Digital Energy
MDS

APPLICATION BULLETIN

NUMBER: AB14002_A
June 2014

MDS Orbit MCR Series

GE MDS, LLC. 175 Science Parkway, Rochester, NY 14620 USA
Phone +1 (585) 242-9600, FAX +1 (585) 242-9620 Web: www.gemds.com

Generating RSA Keys and X.509 Certificates

Using OpenSSL

Introduction

This document describes how to generate RSA keys and X.509 certificates using OpenSSL tool for use with various services on Orbit (like IPsec VPN).

Scope

This bulletin is intended for network administrators and end users who would like to generate keys and certificates. Orbit MCR requires this material for secure services such as IPsec VPN. Note that the key and certificate generation techniques described here are standard and not specific to the Orbit product line.

Terms

CA	Certificate Authority

General Notes

The OpenSSL utility is available on many platforms (Windows, Linux etc.).

Windows

Install OpenSSL by installing following packages (in specified order):

a. Visual C++ 2008 Redistributables package (http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF)

b. Win32 OpenSSL v1.0.1g Light (http://slproweb.com/download/Win32OpenSSL_Light-1_0_1g.exe)

NOTE: Add “c:\OpenSSL-Win32\bin” to PATH environment variable to make “openssl” command accessible from command prompt.

Ubuntu Linux

Install OpenSSL as follows:

```
$ sudo apt-get install openssl
```

Generating CA Key and Certificate

1. Generate RSA key for root CA with length of 4096 bits.

```
C:\Temp\pki>openssl genrsa -out ca.key 4096
Loading 'screen' into random state - done
Generating RSA private key, 4096 bit long modulus
........++
..............................................................................
..............................................++
unable to write 'random state'
e is 65537 (0x10001)
```

2. Generate self-signed certificate for root CA with validity of 10 years, Common Name = TEST-CA.

NOTE: Press “return” key on fields that you want to leave blank (like Locality, Email Address)

```
C:\Temp\pki>openssl req -new -x509 -days 3650 -key ca.key -out ca.cert
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NY
```

```
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XYZ
Organizational Unit Name (eg, section) []:TECH
Common Name (e.g. server FQDN or YOUR name) []:TEST-CA
Email Address []:
```

Generating Device Key and Certificate

1. Generate RSA key for device with length of 4096 bits.

```
C:\Temp\pki>openssl genrsa -out id1.key 4096
Loading 'screen' into random state - done
Generating RSA private key, 4096 bit long modulus
..........................++
............++
unable to write 'random state'
e is 65537 (0x10001)
```

2. Generate device certificate signing request (csr)

NOTE: Press “return” key on fields that you want to leave blank (like Locality, Email Address, Challenge password, optional company name).

```
C:\Temp\pki>openssl req -new -key id1.key -out id1.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NY
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XYZ
Organizational Unit Name (eg, section) []:TECH
Common Name (e.g. server FQDN or YOUR name) []:ID1
Email Address []:

Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3. Generate device certificate (with validity of 1 year) by signing it with the root CA key.

```
C:\Temp\pki>openssl x509 -req -days 365 -in id1.csr -CA ca.cert -CAkey ca.key -s
et_serial 01 -out id1.cert
Loading 'screen' into random state - done
Signature ok
subject=/C=US/ST=NY/O=XYZ/OU=TECH/CN=ID1
Getting CA Private Key
unable to write 'random state'
```

4. The device certificate (id1.cert), device key (id1.key) and root CA certificate (ca.cert) can be used to configure various services on Orbit that use certificates for security (like IPSec VPN).

NOTE: Ensure unauthorized personnel do not have access to device and root CA keys.

End of application bulletin.