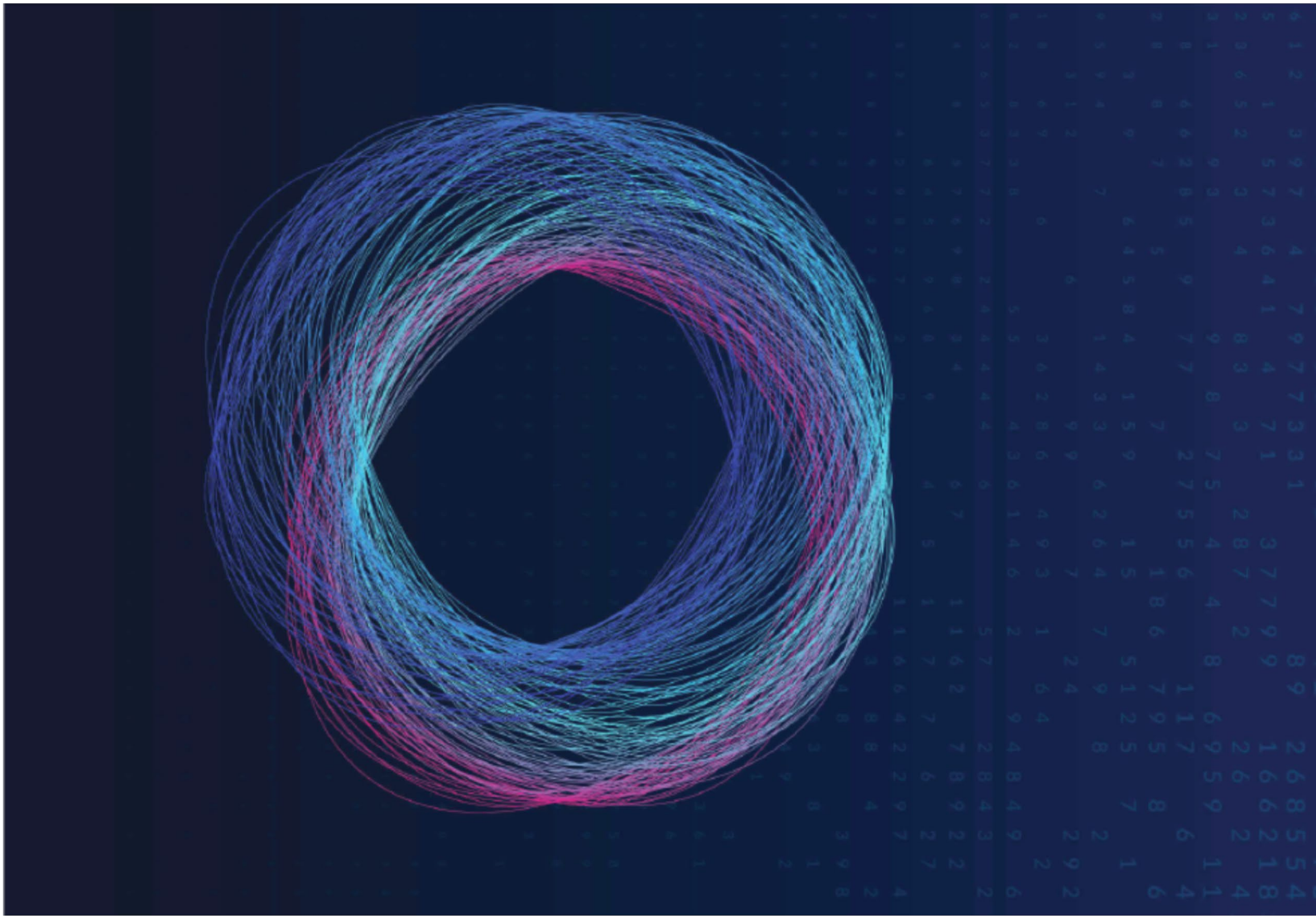
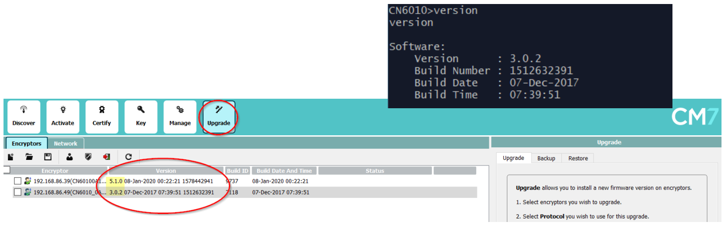


Thales ETSI Integration with Cerberis3

Version 1.0
07-August-2020

Table of Contents

Prerequisites



```
CN6010>version
version

Software:
    Version      : 3.0.2
    Build Number : 1512632391
    Build Date   : 07-Dec-2017
    Build Time   : 07:39:51
```

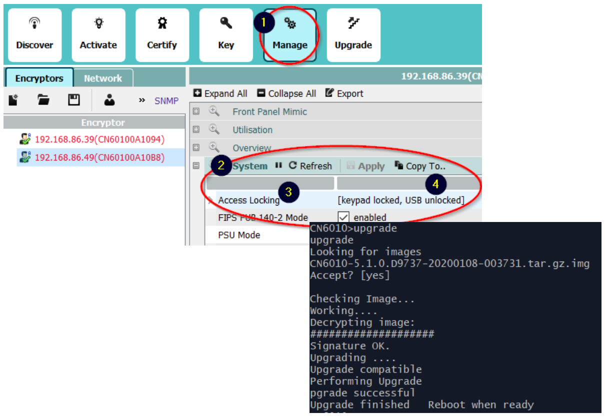
Encryptor	Version	Build ID	Build Date And Time	Status
192.168.86.39(CN60100A1...	5.1.0 08-Jan-2020 00:22:21 1578442941	9737	08-Jan-2020 00:22:21	
192.168.86.49(CN6010_0A...	3.0.2 07-Dec-2017 07:39:51 1512632391	7118	07-Dec-2017 07:39:51	

Upgrade allows you to install a new firmware version on encryptors.

1. Select encryptors you wish to upgrade.

2. Select **Protocol** you wish to use for this upgrade.

- ENC F/W version >= 5.0.1
  - check using either
    - CLI command : version
    - CM7 > Ugrade
- Must check Senetas RN for upgrade path
- Upgrade w/ CLI
  - check CM7 event/alarm to confirm there's no incompatible SFP warning
    - SFP compatibility issue may render ENC unresponsive requiring factory reset
  - ensure that ENC USB is unlocked
    - run command 'usb' or
    - check CM7 > System > access locking
  - insert USB stick with F/W into ENC
  - run 'upgrade' – will take about 5 min > Wait till "Upgrade finished" > then run 'reboot'



Access Locking	[keypad locked, USB unlocked]
FIPS PUB 140-2 Mode	☑ enabled
PSU Mode	

```
CN6010>upgrade
upgrade
Looking for images
CN6010-5.1.0.D9737-20200108-003731.tar.gz.img
Accept? [yes]

Checking Image...
Working....
Decrypting image:
###################
Signature OK.
Upgrading ....
Upgrade compatible
Performing Upgrade
pgrade successful
Upgrade finished   Reboot when ready
```

This presentation assumes you have already installed, activated, and certified the Thales encryptors per the quick start or similar guide.
You should be able to bring up a tunnel connection via non-QKD keys.
Make sure you have properly set the date/time.

If you are running in IDQ3P QKD Mode you'll need to first run the script to disable this mode. After disabling you may need to re-activate and certify the encryptor.

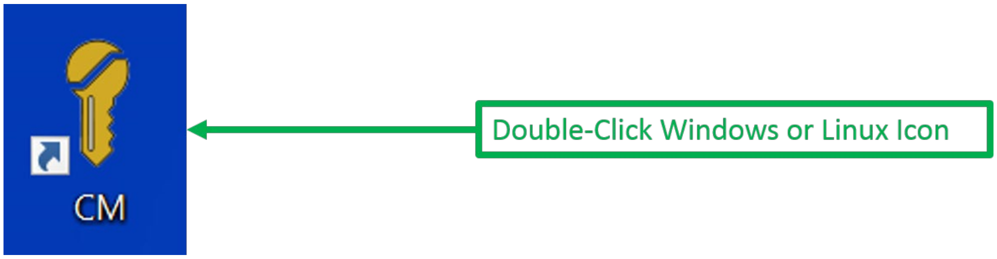
Make sure you are running a version of software capable of ETSI QKD Mode

Steps needed for a successful integration:

- **Enable eQKD Mode on Thales encryptor**
- **Configure eQKD parameters**
- **Import or create CA and client certificates**

Launch CM7 Manager and Enable eQKD Mode

Launch CM7 Management GUI



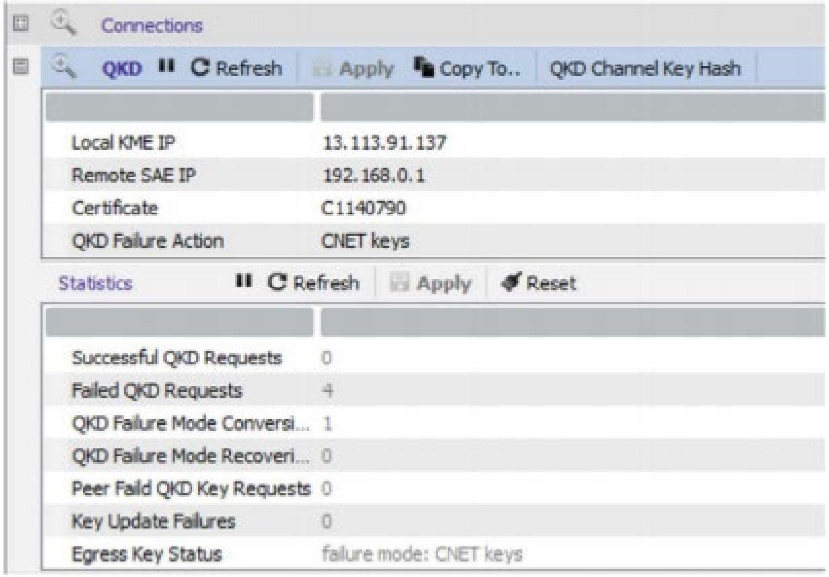
Double-Click Windows or Linux Icon

Enable eQKD Mode

Note that a reboot is required after enabling ETSI QKD Mode

- A separate panel will be displayed after the reboot containing configuration and statistics related to eQKD operation:

Local KME IP:
The local Key Management Entity (QKD device), with IP accessibility from the front panel management port.



Local KME IP	13.113.91.137
Remote SAE IP	192.168.0.1
Certificate	C1140790
QKD Failure Action	CNET keys

Successful QKD Requests	0
Failed QKD Requests	4
QKD Failure Mode Conversi...	1
QKD Failure Mode Recoveri...	0
Peer Faild QKD Key Requests	0
Key Update Failures	0
Egress Key Status	failure mode: CNET keys

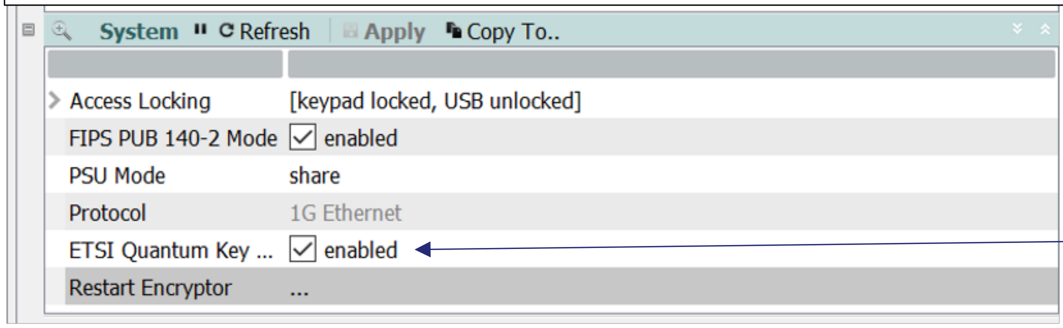
Remote SAE IP:
The remote Encryptors front panel IP address

Certificate:
The certificate hash for the secure HTTPS connection to the KME (QKD) device. This can be the CA certificate for host only authentication, or a signed end user certificate for client authentication.

