can be read with a smart card reader. By using the third-party Secure Shell (SSH) clients PuTTY-CAC and SecureCRT, in conjunction with ActivClient software, to access the reader and the CAC, an ONTAP storage administrator can be authenticated via the public key stored on the CAC when it is configured in ONTAP.

2 Configuration

2.1 ActivClient

ActivClient software from HID Global is used by both PuTTY-CAC and SecureCRT SSH client software for access to the X.509 certificates stored on the CAC, which is inserted into a smart card reader. Testing performed to validate this report used ActivID ActivClient x64 (7.1.0.153) running on a Windows 10 Enterprise OS version 1709, OS build 16299.611.

Figure 1) About ActivID ActivClient.



About ActivClient

ActivID®
ActivClient®

ActivID ActivClient x64 (7.1.0.153)

Copyright © 2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

Information about your system:

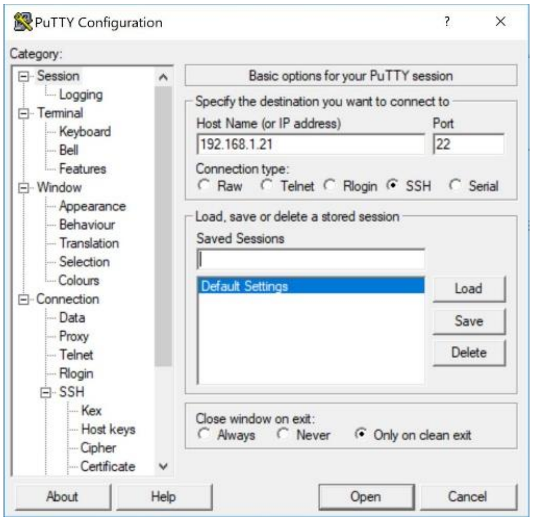
```
-- WINDOWS VERSION --

Platform Info = Microsoft® Windows 10 (TM) or later
Major Version = 10 or later
Minor Version = 0 or later
Service Pack = 0

-- LIBRARY VERSION --

Mini Driver Library:
Name:  ac.scapi.scmd.dll
Version: 7-1-0-128
```

2.2 PUTTY-CAC

PuTTY-CAC is public domain SSH client software. It can be obtained at https://github.com/NoMoreFood/putty-cac/releases. In testing performed to validate this report, puttycac-64bit-0.70u4-installer.msi was used in conjunction with the ActivClient described in section 2.1.

Configuration steps to access ONTAP -application ssh with -authentication-method publickey

1. Open Putty-CAC. In the Host Name field, enter the Cluster Management IP address or host name of ONTAP.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.21

