NAREGI-CA

Quick Startup Guide

October 13, 2006

National Institute of Informatics

CONTENTS

1. INTRODUCTION

This document explains the features and operating environment of the NAREGI-CA.

1.1. Features of NAREGI-CA

The NAREGI-CA is a certificate authority server command group that operates on UNIX. It is a package of various utility commands that generate keys, and issue, verify, and store certificates.

1.2. Procedure for Configuring Certificate Authority Using NAREGI-CA

This document explains the procedure for starting up a certificate authority by using the NAREGI-CA, giving an example. The certificate authority in the example can issue certificates for the grid middleware, GlobusToolkit. The certificates for Globus come in three types: user certificate, host certificate, and LDAP certificate. Taking security into consideration, a certificate authority (CA) and registration authority (RA) are configured on separate machines.

"CA" denotes a server that has a function to issue a certificate, and "RA" denotes a server that has license ID management and Web enroll functions.

"Certificate authority" means an entire system including "CA", "RA", and administrator.

The following shows the procedure for configuring a certificate authority in this document.

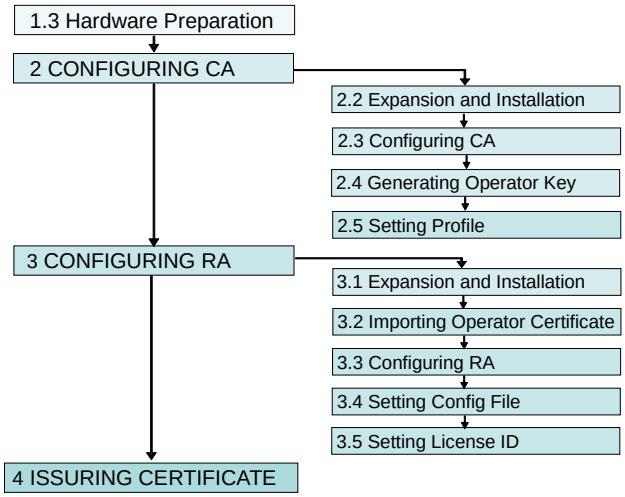

Figure 1. Procedure for Configuring a Certificate Authority

1.3. Hardware Preparation

The NAREGI CA operates in the following environment.

Supported machines	PC/AT-compatible machine (DOS/V) Sun Microsystems SPARC machine
CPU	Pentium III 500 MHz or more (recommended)
Supported OSs	Turbolinux Server 6.5 MIRACLE LINUX Standard Edition V2.1 Solaris 2.6, 2.8 Red Hat 7.3 or later
Memory	128 MB or more (recommended)
Hard disk capacity	10 MB as software installation area Depends on number of certificates issued (e.g., 10 MB for 1,000 certificates)
Display	800 × 600 dots or more, high color or more (recommended)

For the hardware, prepare one machine dedicated to the CA and one machine dedicated to the RA, which satisfy the above specifications. The network configuration is shown below.

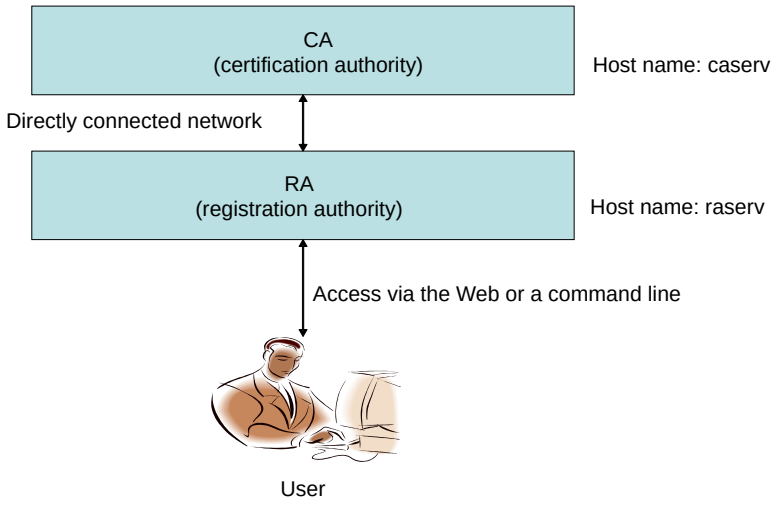

Figure 2. Network Configuration

2. CONFIGURING CA

This chapter explains how to configure the CA by using the NAREGI-CA. The CA can be easily configured by executing aisetup.sh and performing operations in accordance with the instructions displayed on the screen.