QKD Failure Action:
CNET_KEYS (default) will failover to internal classical keys on failure to retrieve QKD keys from KME devices at either end.
Use last keys – on failover, use last QKD keys until operation is corrected.

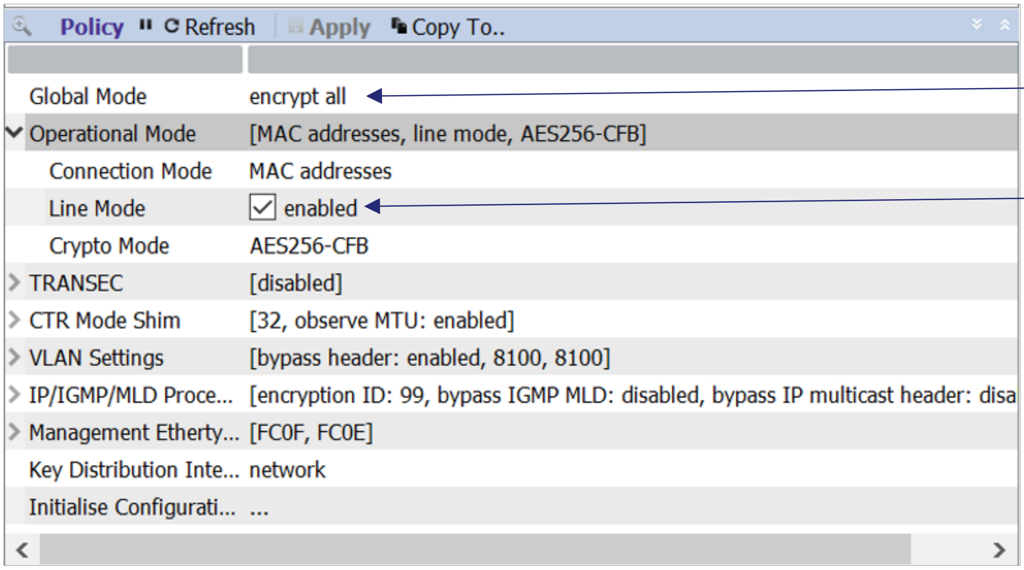
Enable QKD Mode and Setting Parameters

1) Launch CM7 Management GUI



Access Locking	[keypad locked, USB unlocked]
FIPS PUB 140-2 Mode	☑ enabled
PSU Mode	share
Protocol	1G Ethernet
ETSI Quantum Key ...	☑ enabled
Restart Encryptor	...

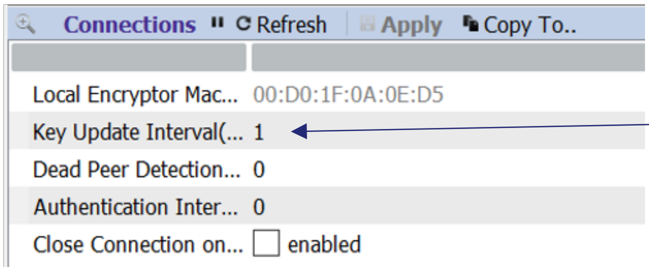
2) Verify you have selected ETSI Quantum Key Mode (Reboot Required)



Global Mode	encrypt all
Operational Mode	[MAC addresses, line mode, AES256-CFB]
Connection Mode	MAC addresses
Line Mode	☑ enabled
Crypto Mode	AES256-CFB
TRANSEC	[disabled]
CTR Mode Shim	[32, observe MTU: enabled]
VLAN Settings	[bypass header: enabled, 8100, 8100]
IP/IGMP/MLD Proce...	[encryption ID: 99, bypass IGMP MLD: disabled, bypass IP multicast header: disa
Management Etherty...	[FC0F, FC0E]
Key Distribution Inte...	network
Initialise Configurati...	...

3) Configure global policy: for example "encrypt all"

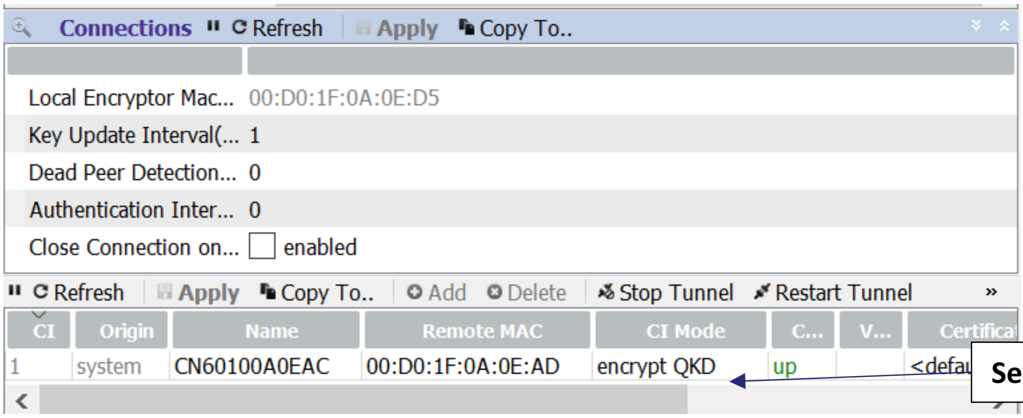
4) Enable Line Mode if point to point configuration is desired



Local Encryptor Mac...	00:D0:1F:0A:0E:D5
Key Update Interval(...	1
Dead Peer Detection...	0
Authentication Inter...	0
Close Connection on...	□ enabled

5) Configure Key Update Interval (minutes) Suggest value =1

In the Connections table, enable QKD encryptions



Local Encryptor Mac...	00:D0:1F:0A:0E:D5
Key Update Interval(...	1
Dead Peer Detection...	0
Authentication Inter...	0
Close Connection on...	□ enabled

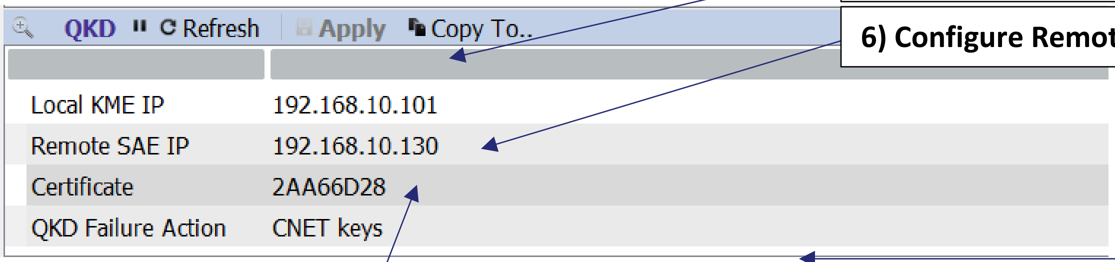
CI	Origin	Name	Remote MAC	CI Mode	C...	V...	Certificat
1	system	CN60100A0EAC	00:D0:1F:0A:0E:AD	encrypt QKD	up		<defau

Select Mode “encrypt QKD”

In the connections table, enable QKD encryption

5) Configure QNC IP

6) Configure Remote Encryptor IP



Local KME IP	192.168.10.101
Remote SAE IP	192.168.10.130
Certificate	2AA66D28
QKD Failure Action	CNET keys

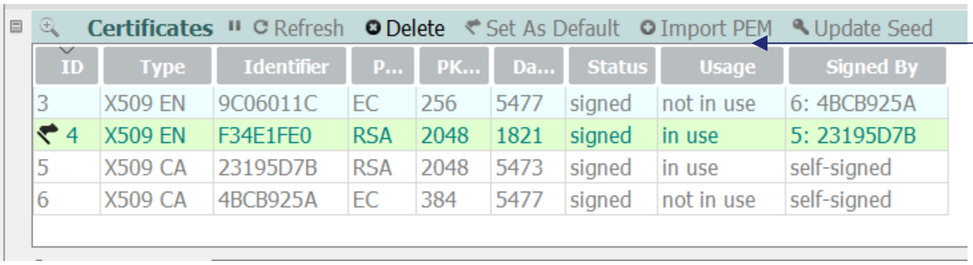
7) Configure Desired QKD Failure Action

We will configure this later after creating and signing the certificates!

Configure on both encryptors

Certificates & Keys

You will need a valid root CA, client certificates and associated private keys. You can import these into the encryptors using CM7:



ID	Type	Identifier	P...	PK...	Da...	Status	Usage	Signed By
3	X509 EN	9C06011C	EC	256	5477	signed	not in use	6: 4BCB925A
4	X509 EN	F34E1FE0	RSA	2048	1821	signed	in use	5: 23195D7B
5	X509 CA	23195D7B	RSA	2048	5473	signed	in use	self-signed
6	X509 CA	4BCB925A	EC	384	5477	signed	not in use	self-signed

Import

The supported algorithm must be FIPS approved and are listed below:

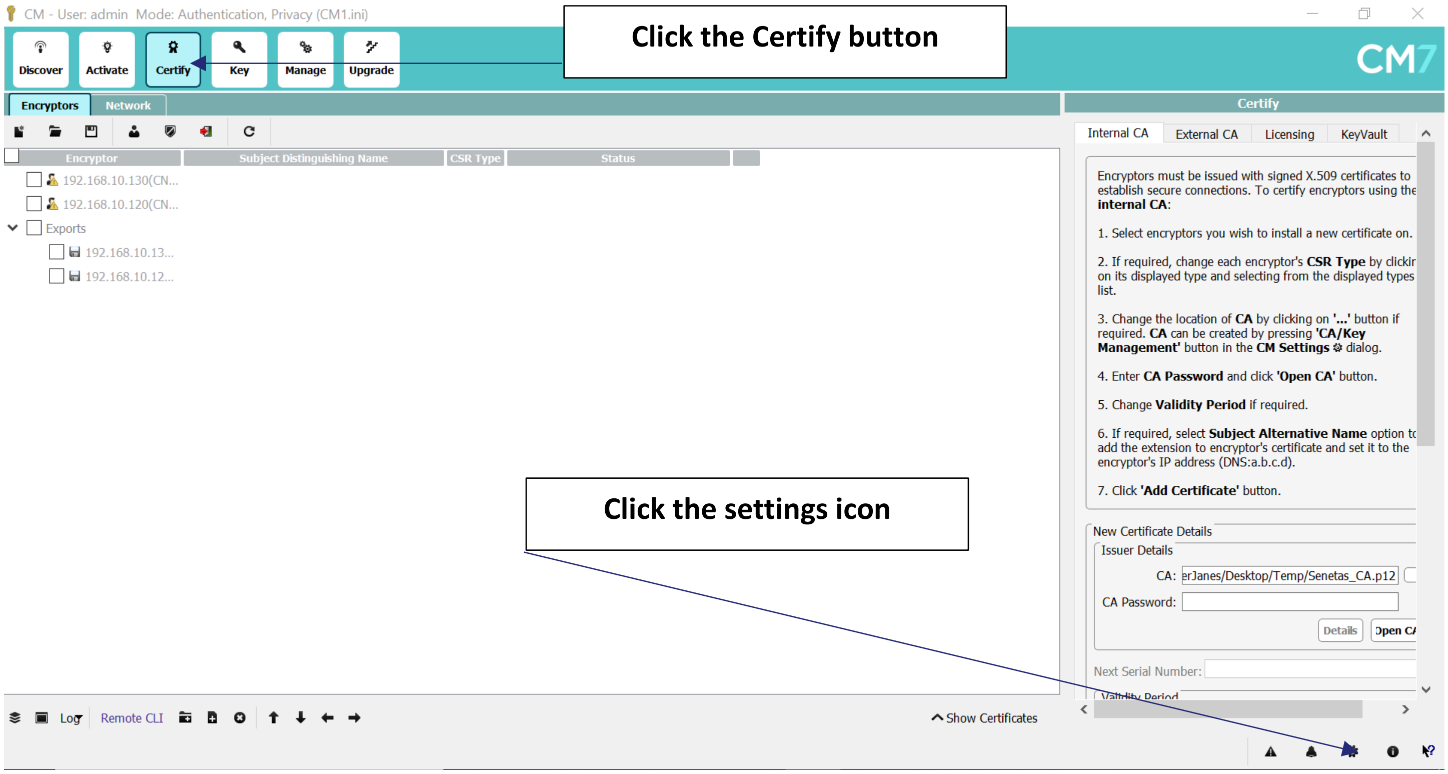
secp384r1 NIST/SECG curve over a 384 bit prime field
secp521r1 NIST/SECG curve over a 521 bit prime field
prime256v1 X9.62/SECG curve over a 256 bit prime field

(**RSA Certs Not Supported**)

Creating your own CA, Certs, and Keys

Alternatively you can use the following steps to easily create your own root CA, certificates and keys using CM7 and openSSL

Create a root CA in CM7:
Launch the CM7 Management Tool



Click the Certify button

Click the settings icon

Encryptors must be issued with signed X.509 certificates to establish secure connections. To certify encryptors using the **internal CA**:

1. Select encryptors you wish to install a new certificate on.

2. If required, change each encryptor's **CSR Type** by clickir on its displayed type and selecting from the displayed types list.