Port: 22

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

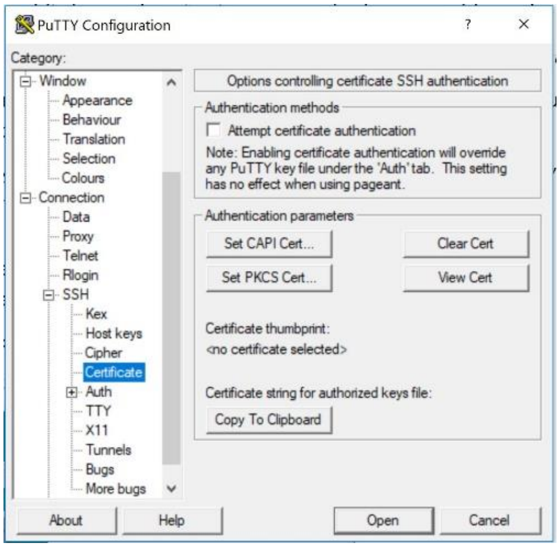
Load, save or delete a stored session

Saved Sessions

Default Settings

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

2. Expand SSH and select Certificates. Then click the Set PKCS Cert button.



Options controlling certificate SSH authentication

Authentication methods

□ Attempt certificate authentication

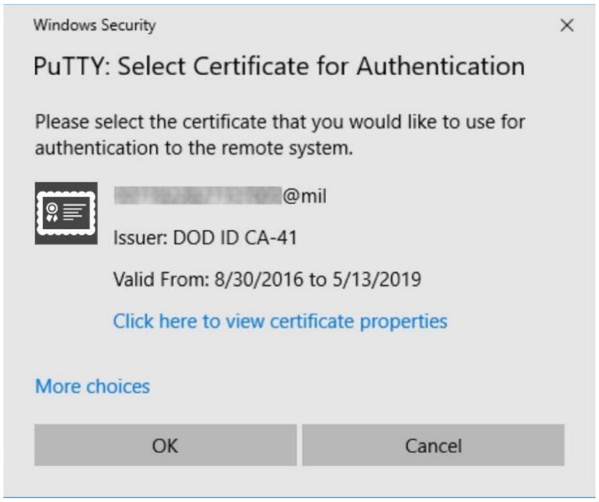
Note: Enabling certificate authentication will override any PuTTY key file under the 'Auth' tab. This setting has no effect when using pageant.

Authentication parameters

Certificate thumbprint:
<no certificate selected>

Certificate string for authorized keys file:

3. Browse for the `acpkcs211.dll` file in the ActivClient installation directory, `C:\Program Files\HID Global\ActivClient`. (Depending on the version, it may be located in the `c:\windows\system32` directory.) Then select your certificate.



PuTTY: Select Certificate for Authentication

Please select the certificate that you would like to use for authentication to the remote system.

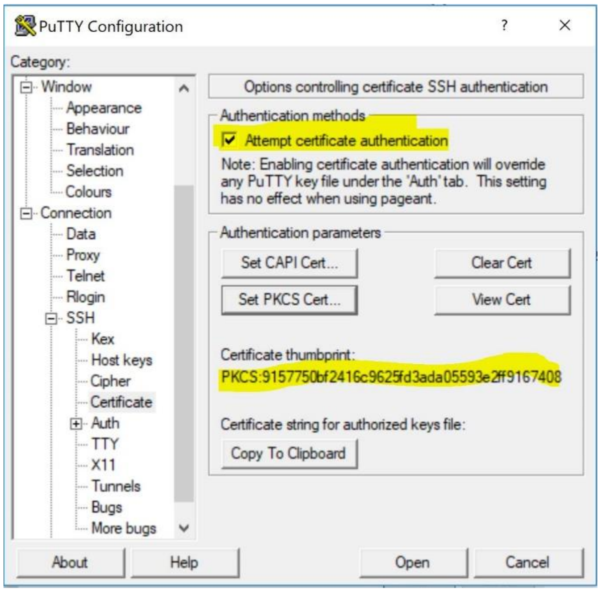
[redacted]@mil

Issuer: DOD ID CA-41

Valid From: 8/30/2016 to 5/13/2019

Click here to view certificate properties

4. Notice that the Attempt Certificate Authentication checkbox is checked and that there is a certificate thumbprint. Click Copy To Clipboard.



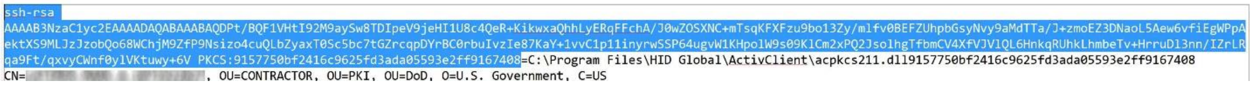
☑ Attempt certificate authentication

Note: Enabling certificate authentication will override any PuTTY key file under the 'Auth' tab. This setting has no effect when using pageant.