For expansion, installation, and configuring, use, for security, an account dedicated to operation, whenever possible, rather than the root account. It is assumed that all the following operations are performed by an “aica” user dedicated to the operations of the NAREGI-CA.

2.1. Creating a account for CA operation

At first, create a UNIX account, “aica”, for NAREGI-CA operation.

```
root# useradd aica
root# passwd aica
```

Make a directory for naregi-ca installation, and change directory owner.

```
root# mkdir /usr/local/naregi-ca
root# chown aica:aica /usr/local/naregi-ca
```

2.2. Expansion and Installation

Obtain a NAREGI-CA package from the following Web site.

http://www.naregi.org/download/index.html

The package is compressed. Extract it in the following procedure.

ex) File name in case of naregi-ca-2.2.tar.gz

```
bash$ gtar zxvf naregi-ca-2.2.tar.gz
```

After extracting, move to the naregi-ca directory, and compile and install the NAREGI-CA in the following procedure. In the following example, the NAREGI-CA package is installed under /user/local/naregi-ca.

(Create /usr/local/naregi-ca in advance with root privileges.)

```
bash$ cd naregi-ca
bash$ ./configure --prefix=/usr/local/naregi-ca --with-lang=jp
bash$ make
bash$ make install
```

2.3. Configuring CA

<1> To configure a new CA and register it to a CA server, use the “aisetup.sh” shell script. To create a new certificate and a private key, execute the following command. When the command is executed, “Step 1. Initialize CA Master Password” starts.

```
bash$ /usr/local/naregi-ca/bin/aisetup.sh -keysize 2048 -days 3650 testca
==========================================
   Registration of Certification Authority
==========================================
Step 1. initialize CA Master Password.
   * this password will be used for CA private key encryption or
   * HSM login password. Also, "CAOperator" private key in the
   * NAREGI CA certificate store will be encrypted with this password.

Input Master Passwd: (Input the password.)
Verify - Input Master Passwd: (Input the password.)
```

<2> When initialization of the CA master password has been completed, generation of the CA private key is automatically started. Wait until generation of the key is completed. A directory to which CA information is to be saved will be displayed, but, CA data is usually created in “NAREGI-CA-installation-directory/CA-name/”.

```
Step 2. create a new Certificate Authority
   * create a new Certificate Authority for the CA server.
   * CA information files are placed in:
   *     /usr/local/naregi-ca/testca

generate private key (size 2048 bit)
.....................................o
.............................o
```

<3> When the CA private key has been successfully generated, input a certificate subject.

input Distinguished Name (DN).
select directory tag (input number)
(1. C, 2. ST, 3. L, 4. O, 5. OU, 6. CN, 7. Email, 8. Quit) [1]: **1** ***←Specify a country name.***
Country [JP]: **JP** ***←Country name***
select directory tag (input number)
(1.C, 2.ST, 3.L, 4.O, 5.OU, 6.CN, 7.Email, 8.Quit) [4]: **4** ***←Specify an organization name.***
Organization [my organization]:**test university** ***←Organization name***
select directory tag (input number)
(1. C, 2. ST, 3. L, 4. O, 5. OU, 6. CN, 7. Email, 8. Quit) [5]: **5** ***←Specify an organizational unit name.***
Organization Unit [business unit]: **test unit** ***←Organizaitonal unit name***
select directory tag (input number)
(1. C, 2. ST, 3. L, 4. O, 5. OU, 6. CN, 7. Email, 8. Quit) [8]: **8** ***←End***

When the above data are input, the subject of CA has the following meaning.

/C=JP/O=test university/OU=test unit

Country name = JP

Organization name = test university

Organizational unit name = test unit

The outline of each tag field is as follows.

C	Name of a country. Be sure to input two 1-byte uppercase characters. E.g., “JP” for Japan.
ST	Name of a state. (Optional).
L	Name of location. (Optional).
O	Name of organization. Up to 64 1-byte characters can be input. Japanese characters can also be input.
OU	Name of organizational unit. Up to 64 1-byte characters can be input. Japanese characters can also be input.
CN	Common name. Up to 64 1-byte characters can be input. Japanese characters can also be input.
EMAIL	E-mail address. Up to 64 1-byte characters can be input.