3. Change the location of **CA** by clicking on **'...'** button if required. **CA** can be created by pressing **'CA/Key Management'** button in the **CM Settings** ⚙ dialog.

4. Enter **CA Password** and click **'Open CA'** button.

5. Change **Validity Period** if required.

6. If required, select **Subject Alternative Name** option tc add the extension to encryptor's certificate and set it to the encryptor's IP address (DNS:a.b.c.d).

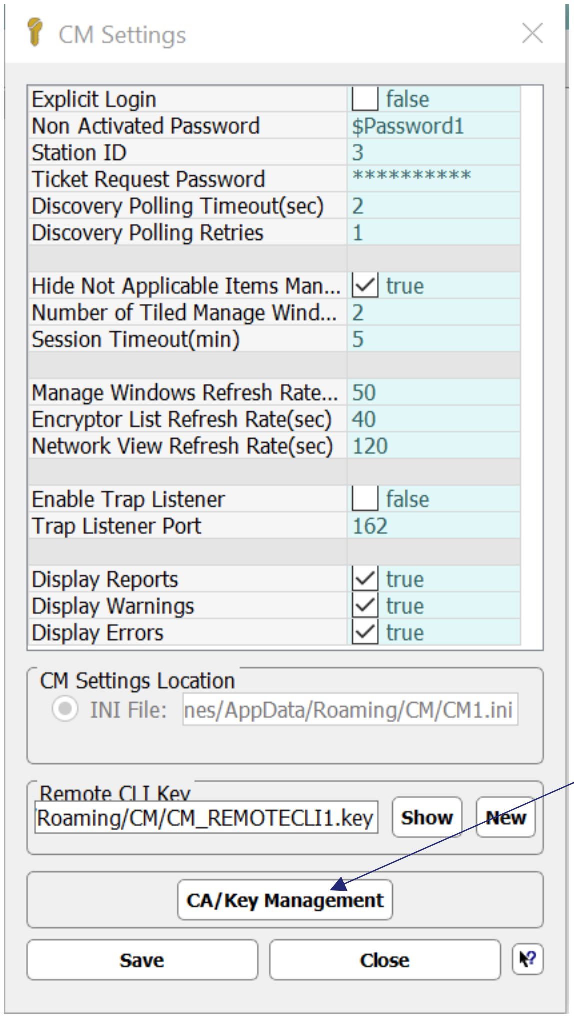
7. Click **'Add Certificate'** button.

New Certificate Details

Issuer Details

CA: erJanes/Desktop/Temp/Senetas_CA.p12

CA Password:



Explicit Login	□ false
Non Activated Password	$Password1
Station ID	3
Ticket Request Password	**********
Discovery Polling Timeout(sec)	2
Discovery Polling Retries	1
Hide Not Applicable Items Man...	☑ true
Number of Tiled Manage Wind...	2
Session Timeout(min)	5
Manage Windows Refresh Rate...	50
Encryptor List Refresh Rate(sec)	40
Network View Refresh Rate(sec)	120
Enable Trap Listener	□ false
Trap Listener Port	162
Display Reports	☑ true
Display Warnings	☑ true
Display Errors	☑ true

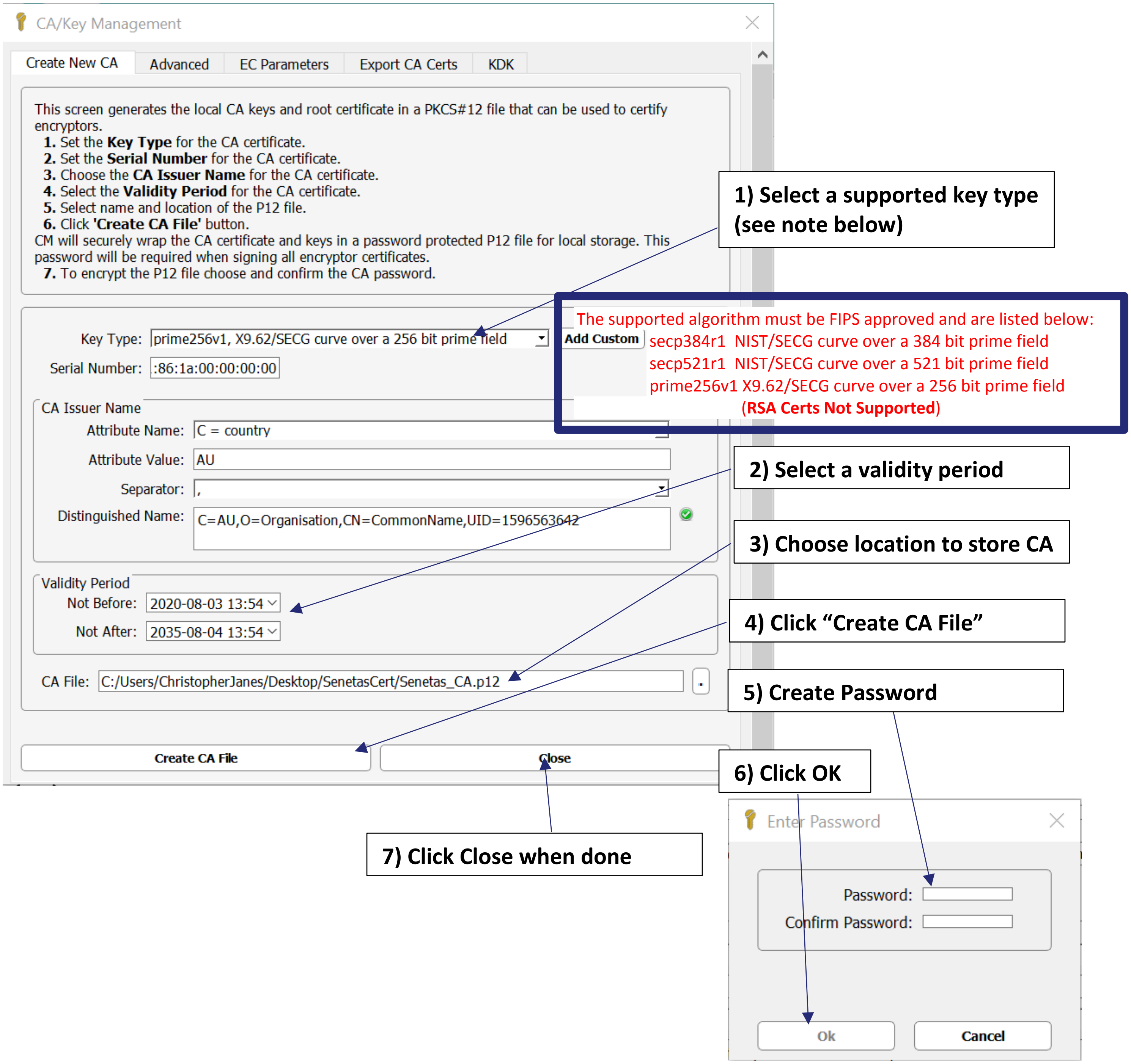
CM Settings Location

○ INI File: nes/AppData/Roaming/CM/CM1.ini

Remote CLI Key

Roaming/CM/CM_REMOTECLI1.key

1) Click on CA/Key Management



This screen generates the local CA keys and root certificate in a PKCS#12 file that can be used to certify encryptors.

1. Set the **Key Type** for the CA certificate.
2. Set the **Serial Number** for the CA certificate.
3. Choose the **CA Issuer Name** for the CA certificate.
4. Select the **Validity Period** for the CA certificate.
5. Select name and location of the P12 file.
6. Click **'Create CA File'** button.

CM will securely wrap the CA certificate and keys in a password protected P12 file for local storage. This password will be required when signing all encryptor certificates.

7. To encrypt the P12 file choose and confirm the CA password.

Key Type: prime256v1, X9.62/SECG curve over a 256 bit prime field

Serial Number: :86:1a:00:00:00:00

CA Issuer Name

Attribute Name: C = country

Attribute Value: AU

Separator: ,

Distinguished Name: C=AU,O=Organisation,CN=CommonName,UID=1596563642

Validity Period

Not Before: 2020-08-03 13:54

Not After: 2035-08-04 13:54

CA File: C:/Users/ChristopherJanes/Desktop/SenetasCert/Senetas_CA.p12

Password:

Confirm Password:

1) Select a supported key type (see note below)

The supported algorithm must be FIPS approved and are listed below:
secp384r1 NIST/SECG curve over a 384 bit prime field
secp521r1 NIST/SECG curve over a 521 bit prime field
prime256v1 X9.62/SECG curve over a 256 bit prime field
(**RSA Certs Not Supported**)

2) Select a validity period

3) Choose location to store CA

4) Click "Create CA File"

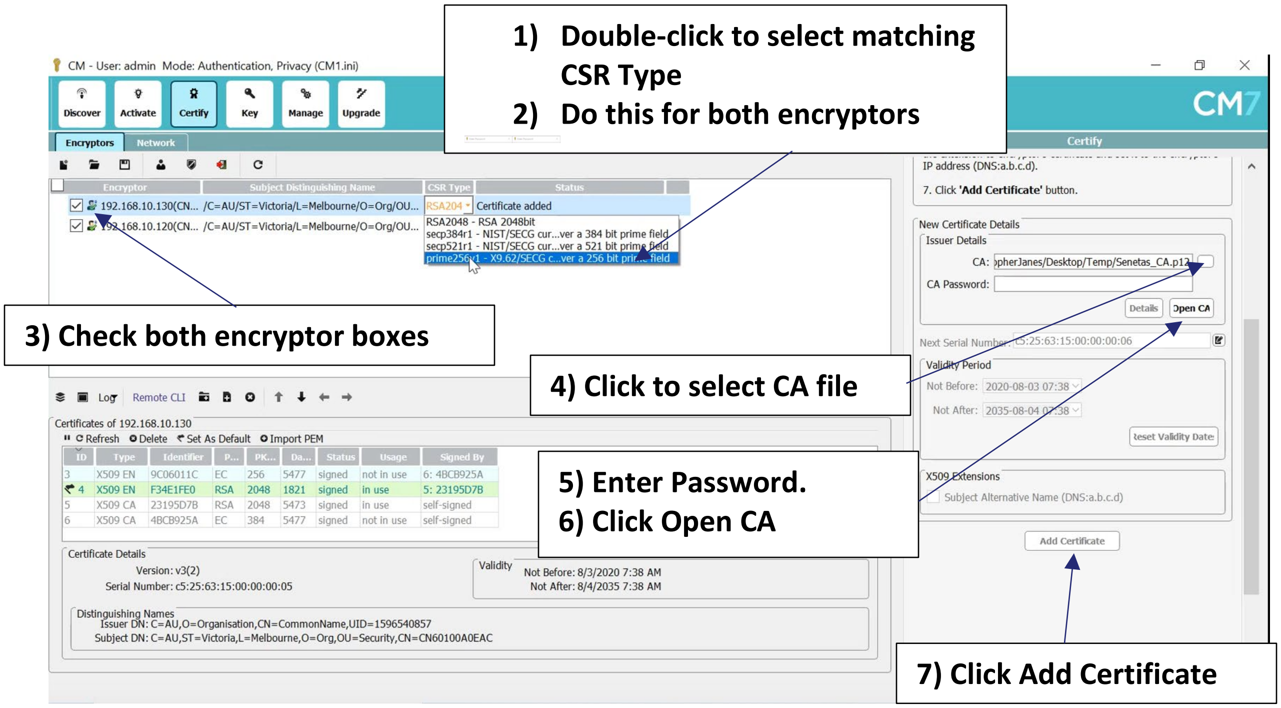
5) Create Password

6) Click OK

7) Click Close when done

Copy the CA you originally created in CM7 to your linux machine:
(in our example filename QKD_Centauris_CA.p12)

Convert this CA to .pem extension using the following openssl command:
openssl pkcs12 -in path.p12 -out newfile.pem -nodes
(openssl pkcs12 -in QKD_Centauris_CA.p12 -out QKD_Centauris_CA.pem -nodes)



1) Double-click to select matching CSR Type
2) Do this for both encryptors

3) Check both encryptor boxes

4) Click to select CA file

5) Enter Password.
6) Click Open CA

7) Click Add Certificate

	Encryptor	Subject Distinguishing Name	CSR Type	Status
☑	192.168.10.130(CN...	/C=AU/ST=Victoria/L=Melbourne/O=Org/OU...	RSA204	Certificate added
☑	192.168.10.120(CN...	/C=AU/ST=Victoria/L=Melbourne/O=Org/OU...		