Certificate thumbprint:
PKCS:9157750bf2416c9625fd3ada05593e2ff9167408

Certificate string for authorized keys file:

5. Open a text editor, paste the contents of the clipboard into it, and select up to `=C:\ Program Files\HID Global\ActivClient\acpkcs211` and copy it into the clipboard.



```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDPt/BQF1VHtI92M9aySw8TDIpeV9jeHI1U8c4QeR+KikwxaQhhLyERqFFchA/J0wZOSXNC+mTsqKFXFzu9bo13Zy/m1fv0BEFZUhpbGsyNvy9aMdTTa/J+zmoEZ3DNaoL5Aew6vfiEgWPpA
ektXS9MLJzJzobQo68WChjM9ZfP9Nsizo4cuQLbZyaxT0Sc5bc7tGZrcqpDYrBC0rbuIvzIe87KaY+1vvC1p11inyrwSSP64ugvW1KHpolW9s09K1Cm2xPQ2Jso1hgTfbmCV4XfVJV1QL6HnkqRUhkLhmbeTv+HrruDl3nn/IZrLR
qa9Ft/qxvyCWnf0y1VKtuwy+6V PKCS:9157750bf2416c9625fd3ada05593e2ff9167408=C:\Program Files\HID Global\ActivClient\acpkcs211.dll9157750bf2416c9625fd3ada05593e2ff9167408
CN=[redacted], OU=CONTRACTOR, OU=PKI, OU=DoD, O=U.S. Government, C=US
```

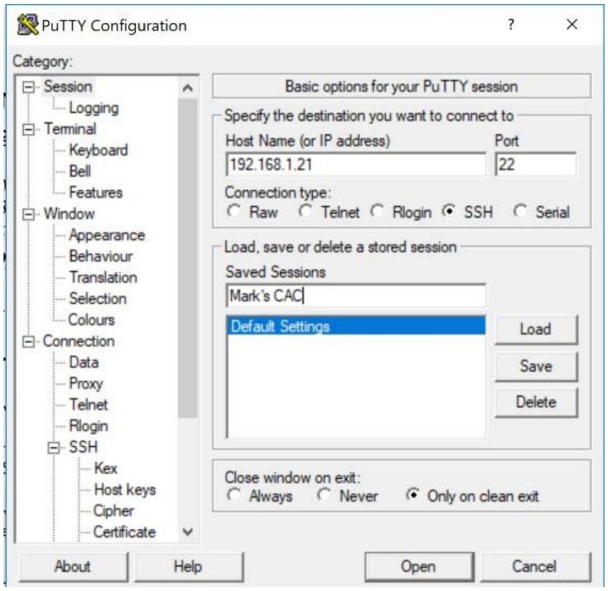
6. Create an admin user in ONTAP with a public key authentication method.

```
security login create -user-or-group-name <username> -application ssh -authentication-method
publickey

Warning: For successful authentication, ensure you create a public key for user "<username>"
using
"security login publickey create" interface.
```

7. Associate the copied public key from step 5 with the admin user created by pasting the public key in quotation marks into the `–publickey` field.

```
security login publickey create -username <username> -index 0 -publickey "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDBh8mgwjshX4P3oXw8Qd+s1p2jW8K73mw8ubYhvb+Alx4ZM9T0QmsmYTtFjQQ+bDbp6
ruqjjoO8hjl+WSVuxUwW5xWRUwYS/rtQmhP/2fudSncwd2cuRxMvMHKSruF8ee2WRTjO7vu7f4akrCfQL9cOhzh3dEHuFR5qo
OgCgr5nq8v3mZpAyoK7C4/uC9Lr8UO3mBctZ6pBfHLnQRCWgxc20FDFI4pM9Lz93fSIQXCCL8xrpCzi0bzH+4Dwug1gPJsrfS
a7Ki3s1SfNtiAWVqSh78D4iHYT8XjJr1TGVjsvZLg0/UUpwx5nvcRBWME9EczWi623tPO5fsUSGhQtCPn" -vserver
<admin vserver name>
```

8. In Putty-CAC, click Session and give the session a unique name to save it.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.21