<4> Next, the user will be only prompted to input “y” and CA will be configured almost automatically. The subject and validity period of the certificate will be checked and a CA certificate will be issued. The CA server setting file, aica.cnf, will also be updated.

```
Certificate DATA:
   serial number : 1
   issuer :
      C=JP, O=my organization, OU=business unit,
   subject:
      C=JP, O=my organization, OU=business unit,
   notBefore: Nov 28 16:00:04 2003
   notAfter : Nov 25 16:00:04 2013

do you sign here ? (y/n)[y]: y
now signing ..
.........oo
oo
Update CA information.

Step 3. CA Server registration
   * new Certificate Authority is created successfully.
   * now this CA will be registerd into the CA Server.
   * if you want to change default setting, you can do it
   * manually by editing aica.cnf file with text editor.
   * aica.cnf file is placed in :
   *      /usr/local/naregi-ca/lib/aica.cnf

import a file to the store successfully.
success to regist a CA : testca
success to regist a CRL Publihser : /usr/local/naregi-ca/testca
success to unregist RAd RegInfo : dummy
success to regist a RAd RegInfo: localhost:testca
------------------------------------------------------------------
CA server registration is finished successfully.

put "aicad" command to start the CA server. then, you can test
following "aica" command to check if server works correctly.

   * aica print -sv localhost:testca -ssl -clid CAOperator001
```

<5> If registration of CA to the CA server is correctly completed, configuring CA is completed. To check if the setting has been correctly made, start the CA server and execute a remote access. Display a profile and confirm that “SMIME user” profile information is displayed as shown below.

```
bash$ /usr/loca/naregi-ca/bin/aicad
## Boot the CA Server : input master password for each CA ##
read config file.
   …(Omitted)…

bash$ /usr/loca/naregi-ca/bin/aica print -sv localhost:testca -ssl -clid CAOperator001
tring to connect localhost(11411):testca (ssl)
Open Private Key: (Input the password.)
-----------------------------------
Certificate Profile : SMIME user
   certificate version    : 3
   current serial number: 1
   signature algorithm    : md5WithRSAEncryption
   …(Omitted)…
```

2.4. Generating Operator Key

<1> To configure a certificate authority with configuring CA and RA on separate machine, SSL client authentication is performed for communication between CA and RA. A CA operator certificate, a private key, and a CA certificate are therefore necessary for the RA server.
How to generate a CA operator certificate and a private key (PKCS#12 format) on the CA server is described below.

```
bash$ cd /usr/local/naregi-ca/testca
bash$ aica export -p 12 -sn 2
CA PKCS#12 file open
Input PKCS$12 Password: (Input the master password.)

get private key file from CA key store.
Input PASS Phrase:    (Input the master password.)

save PKCS#12 file. input new password.
Input Export Password : (Input the password.)
Verifying ? Input Export Password : (Input the password.)
```

File /usr/local/naregi-ca/testca/newcert.p12 will be generated.

<2> The file and CA certificate generated on the CA server must be transferred to the RA server.

Here is an example of the method for transferring. Any method may be used as long as newcert.p12 and ca.cer can be transferred to the RA server.

```
bash$ scp /usr/local/naregi-ca/testca/newcert.p12 raserv:/usr/local/naregi-ca

bash$ scp / usr/local/naregi-ca/serv-ssl/ca.cer raserv:/usr/local/naregi-ca
```

2.5. Setting Profile

A profile must be set so that three types of certificates for Globus can be issued. By default, only a certificate for “SMIME Client” can be issued.

Therefore, add two profiles. One for the client and the other for being shared by the host and LDAP.