RSA2048 - RSA 2048bit
secp384r1 - NIST/SECG cur...ver a 384 bit prime field
secp521r1 - NIST/SECG cur...ver a 521 bit prime field
prime256v1 - X9.62/SECG c...ver a 256 bit prime field

Certificates of 192.168.10.130

ID	Type	Identifier	P...	PK...	Da...	Status	Usage	Signed By
3	X509 EN	9C06011C	EC	256	5477	signed	not in use	6: 4BCB925A
4	X509 EN	F34E1FE0	RSA	2048	1821	signed	in use	5: 23195D7B
5	X509 CA	23195D7B	RSA	2048	5473	signed	in use	self-signed
6	X509 CA	4BCB925A	EC	384	5477	signed	not in use	self-signed

Certificate Details
Version: v3(2)
Serial Number: c5:25:63:15:00:00:00:05

Validity
Not Before: 8/3/2020 7:38 AM
Not After: 8/4/2035 7:38 AM

Distinguishing Names
Issuer DN: C=AU,O=Organisation,CN=CommonName,UID=1596540857
Subject DN: C=AU,ST=Victoria,L=Melbourne,O=Org,OU=Security,CN=CN60100A0EAC

IP address (DNS:a.b.c.d).

7. Click **'Add Certificate'** button.

New Certificate Details
Issuer Details
CA: pherJanes/Desktop/Temp/Senetas_CA.p12
CA Password:

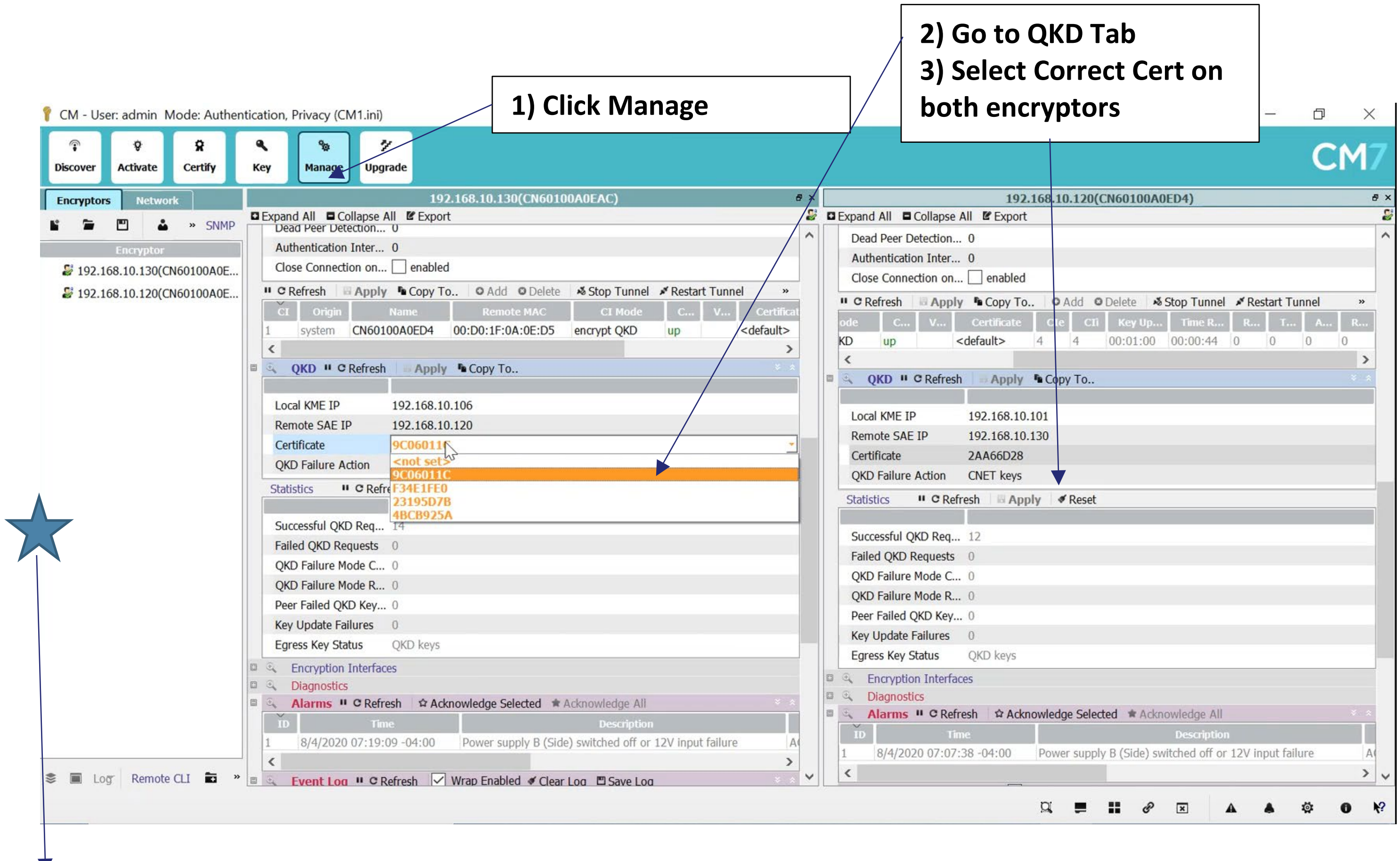
Next Serial Number: c5:25:63:15:00:00:00:06

Validity Period
Not Before: 2020-08-03 07:38
Not After: 2035-08-04 07:38

X509 Extensions
□ Subject Alternative Name (DNS:a.b.c.d)

1) Click Manage

2) Go to QKD Tab
3) Select Correct Cert on both encryptors



192.168.10.130(CN60100A0EAC)

Dead Peer Detection...	0
Authentication Inter...	0
Close Connection on...	□ enabled

CI	Origin	Name	Remote MAC	CI Mode	C...	V...	Certificat
1	system	CN60100A0ED4	00:D0:1F:0A:0E:D5	encrypt QKD	up		<default>

QKD

Local KME IP	192.168.10.106
Remote SAE IP	192.168.10.120
Certificate	9C06011C <not set> 9C06011C F34E1FE0 23195D7B 4BCB925A
QKD Failure Action	

Statistics

Successful QKD Req...	14
Failed QKD Requests	0
QKD Failure Mode C...	0
QKD Failure Mode R...	0
Peer Failed QKD Key...	0
Key Update Failures	0
Egress Key Status	QKD keys

Alarms

ID	Time	Description	A
1	8/4/2020 07:19:09 -04:00	Power supply B (Side) switched off or 12V input failure	A(

192.168.10.120(CN60100A0ED4)

Dead Peer Detection...	0
Authentication Inter...	0
Close Connection on...	□ enabled

ode	C...	V...	Certificate	CIe	CIi	Key Up...	Time R...	R...	T...	A...	R...
KD	up		<default>	4	4	00:01:00	00:00:44	0	0	0	0

QKD

Local KME IP	192.168.10.101
Remote SAE IP	192.168.10.130
Certificate	2AA66D28
QKD Failure Action	CNET keys

Statistics

Successful QKD Req...	12
Failed QKD Requests	0
QKD Failure Mode C...	0
QKD Failure Mode R...	0
Peer Failed QKD Key...	0
Key Update Failures	0
Egress Key Status	QKD keys

Alarms

ID	Time	Description	A
1	8/4/2020 07:07:38 -04:00	Power supply B (Side) switched off or 12V input failure	A(

(You can find the Certificates in the "Certificates" Section of the GUI. Note the new client certificate is signed by the CA you created first)

Create a CSR for the QKD server that you will sign with the CA created in CM7:

On a linux machine with openssl installed perform the follow steps:

Verify you have a .rnd file in your home directory. You can create one using the command "touch .rnd" from your home directory or "touch ~/.rnd"

(Our examples use the prime256v1 key type. Make sure they match what you create in CM7)

```
openssl ecparam -out QKDServer.pkey -name prime256v1 -genkey && openssl req -new -key
QKDServer.pkey -nodes -out QKDServer.csr -subj "/C=CH/ST=Geneva/L=Geneva/O=ID
Quantique/OU=QuantumSafe/CN=QKDServer"
```

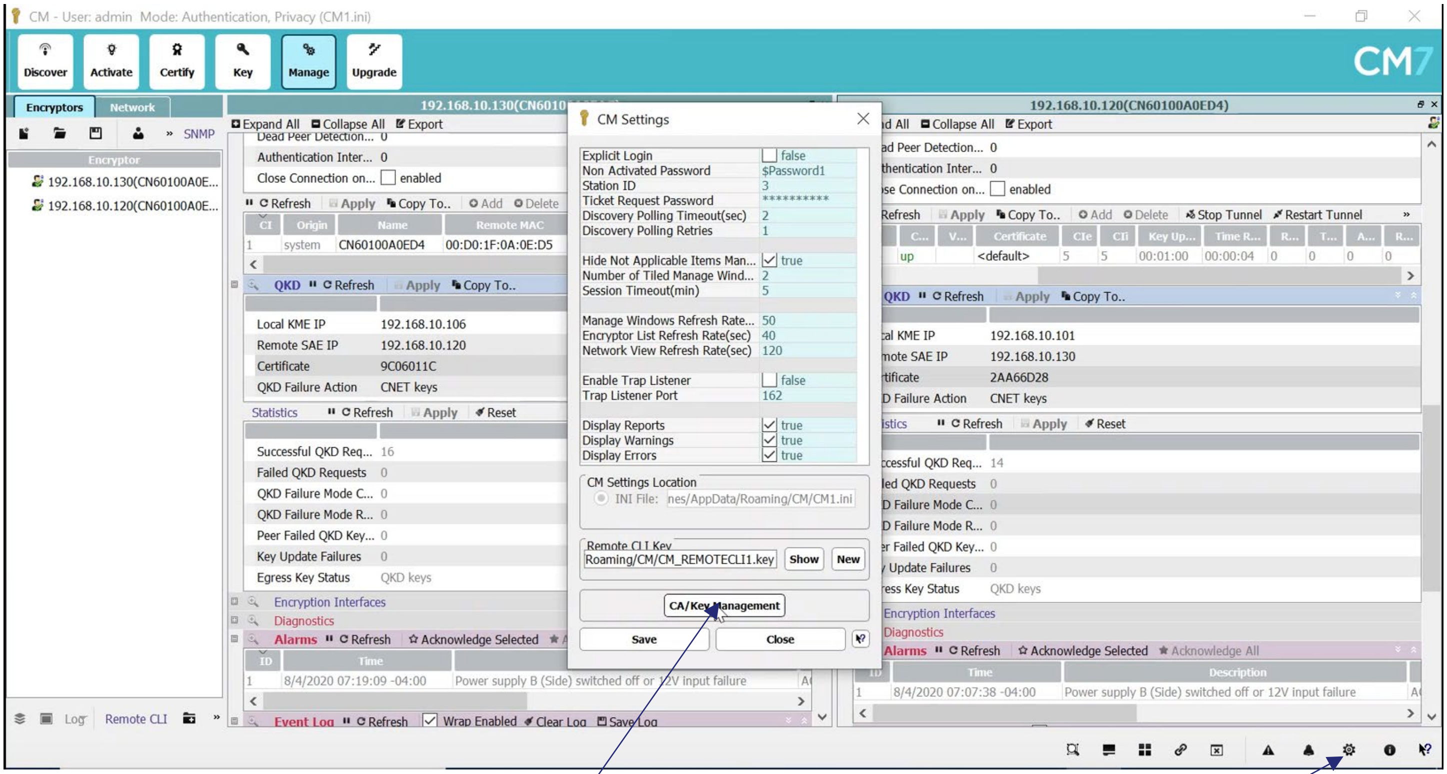
You will have the following files created in your linux directory:
QKDServer.csr QKDServer.pkey

