HITACHI
Inspire the Next

APPLICATION NOTE

FOXMAN-UN
DIRAC Certificates Recreation

Hitachi Energy

Document ID	1KHW029159	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-06-03

Copyright and confidentiality

Disclaimer

This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.
Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.
All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.
Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.
The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Preface & Introduction

This Application Note covers the FOXMAN-UN add-on

- DIRAC (Encryption key manager)

with respect to the key recreation procedure. It provides some useful information related to the DIRAC certificates and guides you to execute a recreation of these certificates in case they are going to expire or have expired.

In this document it is assumed that you are familiar with the basics of FOXMAN-UN and DIRAC, and that you have read the DIRAC user manuals [1KHW029081] User Manual “DIRAC R18 - DIRAC Server Installation” and [1KHW029082] User Manual “DIRAC R18 - DIRAC Server Operation”.

2 Certificates

The following certificates are present/created when you install DIRAC. Certificates are created at installation time under:

/etc/pki/dirac

2.1 Certification Authority

diracCA.crt
diracCA.srl (serial number of generated certificates)

2.2 Server

server.crt
server.key
server_keystore.p12 (key store with certificate and CA)
server_truststore.jks

2.3 CLI

cli.pem (private key of cli, as DIRAC client)
cli.crt (public certificate of cli, signed by diracCA)
cli_keystore.p12 (key store with certificate and CA)

2.4 NEM

nem.pem (private key of nem, as DIRAC client)
nem.crt (public certificate of cli, signed by diracCA)
(Nem requires also diracCA.crt, to trust on it)

nem.p12: required for nms api gateway

2.5 GRPC

dirac.cer (public certificate for communication DIRAC-SENC1)
dirac.key (private key for communication DIRAC-SENC1).

3 Alarming

You receive a FOXMAN-UN System Alarm in the following to cases:

- When the certificate on server_keystore (server.crt) is about to expire (100 days before effective expiry date);
- When the certificate has expired.

4 Certificates to update

The following certificates have an expiry date.

- The DIRAC/FOXMAN-UN certificates are located under

  /etc/pki/dirac

Example:

```
[dirac@nmssrv ~]$ ls -l /etc/pki/dirac/*.crt
-rw-r-----. 1 dirac dirac 1281 Apr 22 08:14 /etc/pki/dirac/cli.crt
-rw-r-----. 1 dirac dirac 1415 Apr 22 08:14 /etc/pki/dirac/diracCA.crt
-rw-r-----. 1 dirac dirac 1281 Apr 22 08:14 /etc/pki/dirac/nem.crt
-rw-r-----. 1 dirac dirac 1415 Apr 22 08:14 /etc/pki/dirac/server.crt
```

NEM related certificates are also copied under /opt/nem/etc/enpsec/ (these files are created/ copied when you install DIRAC on the system):

```
[dirac@nmssrv ~]$ ll /opt/nem/etc/enpsec/
-rw-r--r--. 1 nemadm nem 1415 Apr 28 18:32 diracCA.crt
-rw-r--r--. 1 nemadm nem 1281 Apr 28 18:32 nem.crt
-rw-r--r--. 1 nemadm nem 2509 Apr 28 18:32 nem.p12
-rw-r--r--. 1 nemadm nem 1708 Apr 28 18:32 nem.pem
```

Verify the certificates validity (all of them will have the same expiry date as per installation). For cli.crt for example:

```
[dirac@nmssrv ~]$ openssl x509 -noout -dates -in /etc/pki/dirac/cli.crt
notBefore=Apr 22 06:14:53 2021 GMT
notAfter=Apr 20 06:14:53 2031 GMT
```

5 Generate new certificates

Generate new certificates as dirac user:

Proceed as follows:

Instruction for recreating DIRAC certificates (follow all steps from Backup of current certificates and cleanup of folder until and including Restart components and test):

5.1 Backup of current certificates and cleanup of folder

Execute the following commands:

```
[dirac@nmssrv ~]$ mkdir  /etc/pki/dirac/temp/
[dirac@nmssrv ~]$ mv /etc/pki/dirac/* /etc/pki/dirac/temp/
[dirac@nmssrv ~]$ cp /etc/pki/dirac/temp/server.key /etc/pki/dirac/
```

5.2 Updating certificates

The only file present in the folder

/etc/pki/dirac/

is “server.key” (our private key to generate all certificates):

```
[dirac@nmssrv ~]$ cd /etc/pki/dirac/
[dirac@nmssrv ~]$ ls -l
-rw-r-----. 1 dirac dirac 1704 May 5 06:17 server.key
```

5.2.1 Server keystore & truststore generation

Regenerate server.crt out of the server.key (please do not change CN):

```
openssl req -x509 -key server.key -out ./server.crt -days 3650 -nodes -
subj "/C=CH/ST=Berne/L=Berne/O=Hitachi Power Grids Switzerland Ltd./
OU=PGGA,PG/CN=localhost"
```

We will use also the server certificate as certification authority for all other generated certificates:

```
cp server.crt diracCA.crt
```