To add profiles, use the aica command as follows.

```
bash$ aica prof –add
CA PKCS#12 file open
Input PKCS#12 Password : (Input the master password.)
-------
Add a certificate profile to this CA.

[1] Cross Cert Profile template
[2] Empty Profile template
[3] IPSEC Profile template
[4] Operator Profile template
[5] SMIME user Profile template
[6] SSL client Profile template
[7] SSL server Profile template
[8] Sub-CA Profile template
[0] Exit

Please select a templete number [0]: 6    ←Profile for user

   Selected profile templete is "SMIME user Profile template"
   Input Profile Name : Globus user    ←Profile name for user

do you continue this operation ? (y/n)[n]: y
Add a certificate profile to this CA.

[1] Cross Cert Profile template
[2] Empty Profile template
[3] IPSEC Profile template
[4] Operator Profile template
[5] SMIME user Profile template
[6] SSL client Profile template
[7] SSL server Profile template
[8] Sub-CA Profile template
[0] Exit

Please select a templete number [0]: 7    ←Profile for server

   Selected profile templete is "SMIME user Profile template"
   Input Profile Name : Globus host    ←Profile name for server

do you continue this operation ? (y/n)[n]: n
Update CA information.
```

3. CONFIGURING RA

This chapter explains how to configure the RA. The RA can be configured only by executing ainewra.sh and inputting an operator password.

3.1. Expansion and Installation

To configure the RA, the NAREGI-CA must be compiled and installed in the same manner as when CA is configured. See 2.1 for how to compile and install the NAREGI-CA.

3.2. Importing Operator Certificate

Before executing ainewra.sh, an operator certificate for CA operation and a CA certificate must be installed to the certificate store of NAREGI CA. This operation can be performed in the following procedure.

```
bash$ aistore –I newcert.p12
   Input PKCS#12 Password: → (Password set for export)
   Save Access Password: → (Input the password.)
   Verifying Save Access Password: → (Input the password for verification.)

bash$ aistore –i ca.cer
```

3.3. Configuring RA

Execute the following command to configure a new RA server.

```
bash$ ainewra.sh -op CAOperator001 -sv caserv:testca
-----------------------------------------
setup a Registration Authority (RA)
-----------------------------------------

>> copy RA template files to /usr/local/naregi-ca/testca_ra

>> update aica.cnf (configuration) file
success to regist a RAd RegInfo : caserv:testca

>> input CA Operator access password
   you need to set access password for CAOperator001 in the
   certificate store.
Input Operator Passwd : (Input the password.)
Verify - Input Operator Passwd : (Input the password for verification.)

RA initialization has been finished successfully.
```

If the name of the connection destination CA is “testca”, directory “testca_ra” is created under the local NAREGI CA installation directory where files necessary for Web enrolling and operation of the **airad** are configured.

Up to 64 RAs can be configured on one server.

3.4. Setting Config File

The config file is aica.cnf. It is located as follows if RA is configured in the procedure described in this document.

/usr/local/naregi-ca/lib/aica.cnf

In this example, the config file is modified to issue certificates for three types for Globus. First, modify the RAd Reginfo 0 section as follows for the user certificate.

```
[RAd RegInfo 0]
raname   =testca_ra
rapath   =/usr/local/naregi-ca/testca_ra

ca_dir   =caserv:testca   ←CA server name:CA name
ca_port  =11411
ca_uid   =caadmin
ca_pwd   =

cl_id    =CAOperator001_00
cl_id_pwd          =$aicry${Rkom+NUqRTn19Kwm1oalzg==}

f_ssl_use          =true
f_ssl_novfycrl     =true

interval           =60
post_mode          =false

authmode           =2   ←License ID mode
wwwpwd             =/usr/local/naregi-ca/globususer/en.passwd
wwwlicense         =/usr/local/naregi-ca/ globususer/en.license
wwwsessions        =/usr/local/naregi-ca/ globususer/sessions.0

#ldap_host         =
ldap_port          =389
ldap_base          =
ldap_user_attr     =cn

smtp_host          =
smtp_port          =25
admin_email        =
web_address        =http://localhost/aienroll

#gridmap           =/usr/local/naregi-ca/testca_ra/grid/grid-mapfile
#gridcertpath      =/usr/local/naregi-ca/testca_ra/grid/certs

groupname.0        =Globus user
groupprof.0        = Globus user   ←Profile name for user
 [RAd RegInfo 0 end]
```

Next, create RAd RegInfo 1 section.