Rename the xxx.csr file to xxx_csr.pem
Rename the xxx.pkey file to xxx_pkey.pem

In Linux type:

```
mv QKDServer.csr QKDServer_csr.pem
mv QKDServer.pkey QKDServer_pkey.pem
```

Next we need to sign the .pem with CM7. This will generate a xxxx_cert.pem file



CM - User: admin Mode: Authentication, Privacy (CM1.ini)

192.168.10.130(CN6010…

Dead Peer Detection...	0
Authentication Inter...	0
Close Connection on...	□ enabled

CI	Origin	Name	Remote MAC
1	system	CN60100A0ED4	00:D0:1F:0A:0E:D5

QKD

Local KME IP	192.168.10.106
Remote SAE IP	192.168.10.120
Certificate	9C06011C
QKD Failure Action	CNET keys

Statistics

Successful QKD Req...	16
Failed QKD Requests	0
QKD Failure Mode C...	0
QKD Failure Mode R...	0
Peer Failed QKD Key...	0
Key Update Failures	0
Egress Key Status	QKD keys

Encryption Interfaces
Diagnostics
Alarms

ID	Time	
1	8/4/2020 07:19:09 -04:00	Power supply B (Side) switched off or 12V input failure

Event Log ☑ Wrap Enabled Clear Log Save Log

CM Settings

Explicit Login	□ false
Non Activated Password	$Password1
Station ID	3
Ticket Request Password	**********
Discovery Polling Timeout(sec)	2
Discovery Polling Retries	1
Hide Not Applicable Items Man...	☑ true
Number of Tiled Manage Wind...	2
Session Timeout(min)	5
Manage Windows Refresh Rate...	50
Encryptor List Refresh Rate(sec)	40
Network View Refresh Rate(sec)	120
Enable Trap Listener	□ false
Trap Listener Port	162
Display Reports	☑ true
Display Warnings	☑ true
Display Errors	☑ true

CM Settings Location
○ INI File: nes/AppData/Roaming/CM/CM1.ini

Remote CLI Key
Roaming/CM/CM_REMOTECLI1.key Show New

CA/Key Management

Save Close

192.168.10.120(CN60100A0ED4)

Dead Peer Detection...	0
Authentication Inter...	0
Close Connection on...	□ enabled

C...	V...	Certificate	CIe	CIi	Key Up...	Time R...	R...	T...	A...	R...
up		<default>	5	5	00:01:00	00:00:04	0	0	0	0

QKD

Local KME IP	192.168.10.101
Remote SAE IP	192.168.10.130
Certificate	2AA66D28
QKD Failure Action	CNET keys

Statistics

Successful QKD Req...	14
Failed QKD Requests	0
QKD Failure Mode C...	0
QKD Failure Mode R...	0
Peer Failed QKD Key...	0
Key Update Failures	0
Egress Key Status	QKD keys

Encryption Interfaces
Diagnostics
Alarms

ID	Time	Description
1	8/4/2020 07:07:38 -04:00	Power supply B (Side) switched off or 12V input failure

1) Click Settings

2) Click CA/Key

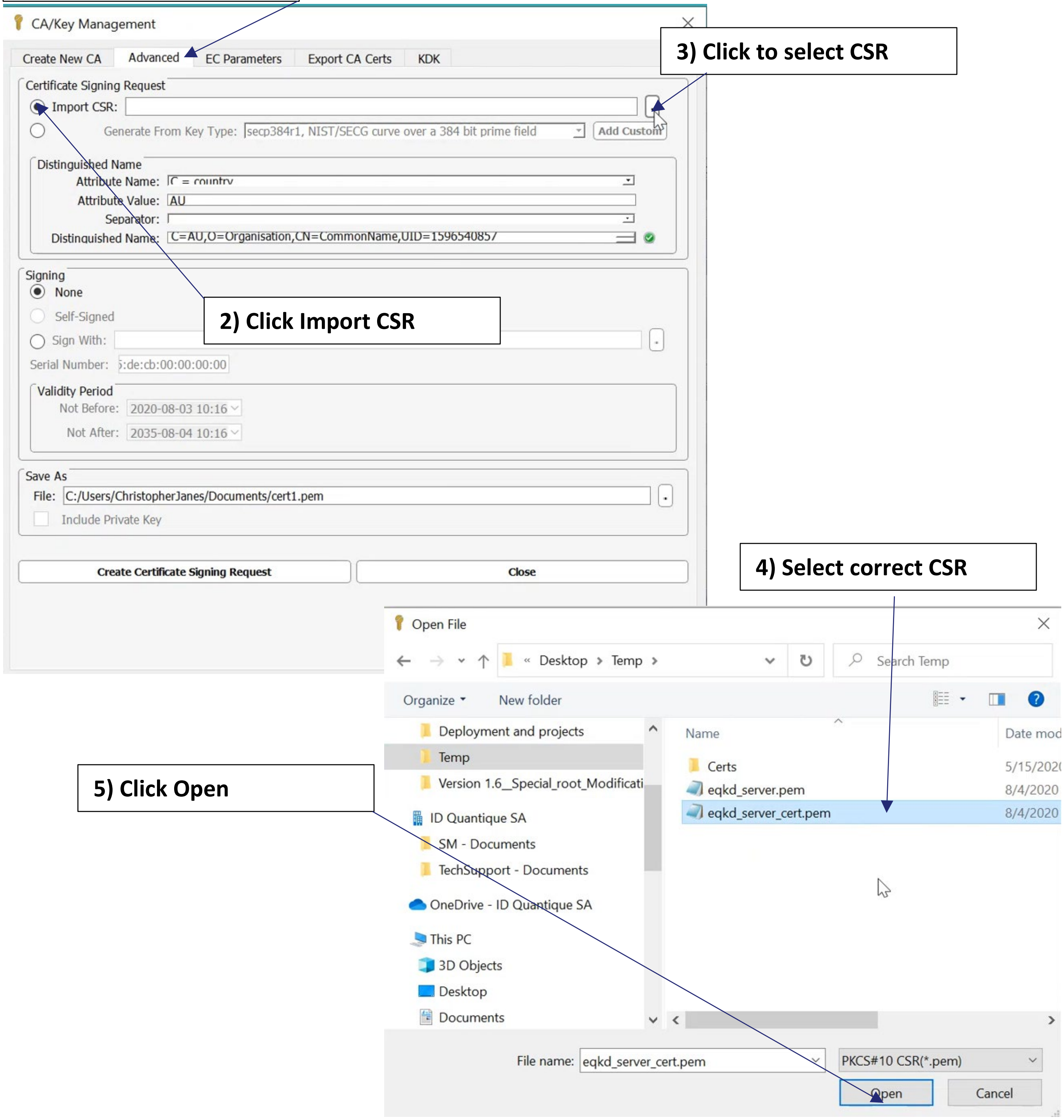
1) Click Advanced

3) Click to select CSR

2) Click Import CSR

4) Select correct CSR

5) Click Open



CA/Key Management

Certificate Signing Request

● Import CSR:

○ Generate From Key Type: secp384r1, NIST/SECG curve over a 384 bit prime field

Distinguished Name

Attribute Name: C = country

Attribute Value: AU

Separator:

Distinguished Name: C=AU,O=Organisation,CN=CommonName,UID=1596540857

Signing

● None

○ Self-Signed

○ Sign With:

Serial Number: 5:de:cb:00:00:00:00

Validity Period

Not Before: 2020-08-03 10:16

Not After: 2035-08-04 10:16

Save As

File: C:/Users/ChristopherJanes/Documents/cert1.pem

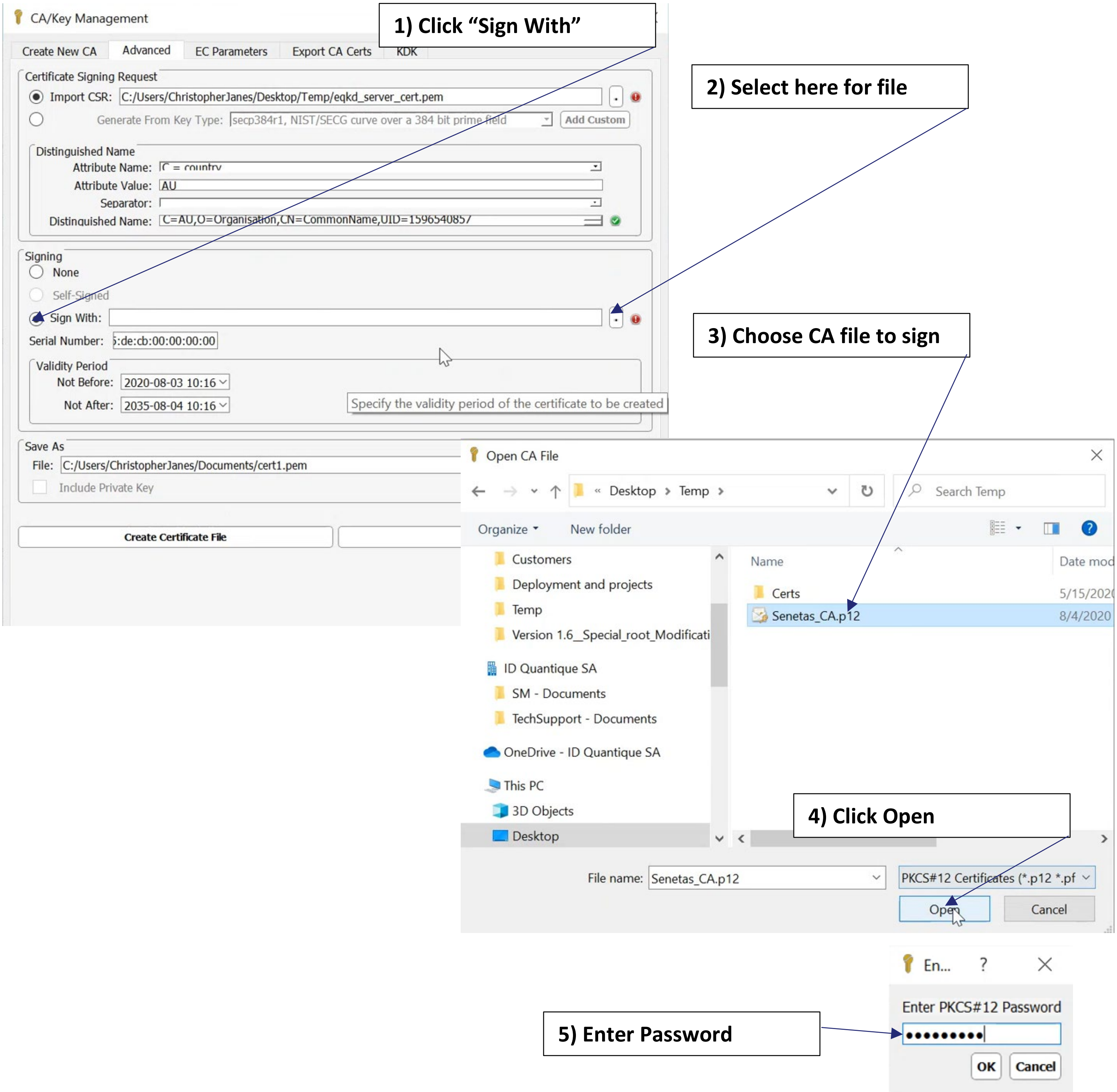
□ Include Private Key

Open File

Name	Date mod
Certs	5/15/202(
eqkd_server.pem	8/4/2020
eqkd_server_cert.pem	8/4/2020