Port: 22

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

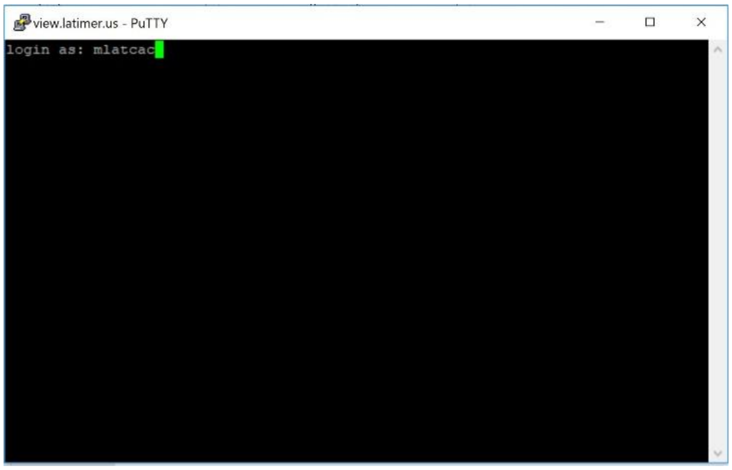
Load, save or delete a stored session

Saved Sessions: Mark's CAC

Default Settings

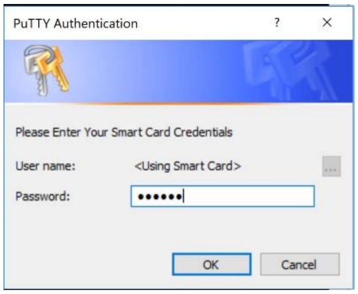
Close window on exit: ○ Always ○ Never ● Only on clean exit

9. Click Open and log in using the user name of the account you created in ONTAP and your CAC token PIN.



view.latimer.us - PuTTY

```
login as: mlatcac
```



PuTTY Authentication

Please Enter Your Smart Card Credentials

User name: <Using Smart Card>

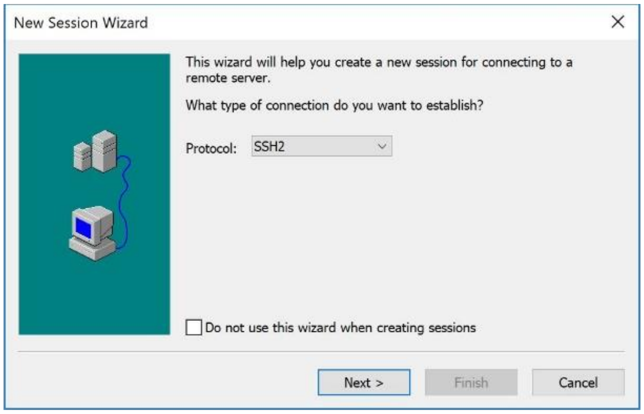
Password: ••••••

SecureCRT

SecureCRT is a commercially available SSH client from VanDyke Software. Testing performed to validate this report used SecureCRT scrt833-x64.exe in conjunction with the ActivClient described in section 2.1.

Configuration steps to access ONTAP -application ssh with -authentication-method publickey

1. Start the New Session Wizard in SecureCRT and click Next.



New Session Wizard

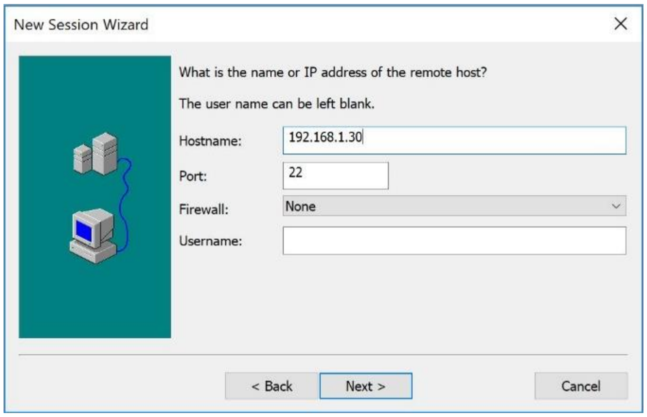
This wizard will help you create a new session for connecting to a remote server.

What type of connection do you want to establish?