The RAd Reginfo 1 section makes the setting that is shared by the host certificate and LDAP certificate.

```
[RAd RegInfo 1]
raname   =testca_ra
rapath   =/usr/local/naregi-ca/testca_ra

ca_dir   =caserv:testca
ca_port  =11411
ca_uid   =caadmin
ca_pwd   =

cl_id    =CAOperator001_00
cl_id_pwd        =$aicry${Rkom+NUqRTn19Kwm1oalzg==}

f_ssl_use        =true
f_ssl_novfycrl   =true

interval         =60
post_mode        =false

authmode         =2
wwwpwd           =/usr/local/naregi-ca/globushost/en.passwd
wwwlicense       =/usr/local/naregi-ca/ globushost/en.license
wwwsessions      =/usr/local/naregi-ca/ globushost/sessions.0

#ldap_host       =
ldap_port        =389
ldap_base        =
ldap_user_attr   =cn

smtp_host        =
smtp_port        =25
admin_email      =
web_address      =http://localhost/aienroll

#gridmap         =/usr/local/naregi-ca/testca_ra/grid/grid-mapfile
#gridcertpath    =/usr/local/naregi-ca/testca_ra/grid/certs

groupname.0      =Globus host
groupprof.0      = Globus host   ←Profile name for user
[RAd RegInfo 1 end]
```

3.5. Setting License ID

A license ID is a ticket, so to speak, for the user to receive a certificate. The administrator of the certificate authority is presumed to generate a bundle of tickets in advance and give one ticket to each user.

This section describes how to generate a list of license IDs.

<1> Creating directories for each certificate

Prepare a directory for issuing user certificates for Globus and a directory for issuing the host and LADP certificates, so that license IDs for the user and host can be separately managed.

```
bash$ cp –R /usr/local/naregi-ca/ratemplate /usr/local/naregi-ca/globususer
bash$ cp –R /usr/local/naregi-ca/ratemplate /usr/local/naregi-ca/globushost
```

<2> Setting license ID

Generate a license ID. A license ID is described in the en.license file as a character string.

/usr/local/naregi-ca/globususer/en.license

/usr/local/naregi-ca/globushost/en.license

```
#
# ** enroll user registration file (One time LicenseID) **
#
# This file will be used by airad and aienroll.cgi.
# These programs can select License ID authentication
# mode, and its mode needs the local "en.license" file.
#
# license ID format is *-*-* type.
# ex.
#     TEST-0000-0001
#     NAREGI-5QEZZG-IABO55
#
# To generate unique license ID, please use "aienrtool"
# command with input header and initialized vector
# information.
#
# ex.
# bash$ aienrtool -lic -hd NAREGI -iv 1234 >> en.license
#
# This example will generate following line in this file.
# NAREGI-O5T49V-CDX8K3
#raname =testca_ra
hoge-hoge-hoge-num1
hoge-hoge-hoge-num2
```

3.6. Starting RA Server

Configuring the RA is completed when the config file has been set. Start the RA server and execute remote access. Display a profile and confirm that “SMIME user” profile information is displayed as shown below.

```
bash$ airad
## Boot the CA Server : input master password for each CA ##
read config file.
   …(Omitted)…

bash$ aica print -sv caserv:testca -ssl -clid CAOperator001
tring to connect localhost(11411):testca (ssl)
Open Private Key: (Input the password.)
-----------------------------------
Certificate Profile : SMIME user
   certificate version    : 3
   current serial number: 1
   signature algorithm    : md5WithRSAEncryption
   …(Omitted)…
```

4. ISSURING CERTIFICATE

This chapter explains the procedure in which the user and host administrator requests issuance of a certificate.

4.1. Expanding and Installing NAREGI-CA-Client

To obtain a certificate from the user environment (UNIX), the NAREGI-CA must also be expanded and installed in the user environment. A NAREGI-CA-Client package that extracts only the client functions of the NAREGI-CA is also available.

To configure the NAREGI-CA-Client, the NAREGI-CA must be compiled and installed in the same manner as when CA is configured.

See 2.2 for how to compile and install the NAREGI-CA.

4.2. Importing RA Certificate

Before obtaining a certificate, the RA certificate on RA must be imported. By importing the RA certificate, reliable relation is created between the RA and client.