File name: eqkd_server_cert.pem

PKCS#10 CSR(*.pem)



1) Click “Sign With”

2) Select here for file

3) Choose CA file to sign

4) Click Open

5) Enter Password

CA/Key Management

Create New CA | Advanced | EC Parameters | Export CA Certs | KDK

Certificate Signing Request

● Import CSR: C:/Users/ChristopherJanes/Desktop/Temp/eqkd_server_cert.pem

○ Generate From Key Type: secp384r1, NIST/SECG curve over a 384 bit prime field | Add Custom

Distinguished Name

Attribute Name: C = country

Attribute Value: AU

Separator:

Distinguished Name: C=AU,O=Organisation,CN=CommonName,UID=1596540857

Signing

○ None

○ Self-Signed

● Sign With:

Serial Number: 5:de:cb:00:00:00:00

Validity Period

Not Before: 2020-08-03 10:16

Not After: 2035-08-04 10:16

Specify the validity period of the certificate to be created

Save As

File: C:/Users/ChristopherJanes/Documents/cert1.pem

□ Include Private Key

Create Certificate File

Open CA File

« Desktop › Temp ›

Search Temp

Organize ▾ New folder

Name	Date mod
Certs	5/15/2020
Senetas_CA.p12	8/4/2020

File name: Senetas_CA.p12

PKCS#12 Certificates (*.p12 *.pf

Open | Cancel

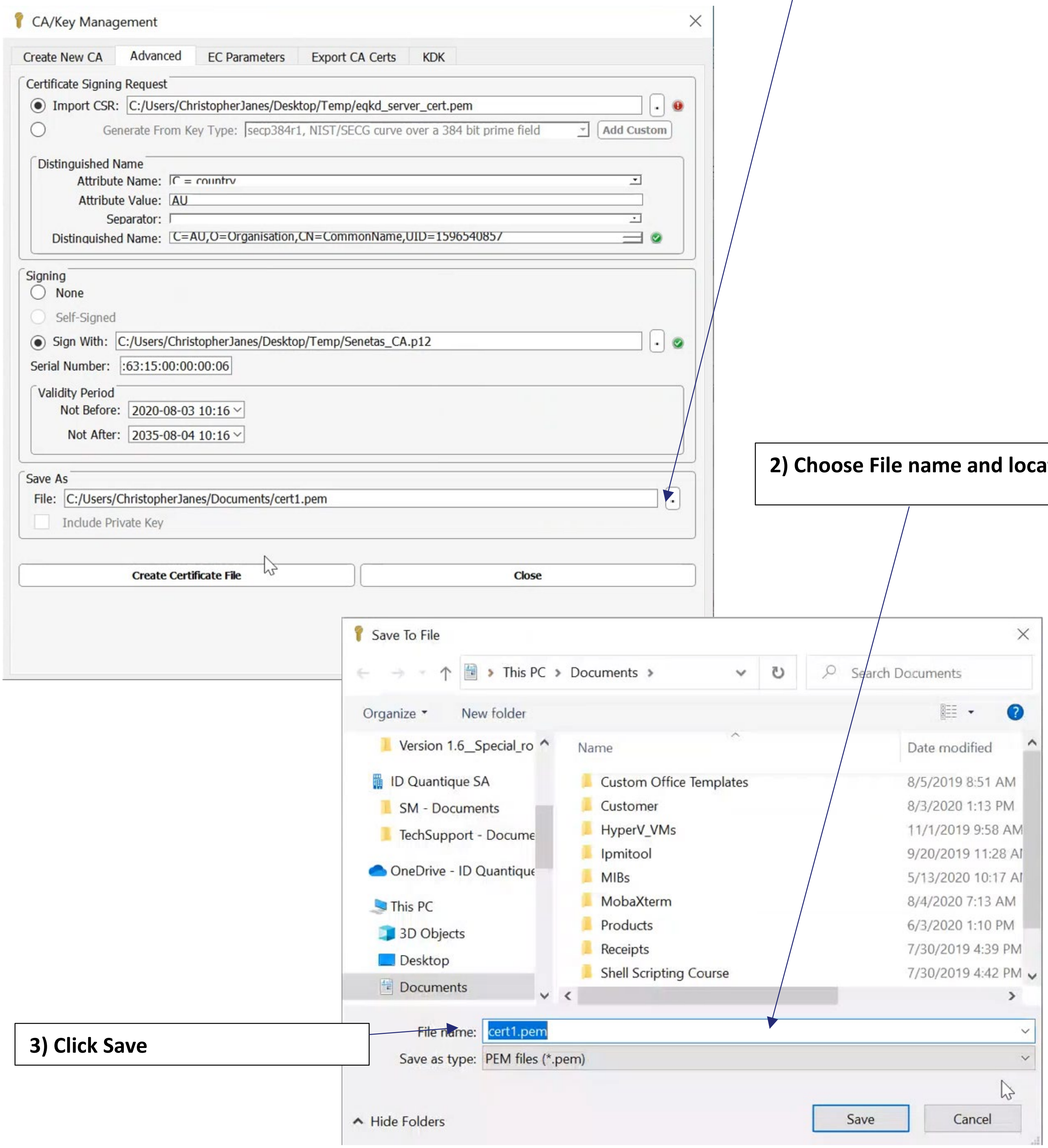
En... ?

Enter PKCS#12 Password

●●●●●●●●●

OK | Cancel

1) Select location to save



CA/Key Management

Certificate Signing Request

● Import CSR: C:/Users/ChristopherJanes/Desktop/Temp/eqkd_server_cert.pem

○ Generate From Key Type: secp384r1, NIST/SECG curve over a 384 bit prime field [Add Custom]

Distinguished Name

Attribute Name: C = country

Attribute Value: AU

Separator:

Distinguished Name: C=AU,O=Organisation,CN=CommonName,UID=1596540857

Signing

○ None

○ Self-Signed

● Sign With: C:/Users/ChristopherJanes/Desktop/Temp/Senetas_CA.p12

Serial Number: :63:15:00:00:00:06

Validity Period

Not Before: 2020-08-03 10:16

Not After: 2035-08-04 10:16

Save As

File: C:/Users/ChristopherJanes/Documents/cert1.pem

□ Include Private Key

Save To File

This PC › Documents ›

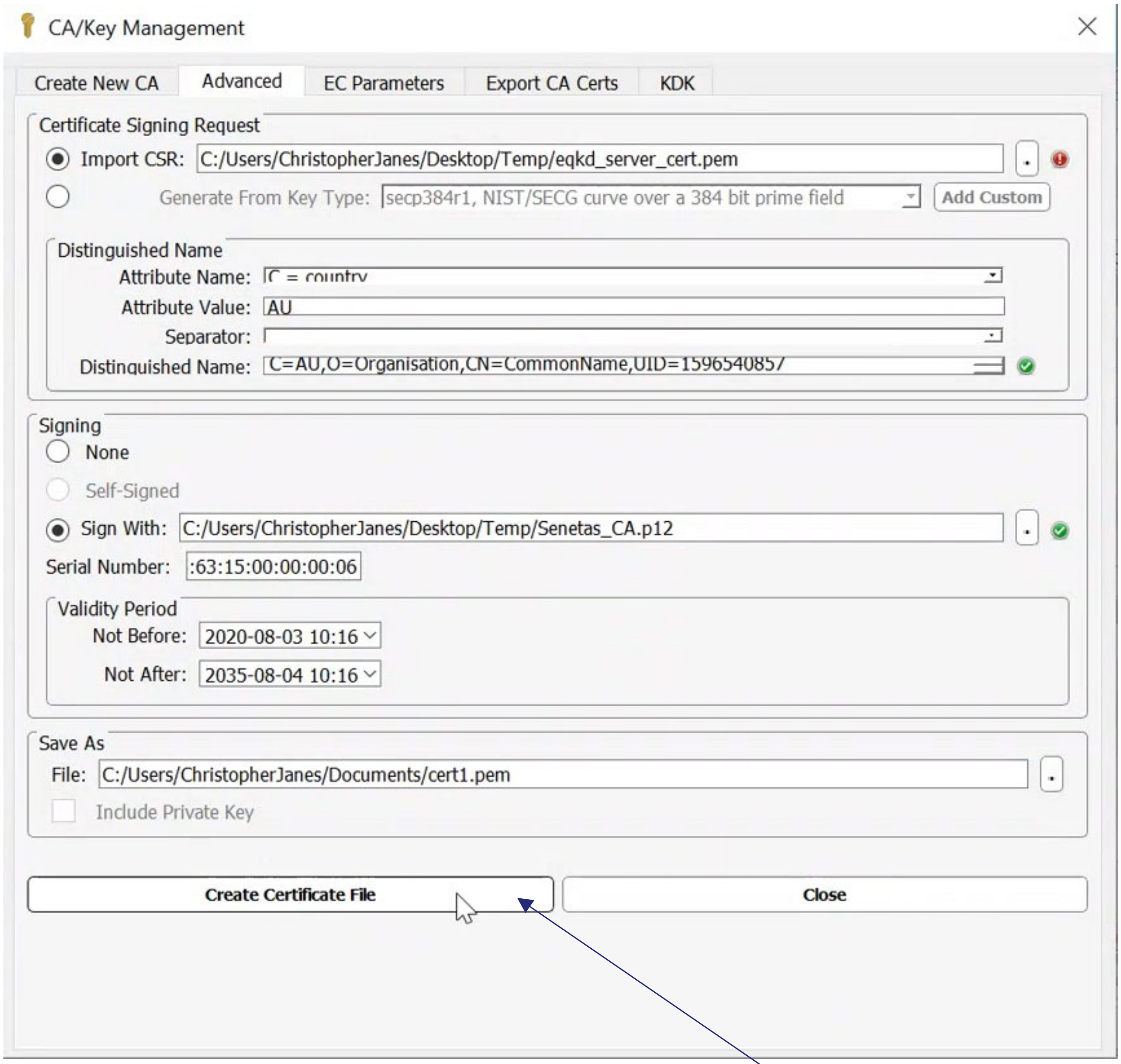
Name	Date modified
Custom Office Templates	8/5/2019 8:51 AM
Customer	8/3/2020 1:13 PM
HyperV_VMs	11/1/2019 9:58 AM
Ipmitool	9/20/2019 11:28 AI
MIBs	5/13/2020 10:17 AI
MobaXterm	8/4/2020 7:13 AM
Products	6/3/2020 1:10 PM
Receipts	7/30/2019 4:39 PM
Shell Scripting Course	7/30/2019 4:42 PM

File name: cert1.pem

Save as type: PEM files (*.pem)

2) Choose File name and location

3) Click Save



CA/Key Management

Certificate Signing Request

● Import CSR: C:/Users/ChristopherJanes/Desktop/Temp/eqkd_server_cert.pem

○ Generate From Key Type: secp384r1, NIST/SECG curve over a 384 bit prime field

Distinguished Name

Attribute Name: C = country

Attribute Value: AU

Separator:

Distinguished Name: C=AU,O=Organisation,CN=CommonName,UID=1596540857

Signing

○ None

○ Self-Signed

● Sign With: C:/Users/ChristopherJanes/Desktop/Temp/Senetas_CA.p12

Serial Number: :63:15:00:00:00:06

Validity Period

Not Before: 2020-08-03 10:16

Not After: 2035-08-04 10:16

Save As

File: C:/Users/ChristopherJanes/Documents/cert1.pem

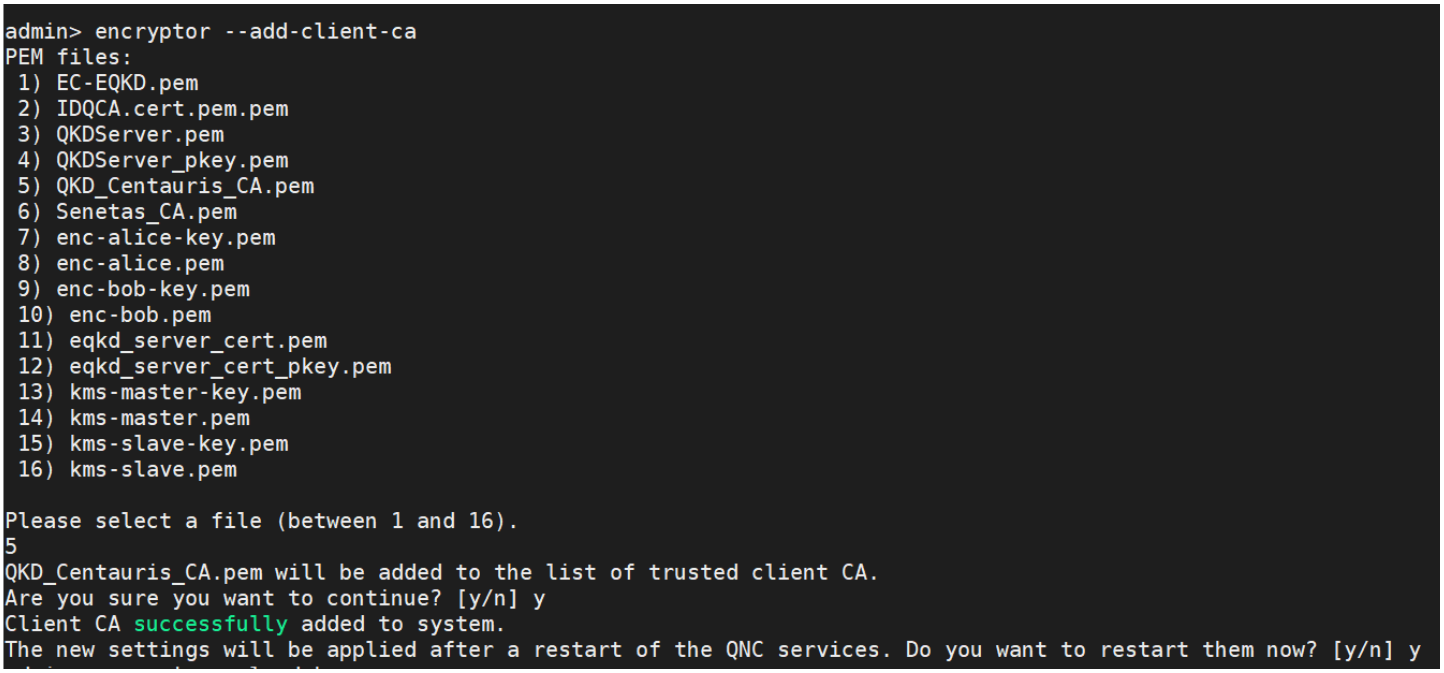
□ Include Private Key

1) Click Create Certificate File

Matching CA, Certificates & Keys on QKD System

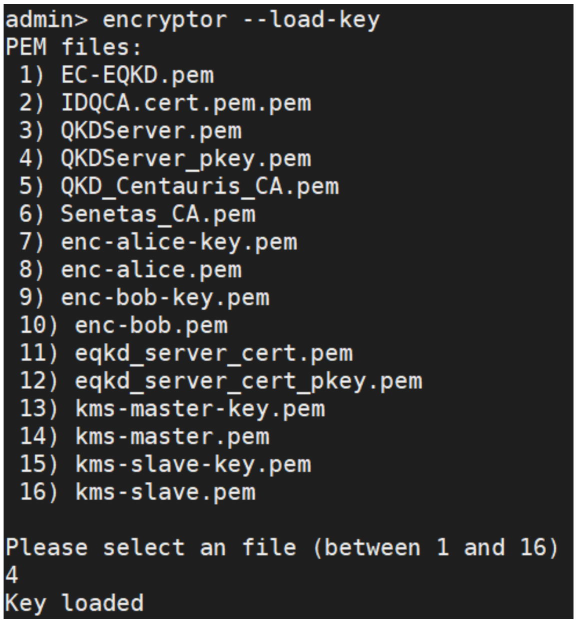
You will need to install the matching CA and server certificates & keys into the QNC. Please refer to the Cerberis3 User Guide and KEMS Configuration Guide briefly described next.

Import the root CA, server certificate and server key as usual:
Do this on both Alice and Bob QNC:

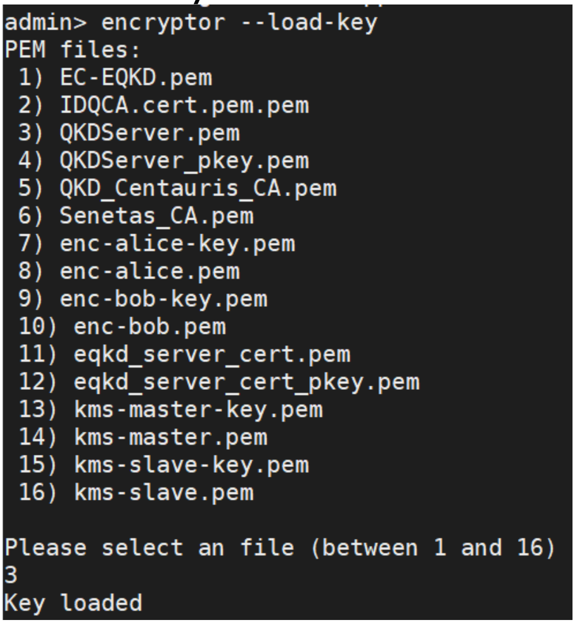


```
admin> encryptor --add-client-ca
PEM files:
 1) EC-EQKD.pem
 2) IDQCA.cert.pem.pem
 3) QKDServer.pem
 4) QKDServer_pkey.pem
 5) QKD_Centauris_CA.pem
 6) Senetas_CA.pem
 7) enc-alice-key.pem
 8) enc-alice.pem
 9) enc-bob-key.pem
 10) enc-bob.pem
 11) eqkd_server_cert.pem
 12) eqkd_server_cert_pkey.pem
 13) kms-master-key.pem
 14) kms-master.pem
 15) kms-slave-key.pem
 16) kms-slave.pem

Please select a file (between 1 and 16).
5
QKD_Centauris_CA.pem will be added to the list of trusted client CA.
Are you sure you want to continue? [y/n] y
Client CA successfully added to system.
The new settings will be applied after a restart of the QNC services. Do you want to restart them now? [y/n] y
```

Load both certificate and key:

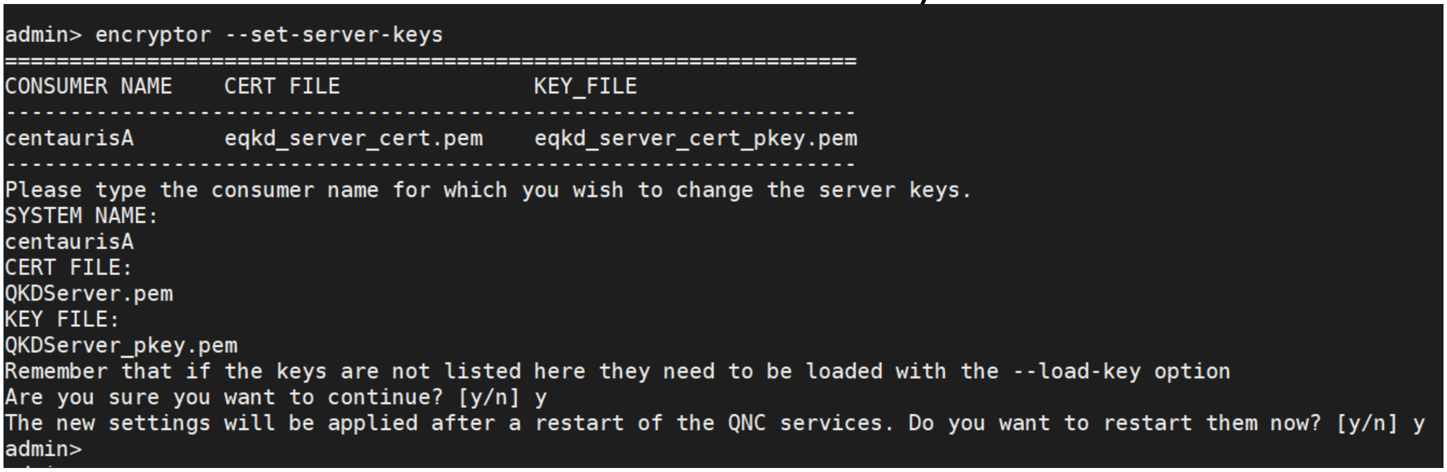


```
admin> encryptor --load-key
PEM files:
 1) EC-EQKD.pem
 2) IDQCA.cert.pem.pem
 3) QKDServer.pem
 4) QKDServer_pkey.pem
 5) QKD_Centauris_CA.pem
 6) Senetas_CA.pem
 7) enc-alice-key.pem
 8) enc-alice.pem
 9) enc-bob-key.pem
 10) enc-bob.pem
 11) eqkd_server_cert.pem
 12) eqkd_server_cert_pkey.pem
 13) kms-master-key.pem
 14) kms-master.pem
 15) kms-slave-key.pem
 16) kms-slave.pem

Please select an file (between 1 and 16)
4
Key loaded
```



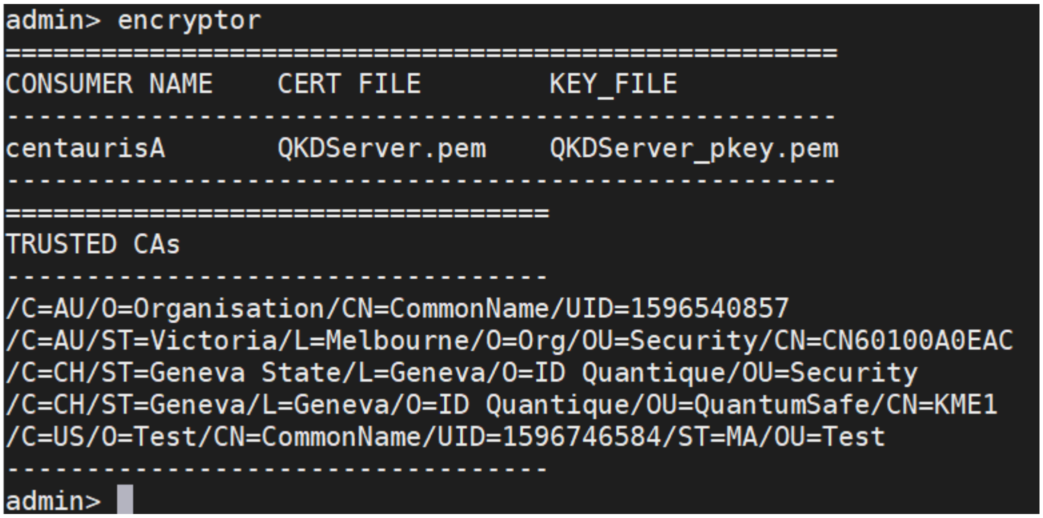
```
admin> encryptor --load-key
PEM files:
 1) EC-EQKD.pem
 2) IDQCA.cert.pem.pem
 3) QKDServer.pem
 4) QKDServer_pkey.pem
 5) QKD_Centauris_CA.pem
 6) Senetas_CA.pem
 7) enc-alice-key.pem
 8) enc-alice.pem
 9) enc-bob-key.pem
 10) enc-bob.pem
 11) eqkd_server_cert.pem
 12) eqkd_server_cert_pkey.pem
 13) kms-master-key.pem
 14) kms-master.pem
 15) kms-slave-key.pem
 16) kms-slave.pem

Please select an file (between 1 and 16)
3
Key loaded
```