We add serverCA to the trust store:

```
keytool -noprompt -import -file diracCA.crt -alias diracCA -keystore
server_truststore.jks -storepass changeit
```

And we create a PKCS12 keystore containing private key and related self-sign certificate:

```
openssl pkcs12 -export -password pass:changeit -in diracCA.crt -inkey
server.key -out server_keystore.p12
```

At the end of this step we should have following files:

```
[dirac@nmssrv dirac]$ ll
-rw-rw-r--. 1 dirac dirac 1415 May 5 06:28 diracCA.crt
-rw-rw-r--. 1 dirac dirac 1415 May 5 06:19 server.crt
-rw-r-----. 1 dirac dirac 1704 May 5 06:17 server.key
-rw-------. 1 dirac dirac 2605 May 5 06:29 server_keystore.p12
-rw-rw-r--. 1 dirac dirac 1298 May 5 06:29 server_truststore.jks
```

5.2.2 CLI certificate generation

Generate client's private key and a certificate signing request (CSR) (please do not change CN):

```
openssl req -new -newkey rsa:2048 -out cli.csr -subj "/C=CH/ST=Berne/
L=Berne/O=Hitachi Power Grids Switzerland Ltd./OU=PGGA,PG/CN=cli" -
keyout cli.pem -nodes
```

Sign client's CSR with server private key and a create related certificate:

```
openssl x509 -req -days 3650 -sha256 -in cli.csr -CA diracCA.crt -CAkey
server.key -CAcreateserial -out cli.crt
```

Delete CSR:

```
rm cli.csr
```

We have now following new files in our folder:

```
-rw-rw-r--. 1 dirac dirac 1281 May 5 06:34 cli.crt
-rw-------. 1 dirac dirac 1704 May 5 06:32 cli.pem
-rw-rw-r--. 1 dirac dirac 41 May 5 06:34 diracCA.srl
```

5.2.3 NEM certificate generation

Generate client's private key and a certificate signing request (CSR) (please do not change CN):

```
openssl req -new -newkey rsa:2048 -out nem.csr -subj "/C=CH/ST=Berne/
L=Berne/O=Hitachi Power Grids Switzerland Ltd./OU=PGGA,PG/CN=nem" -
keyout nem.pem -nodes
```

Sign nem's CSR with server private key and a related certificate

```
openssl x509 -req -days 3650 -sha256 -in nem.csr -CA diracCA.crt -CAkey
server.key -CAserial diracCA.srl -out nem.crt
```

Delete CSR:

```
rm nem.csr
```

Generate p12 store for NMS apigateway

```
openssl pkcs12 -export -password pass:changeit -in nem.crt -inkey
nem.pem -out nem.p12
```

Curl client in FOXMAN-UN does require the nem.pem, nem.crt and diracCA.crt files.
We have now following new files in the folder `/etc/pki/`:

```
-rw-rw-r--. 1 dirac dirac 1281 May 5 06:40 nem.crt
-rw-------. 1 dirac dirac 2509 May 5 06:41 nem.p12
-rw-------. 1 dirac dirac 1708 May 5 06:39 nem.pem
```

5.2.4 Making NEM aware of new certificates

The following files are required by NMS:

- curl client in FOXMAN-UN requires the nem.pem, nem.crt and diracCA.crt files
- nms api gateway requires the nem.p12 store

Make a backup of all your files in `enpsec` folder (as a NEM administrator user):

```
mkdir /opt/nem/etc/enpsec/backup
mv /opt/nem/etc/enpsec/nem* /opt/nem/etc/enpsec/backup/
mv /opt/nem/etc/enpsec/dirac* /opt/nem/etc/enpsec/backup/
```

You'll need now a user with access to NEM generated certificates, or you can ask dirac user to provide them to you.

```
sudo cp /etc/pki/dirac/nem.* /opt/nem/etc/enpsec/
sudo cp /etc/pki/dirac/diracCA.crt /opt/nem/etc/enpsec/
```

Then change ownership:

```
sudo chown nemadm:nem /opt/nem/etc/enpsec/*
```

5.2.5 Restart components and test

As dirac user, restart DIRAC:

```
diracstop; diracstart
```

Check you can use new certificates:

```
curl -ik https://localhost:9343/api/v2.0/functionalunits --cert /etc/
pki/dirac/cli.crt --key /etc/pki/dirac/cli.pem
```

As a NEM administrator user, restart FOXMAN-UN:

```
nembasestop; nemstart
```

Check you can use new certificates:

```
curl -ik https://localhost:9343/api/v2.0/functionalunits --cert /opt/
nem/etc/enpsec/nem.crt --key /opt/nem/etc/enpsec/nem.pem
```

End of instruction

6 Annex

6.1 Associated Documents

[1KHW029081] User Manual “DIRAC R18 - DIRAC Server Installation”

[1KHW029082] User Manual “DIRAC R18 - DIRAC Server Operation”

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to https://www.hitachienergy.com/contact-us/Customer-Connect-Center (Customer Connect Center)
Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks

Document ID: 1KHW029159 R18 Rev. A