Copy the RA certificate as follows.

```
bash$ scp raserv:/usr/local/naregi-ca/serv-ssl/ca.cer /usr/local/naregi-ca/ra.cer
```

Next, import the RA certificate as follows.

```
bash$ aistore –i ra.cer
```

4.3. Obtaining Certificate from Command Line (User Certificate)

<1> To obtain a user certificate, apply for an electronic certificate by using the **grid-certreq** command. The license ID created in 3.5 is necessary for applying for a certificate.
Execute the command as follows, and generate a key pair, and input a group name, a name, and an E-mail address. Specify “Globus user” as the group name.

```
bash$ /usr/local/naregi-ca/bin/grid-certreq –sv raserv:globususer –new hoge-hoge-hoge-num1
----------------------------------------
  creating a certificate signing request
----------------------------------------
generate private key (size 1024 bit)
.....................oo
.........................oo

*** input user subject information ***
input group : Globus user ←Profile name for user (Certificate cannot be issued if this is incorrect.)
input user name : Naregi Taro
input user email : taro@grid.nii.ac.jp
```

<2> Check the input character strings. Check if the group name, user name, and E-mail address are correct, and then input **y**, **n**, or **r** (continue, cancel, or retry). To proceed, press the return key without inputting anything.

```
*** please confirm your inputs ***
GROUP     : Globus user
SUBJECT : CN=Naregi Taro, Email=taro@grid.nii.ac.jp

do you continue operation? (yes/no/retry)[y]: (Input return.)
```

<3> Connect to the certificate application server and apply for a certificate. If the license ID is correct and if there is no problem in the subject information of the certificate, the certificate is issued. Inputting a pass phrase to the certificate is prompted. Input an appropriate phrase.

```
trying to connect RA server : 172.168.3.2 (11412) ... ok.
request for issuing a new certificate ... ok.
save a CA certificate file : /home/myname/.globus/cacert.pem
save a certificate file : /home/myname/.globus/usercert.pem
save a private key file : /home/myname/.globus/userkey.pem
Input PASS Phrase: (Input a pass phrase.)
Verifying - Input PASS Phrase: (Input a pass phrase.)
```

A CA certificate, a user certificate, and a private key for the user will be created under .globus of the home directory (the location of creation can be checked in the above message).

The CA certificate file (cacert.pem) may be deleted.

Carefully save the certificate (ussercert.pem) and private key and, if necessary, move them to another machine in accordance with the grid computer environment.

4.4. Obtaining Certificate from Command Line (Host Certificate)

<1> To obtain a host certificate, apply for an electronic certificate by using the **certreq** command. The license ID created in 3.5 is necessary for applying for the certificate.

Execute the command as follows, and generate a key pair, and input a group name and a host name. Specify “Globus server” as the group name.

```
bash$ /usr/local/naregi-ca/bin/certreq –s –size 1024 –noenc –cer hostcert.pem –key hostkey.pem –cacer naregica.cer –sv raserv:globushost –new hoge-hoge-hoge-num1
----------------------------------------
  creating a certificate signing request
----------------------------------------
generate private key (size 1024 bit)
.....oo
.....oo

      *** input user subject information ***
input group : Globus server ←Profile name for server (Certificate cannot be issued if this is incorrect.)
input user name : host/hostname ←Specification of Globus is host/host name.
input user email : .   ←Email is not included in Subject if dot (.) is input.
```

<2> Check the input character strings. Check if the group name and host name are correct, and then input **y**, **n**, or **r** (continue, cancel, or retry). To proceed, press the return key without inputting anything.

```
*** please confirm your inputs ***
GROUP     : Globus server
SUBJECT : CN=host/hostname, Email=.

do you continue operation? (yes/no/retry)[y]: (Input return.)
```

<3> Connect to the certificate application server and apply for a certificate. If the license ID is correct and if there is no problem in the subject information of the certificate, the certificate is issued.

```
trying to connect RA server : 172.168.3.2 (11412) ... ok.
request for issuing a new certificate ... ok.
save a CA certificate file : naregica.cer
save a certificate file : hostcert.pem
save a private key file : hostkey.pem
```

4.5. Obtaining Certificate from Command Line (LDAP Certificate)

<1> To obtain an LDAP certificate, apply for an electronic certificate by using the **certreq** command. The license ID created in 3.5 is necessary for applying for the certificate.