Set Server Certificate and Key

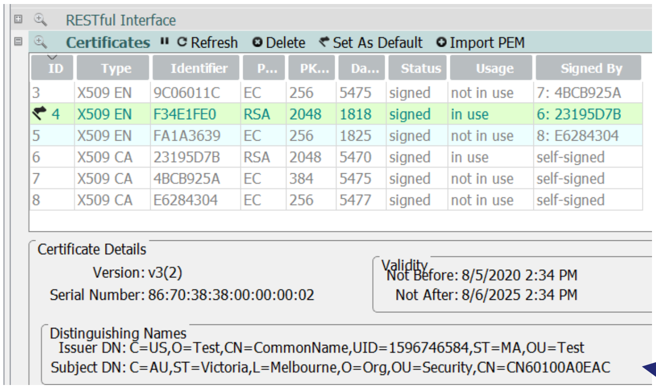


```
admin> encryptor --set-server-keys
==================================================================
CONSUMER NAME    CERT FILE               KEY_FILE
------------------------------------------------------------------
centaurisA       eqkd_server_cert.pem    eqkd_server_cert_pkey.pem
------------------------------------------------------------------
Please type the consumer name for which you wish to change the server keys.
SYSTEM NAME:
centaurisA
CERT FILE:
QKDServer.pem
KEY FILE:
QKDServer_pkey.pem
Remember that if the keys are not listed here they need to be loaded with the --load-key option
Are you sure you want to continue? [y/n] y
The new settings will be applied after a restart of the QNC services. Do you want to restart them now? [y/n] y
admin>
```

Verify



```
admin> encryptor
====================================================
CONSUMER NAME    CERT FILE        KEY_FILE
----------------------------------------------------
centaurisA       QKDServer.pem    QKDServer_pkey.pem
----------------------------------------------------
==================================
TRUSTED CAs
----------------------------------
/C=AU/O=Organisation/CN=CommonName/UID=1596540857
/C=AU/ST=Victoria/L=Melbourne/O=Org/OU=Security/CN=CN60100A0EAC
/C=CH/ST=Geneva State/L=Geneva/O=ID Quantique/OU=Security
/C=CH/ST=Geneva/L=Geneva/O=ID Quantique/OU=QuantumSafe/CN=KME1
/C=US/O=Test/CN=CommonName/UID=1596746584/ST=MA/OU=Test
----------------------------------
admin>
```



ID	Type	Identifier	P...	PK...	Da...	Status	Usage	Signed By
3	X509 EN	9C06011C	EC	256	5475	signed	not in use	7: 4BCB925A
4	X509 EN	F34E1FE0	RSA	2048	1818	signed	in use	6: 23195D7B
5	X509 EN	FA1A3639	EC	256	1825	signed	not in use	8: E6284304
6	X509 CA	23195D7B	RSA	2048	5470	signed	in use	self-signed
7	X509 CA	4BCB925A	EC	384	5475	signed	not in use	self-signed
8	X509 CA	E6284304	EC	256	5477	signed	not in use	self-signed

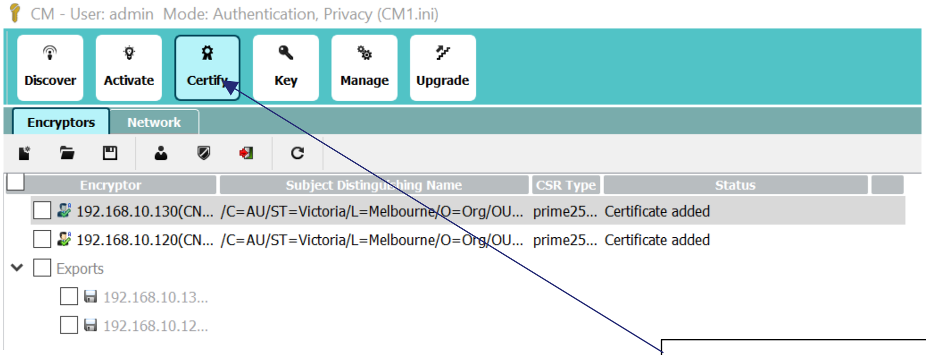
Certificate Details

Version: v3(2)
Serial Number: 86:70:38:38:00:00:00:02

Validity
Not Before: 8/5/2020 2:34 PM
Not After: 8/6/2025 2:34 PM

Distinguishing Names
Issuer DN: C=US,O=Test,CN=CommonName,UID=1596746584,ST=MA,OU=Test
Subject DN: C=AU,ST=Victoria,L=Melbourne,O=Org,OU=Security,CN=CN60100A0EAC

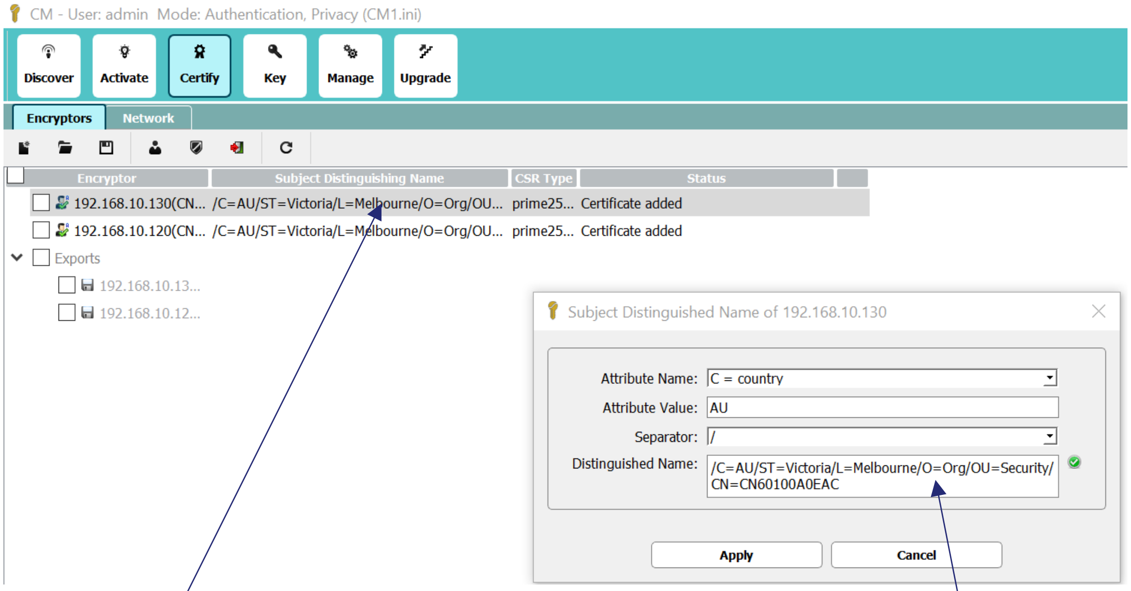
1) We need to copy the Subject DN from the client certificate to configure in KEMS Consumer (copy/paste won't work here)



Encryptor	Subject Distinguishing Name	CSR Type	Status
□ 192.168.10.130(CN...	/C=AU/ST=Victoria/L=Melbourne/O=Org/OU...	prime25...	Certificate added
□ 192.168.10.120(CN...	/C=AU/ST=Victoria/L=Melbourne/O=Org/OU...	prime25...	Certificate added

□ Exports
□ 192.168.10.13...
□ 192.168.10.12...

2) Click on Certify



CM - User: admin Mode: Authentication, Privacy (CM1.ini)

Encryptor	Subject Distinguishing Name	CSR Type	Status
□ 192.168.10.130(CN...	/C=AU/ST=Victoria/L=Melbourne/O=Org/OU...	prime25...	Certificate added
□ 192.168.10.120(CN...	/C=AU/ST=Victoria/L=Melbourne/O=Org/OU...	prime25...	Certificate added

□ Exports
- □ 192.168.10.13...
- □ 192.168.10.12...

Subject Distinguished Name of 192.168.10.130

Attribute Name: C = country

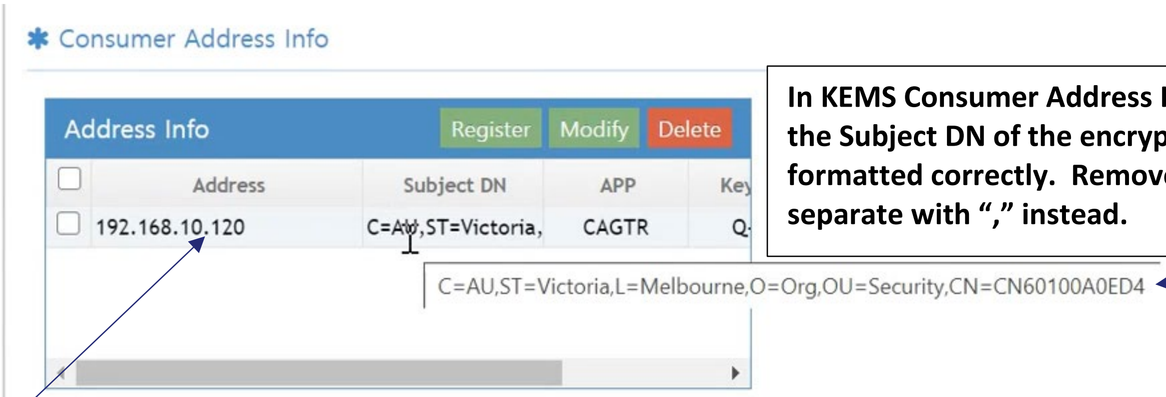
Attribute Value: AU

Separator: /

Distinguished Name: /C=AU/ST=Victoria/L=Melbourne/O=Org/OU=Security/CN=CN60100A0EAC

1) Click on the Encryptor/Subject DN

2) Copy the Subject DN
(Remember we need to re-format this without "/")



□	Address	Subject DN	APP	Key
□	192.168.10.120	C=AU,ST=Victoria,	CAGTR	Q-

C=AU,ST=Victoria,L=Melbourne,O=Org,OU=Security,CN=CN60100A0ED4

In KEMS Consumer Address Info: Make sure the Subject DN of the encryptor certificate is formatted correctly. Remove the "/" and separate with "," instead.

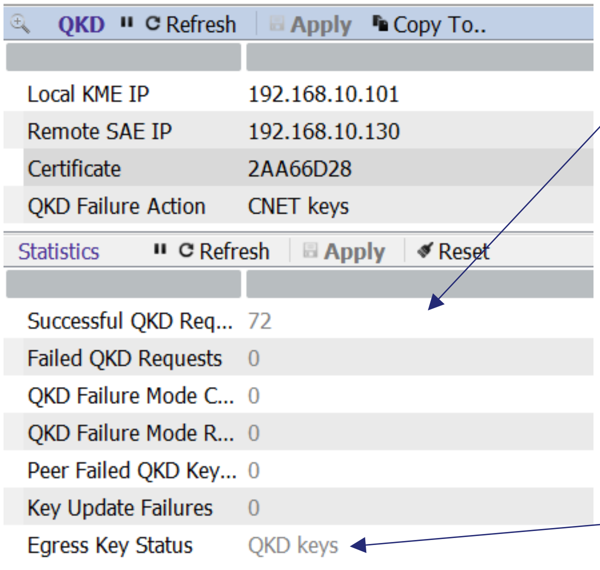
SAE Address for Thales Encryptor should be the IP address of the encryptor

eQKD Statistics

Use the eQKD statistics to verify successful key ingestion using ETSI

Statistics:

The statistics and current status displays relevant details for the current QKD connection. The egress key status should read CNET keys during normal operation.



Local KME IP	192.168.10.101
Remote SAE IP	192.168.10.130
Certificate	2AA66D28
QKD Failure Action	CNET keys

Successful QKD Req...	72
Failed QKD Requests	0
QKD Failure Mode C...	0
QKD Failure Mode R...	0
Peer Failed QKD Key...	0
Key Update Failures	0
Egress Key Status	QKD keys

Verify Successful QKD Requests

Verify we are getting QKD Keys and not

End of Configuration Document