Protocol: SSH2

☐ Do not use this wizard when creating sessions

2. In the Host Name field, enter the Cluster Management IP address or host name of ONTAP.



New Session Wizard

What is the name or IP address of the remote host?

The user name can be left blank.

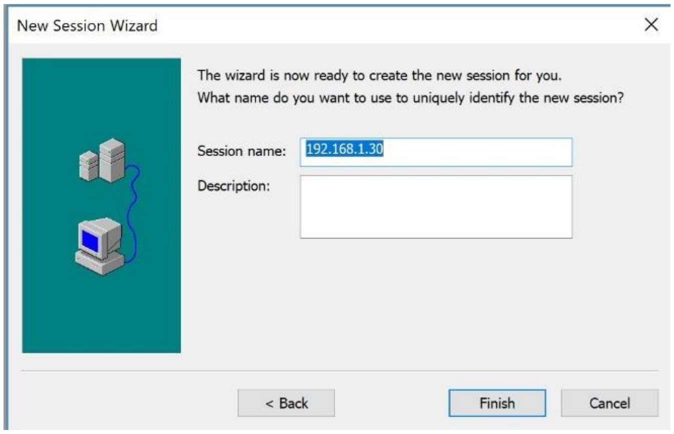
Hostname: 192.168.1.30

Port: 22

Firewall: None

Username:

3. Enter a unique session name and then click Finish.



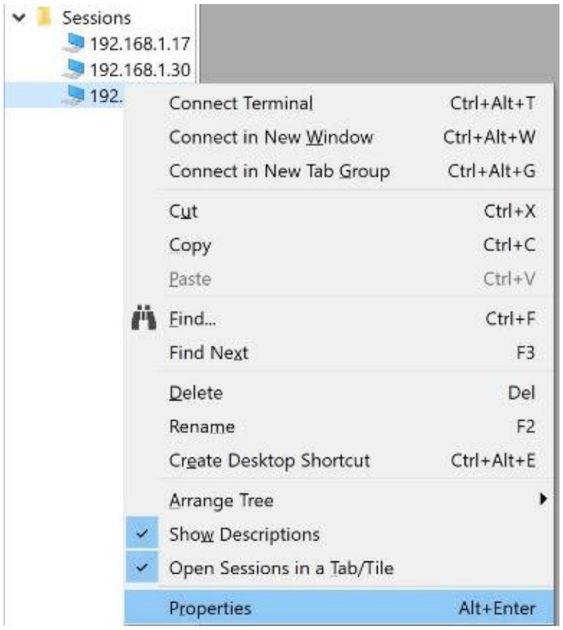
New Session Wizard

The wizard is now ready to create the new session for you.
What name do you want to use to uniquely identify the new session?

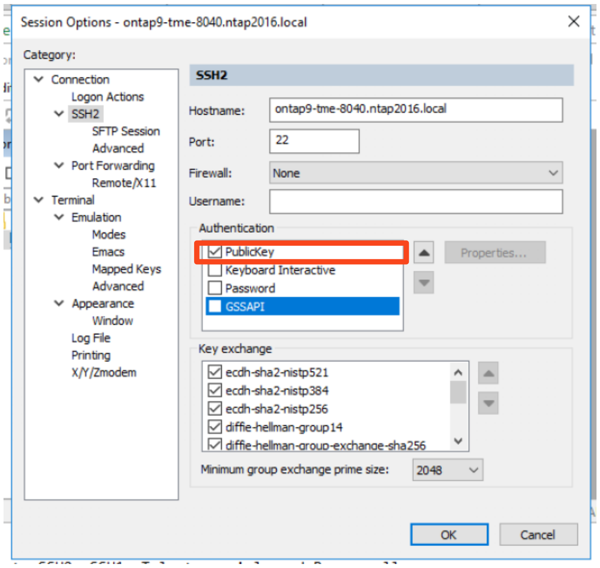
Session name: 192.168.1.30

Description:

4. In the Sessions pane, right-click the session you just created and then select Properties.



5. In the Connection pane, select SSH2. In the Authentication section in the right pane, uncheck everything except for PublicKey. Highlight PublicKey and click Properties.