Execute the command as follows, and generate a key pair, and input a group name and a host name. Specify “Globus server” as the group name.

```
bash$ /usr/local/naregi-ca/bin/certreq –s –size 1024 –noenc –cer ldapcert.pem –key ldapkey.pem –cacer naregica.cer –sv raserv:globushost –new hoge-hoge-hoge-num2
-----------------------------------------
 creating a certificate signing request
-----------------------------------------
generate private key (size 1024 bit)
.....oo
.....oo

      *** input user subject information ***
input group : Globus server ←Profile name for server (Certificate cannot be issued if this is incorrect.)
input user name : ldap/hostname ←Specification of Globus is ldap/host name.
input user email : .   ←Email is not included in Subject if dot (.) is input.
```

<2> Check the input character strings. Check if the group name and host name are correct, and input **y**, **n**, or **r** (continue, cancel, or retry). To proceed, press the return key without inputting anything.

```
*** please confirm your inputs ***
GROUP     : Globus server
SUBJECT : CN=ldap/hostname, Email=.

do you continue operation? (yes/no/retry)[y]: (Input return.)
```

<3> Connect to the certificate application server and apply for the certificate. If the license ID is correct and if there is no problem in the subject information of the certificate, the certificate is issued.

```
trying to connect RA server : 172.168.3.2 (11412) ... ok.
request for issuing a new certificate ... ok.
save a CA certificate file : naregica.cer
save a certificate file : ldapcert.pem
save a private key file : ldapkey.pem
```

4.6. Location of Host and LDAP Certificates

After obtaining the host certificate and LDAP certificate, locate them so that they can be used with Globus. The location is as follows.

```
/etc/grid-security
                    +-hostcert.pem
                    |
                    +-hostkey.pem
                    |
                    +-ldap -|
                    |       +-ldapcert.pem
                    |       |
                    |       +-ldapkey.pem
                    |
                    +- globus-user-ssl.conf-->TRUSTED_CA/globus-user-ssl.conf.xxxx
                    |
                    +- globus-host-ssl.conf-->TRUSTED_CA/globus-host-ssl.conf.xxxx
                    |
                    +- grid-security.conf-->TRUSTED_CA/grid-security.conf.xxxx
                    |
                    +- certificates+
                                   |
                                   +-xxxx.0
                                   |
                                   +-xxxx.signing_policy
                                   |
                                   +-TRUSTED_CA/globus-user-ssl.conf.xxxx
                                   |
                                   +-TRUSTED_CA/globus-host-ssl.conf.xxxx
                                   |
                                   +-TRUSTED_CA/grid-security-ssl.conf.xxxx
```

Caution:

- All the owners of the host certificate must be the root user.
- Change the permission so that only the root user can read /etc/grid-security/hostkey.pem and /etc/grid-security/ldap/ldapkey.pem.

After locating the certificate, a reliable CA certificate must be registered.

According to the specification of Globus, the name of the CA certificate must be “hush value.0” (dot zero).

```
bash$ openssl x509 –in ca.cer –hash    ←Displays hush value of CA certificate.
eg12xz7hfr
bash$ cp –p ca.cer /etc/grid-security/certificates/eg12xz7hfr.0
```

A new policy file must also be created.

file-name:**/etc/grid-security/certificates/*hush-value*.signing_policy**

```
access_id_CA        X509          '/C=JP/O=test university/OU=test unit'
pos_rights          globus        CA:sign
cond_subjects       globus        '"/C=JP/O=test university/OU=test unit/*"'
```

Copy each config file as follows.

```
bash$ cd /etc/grid-security
bash$ cp –p globus-user-ssl.conf certificates/globus-user-ssl.conf.eg12xz7hfr
bash$ cp –p globus-host-ssl.conf certificates/globus-user-ssl.conf.eg12xz7hfr
bash$ cp –p grid-security-ssl.conf certificates/grid-security-ssl.conf.eg12xz7hfr

bash$ rm globus-user-ssl.conf
bash$ ln –s certificates/globus-user-ssl.conf.eg12xz7hfr globus-user-ssl.conf
bash$ rm globus-host-ssl.conf
bash$ ln –s certificates/globus-host-ssl.conf.eg12xz7hfr globus-host-ssl.conf
bash$ rm grid-security-ssl.conf
bash$ ln –s certificates/grid-security-ssl.conf.eg12xz7hfr grid-security-ssl.conf
```

This completes use of the Globus certificate using the NAREGI-CA.