Hostname: ontap9-tme-8040.ntap2016.local

Port: 22

Firewall: None

Username:

Authentication

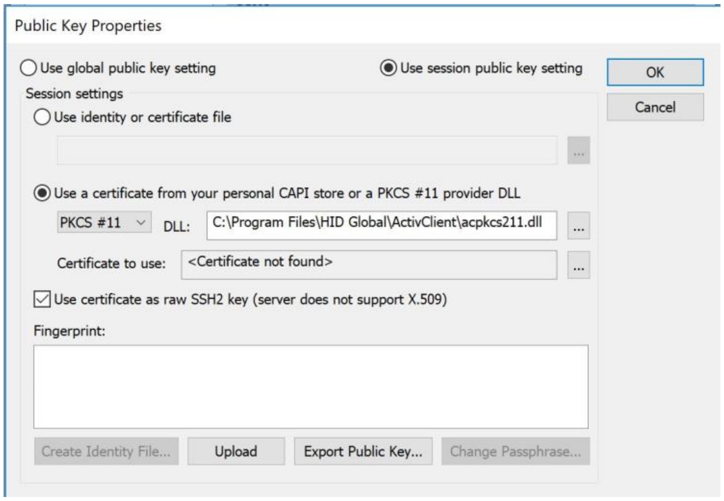
☑ PublicKey
□ Keyboard Interactive
□ Password
□ GSSAPI

Key exchange

☑ ecdh-sha2-nistp521
☑ ecdh-sha2-nistp384
☑ ecdh-sha2-nistp256
☑ diffie-hellman-group14
☑ diffie-hellman-group-exchange-sha256

Minimum group exchange prime size: 2048

6. Select Use Session Public Key Setting and PKCS #11. Browse for the `acpkcs211.dll` file in the ActivClient installation directory. (Depending on the version, it may be located in the `c:\windows\system32` directory.)



Public Key Properties

○ Use global public key setting   ● Use session public key setting

Session settings

○ Use identity or certificate file

● Use a certificate from your personal CAPI store or a PKCS #11 provider DLL

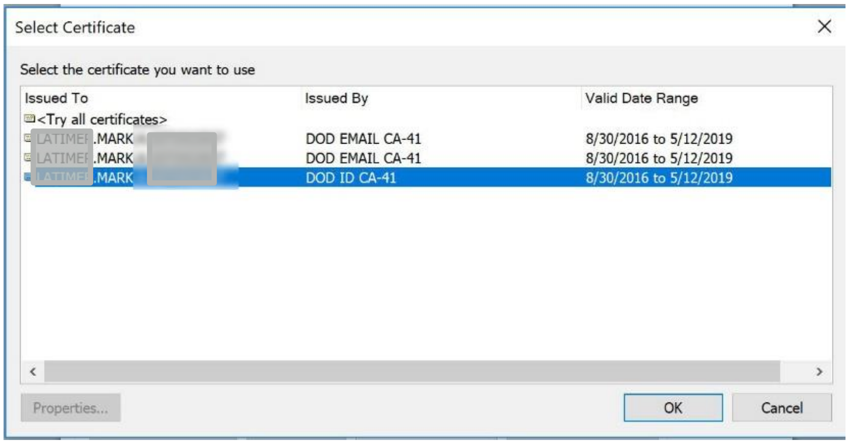
PKCS #11   DLL: C:\Program Files\HID Global\ActivClient\acpkcs211.dll

Certificate to use: <Certificate not found>

☑ Use certificate as raw SSH2 key (server does not support X.509)

Fingerprint:

7. Under Select the Certificate You Want to Use, select your DoD ID certificate, then click OK.

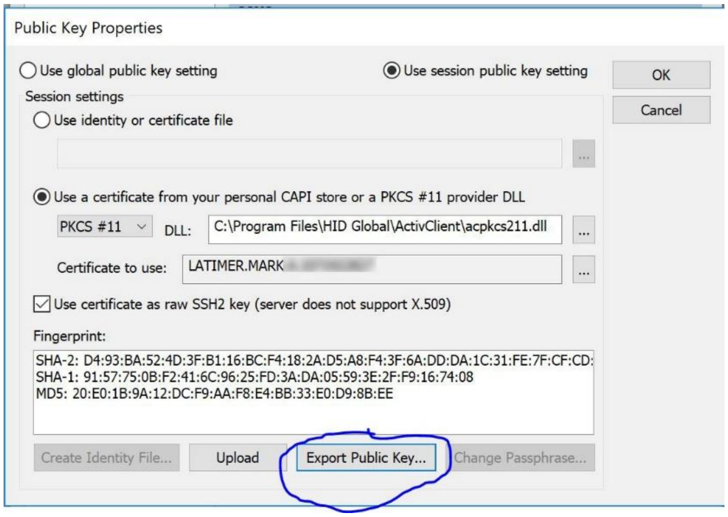


Select Certificate

Select the certificate you want to use

Issued To	Issued By	Valid Date Range
<Try all certificates>		
[redacted].MARK[redacted]	DOD EMAIL CA-41	8/30/2016 to 5/12/2019
[redacted].MARK[redacted]	DOD EMAIL CA-41	8/30/2016 to 5/12/2019
[redacted].MARK[redacted]	DOD ID CA-41	8/30/2016 to 5/12/2019

8. Check the Use Certificate as Raw SSH2 Key checkbox and then click Export Public Key.



Public Key Properties

○ Use global public key setting   ● Use session public key setting

Session settings

○ Use identity or certificate file

● Use a certificate from your personal CAPI store or a PKCS #11 provider DLL

PKCS #11   DLL: C:\Program Files\HID Global\ActivClient\acpkcs211.dll

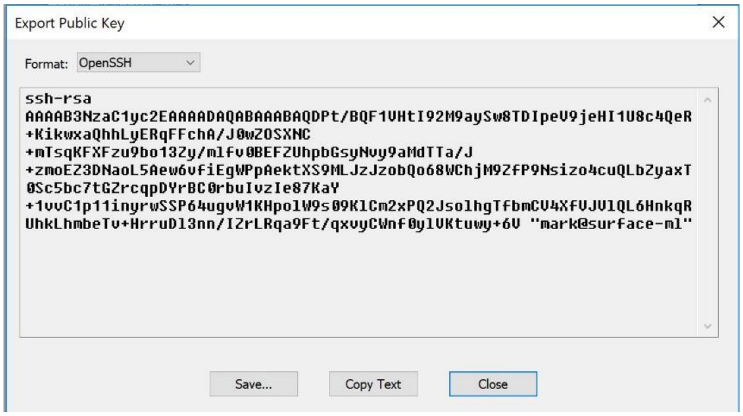
Certificate to use: LATIMER.MARK[redacted]

☑ Use certificate as raw SSH2 key (server does not support X.509)

Fingerprint:

```
SHA-2: D4:93:BA:52:4D:3F:B1:16:BC:F4:18:2A:D5:A8:F4:3F:6A:DD:DA:1C:31:FE:7F:CF:CD:
SHA-1: 91:57:75:0B:F2:41:6C:96:25:FD:3A:DA:05:59:3E:2F:F9:16:74:08
MD5: 20:E0:1B:9A:12:DC:F9:AA:F8:E4:BB:33:E0:D9:8B:EE
```

9. Click the Copy Text button and then click Close.



```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDPt/BQF1VHtI92M9aySw8TDIpeV9jeHI1U8c4QeR
+KikwxaQhhLyERqFFchA/J0wZOSXNC
+mTsqKFXFzu9bo13Zy/mlfv0BEFZUhpbGsyNvy9aMdTTa/J
+zmoEZ3DNaoL5Aew6vfiEgWPpAektXS9MLJzJzobQo68WChjM9ZfP9Nsizo4cuQLbZyaxT
0Sc5bc7tGZrcqpDYrBC0rbuIvzIe87KaY
+1vvC1p11inyrwSSP64ugvW1KHpolW9s09K1Cm2xPQ2JsolhgTfbmCV4XfVJV1QL6HnkqR
UhkLhmbeTv+HrruDl3nn/IZrLRqa9Ft/qxvyCWnf0ylVKtuwy+6V "mark@surface-ml"
```

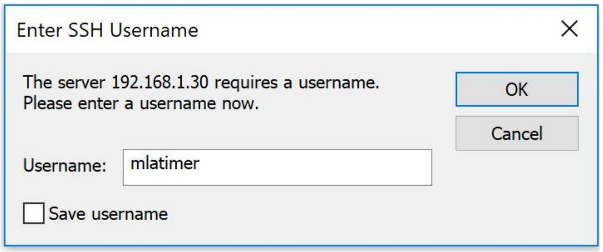
10. Paste the clipboard contents from step 9 into a text editor and delete the last bit in quotes (name, computer name) and copy the public key.
11. Click Close, then click OK, then OK again.
12. Create an admin user in ONTAP with a public key authentication method.

```
security login create -user-or-group-name <username> -application ssh -authentication-method
publickey

Warning: For successful authentication, ensure you create a public key for user "<username>"
using
"security login publickey create" interface.
```

13. Associate the copied public key from step 10 with the admin user created by pasting the public key in quotation marks into the –publickey field.

```
security login publickey create -username <username> -index 0 -publickey "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDBh8mgwjshX4P3oXw8Qd+s1p2jW8K73mw8ubYhvb+Alx4ZM9T0QmsmYTtFjQQ+bDbp6
ruqjjoO8hjl+WSVuxUwW5xWRUwYS/rtQmhP/2fudSncwd2cuRxMvMHKSruF8ee2WRTjO7vu7f4akrCfQL9cOhzh3dEHuFR5qo
OgCgr5nq8v3mZpAyoK7C4/uC9Lr8UO3mBctZ6pBfHLnQRCWgxc20FDFI4pM9Lz93fSIQXCCL8xrpCzi0bzH+4Dwug1gPJsrfS
a7Ki3s1SfNtiAWVqSh78D4iHYT8XjJr1TGVjsvZLg0/UUpwx5nvcRBWME9EczWi623tPO5fsUSGhQtCPn" -vserver
<admin vserver name>
```

14. In SecureCRT, open the session you created. In the Enter SSH Username box, enter the username for the account you created in ONTAP:

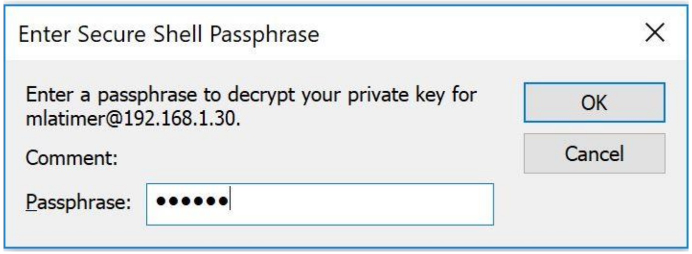


The server 192.168.1.30 requires a username.
Please enter a username now.

Username: mlatimer

□ Save username

15. In the Enter Secure Shell Passphrase box, enter the token PIN number.



Enter Secure Shell Passphrase

Enter a passphrase to decrypt your private key for mlatimer@192.168.1.30.

Comment:

Passphrase: ••••••

3 Disclaimer

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

4 Where to Find Additional Information

- HID ActivID ActivClient
- PuTTY-CAC on Github
- VanDyke Software SecureCRT
- ONTAP 9 Administrator Authentication and RBAC Power Guide

5 Contact Us

Let us know how we can improve this technical report.

Contact us at docfeedback@netapp.com.

Include TECHNICAL REPORT xxxx in the subject line.

Acknowledgement

Many thanks to Mark Latimer for his contributions toward publication of this document.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information

NetApp