How to Request Host Certificate

호스트 인증서 신청 방법

2007.10.01
2017.05.25(Update)

KISTI Grid Certificate Authority

- Home
- CA Certificates
- Documents
  - CP/CPS
  - Minimum CA Requirement
- Request Certificates
- Issued Certificates
- Contact Information
- Related Sites
- KISTI CA(old site)

Introduction

Welcome to KISTI Grid Certificate Authrity web site.

KISTI Grid Certificate Authority is operated by the Grid Technology Research Team of KISTI (Korea Institute of Science and Technology Information).

The authority satisfies requirements from APGrid PMA.

Certificate issues by the KISTI Grid CA are compatible with the Globus Toolkit middleware.

The public key cryptography is the basis of grid security architecture.

Certificate Authority(CA) is a mandatory componant of public key infrastructure(PKI).

Please read "Overview of the Grid Security Infrastructure" from Globus site.

Best viewed with Firefox browser.
Copyright 2006 Korea Institute of Science and Technology Information

인터넷

Fill out the subscription form.

2. Interview with a RA with the application form. (RA contact information)
   Provide the following information when interview with a RA:

   o the application form
   o proof of identity (work ID card, passport, national ID card, etc.)

3. Keep the PIN number of the application form securely.
   The RA should fill the PIN number field in the form.
   Fax the form to the number specified in the form.

4. Please send an notification e-mail to ca@gridcenter.or.kr after sending a FAX.

5. KISTI Grid CA staff will respond immediately when we receive your request form.

6. KISTI Grid CA will send an Web Access Client Certificate(WACC) to your e-mail, if everything is okay.
   Install this certificate in your web browser to access to the on-line certificate request service web site.
   Your PIN number is the password for your WACC.
   Follow this insturction to install the web access certificate(WACC) in your browser.

Step 2. Request a Grid Certificate from KISTI GRID CA

- If you are applying for a **user certificate**,

   Click **User Certificate Request**

- If you are applying for a **host/service certificate**,

   Click **Host/Service Certificate Request**

KISTI Grid Certificate Authority

- Home
- CA Certificates
- Documents
  - CP/CPS
  - Minimum CA Requirement
- Request Certificates
- Issued Certificates
- Contact Information
- Related Sites
- KISTI CA(old site)

Instruction for requesting an Host or Service Certificate

By requesting a certificate, you indicate that you accept the Certificate Policy and Certificate Practice Statement and that you agree to the Subscriber Obligation specified in the document.

Step 1. Enroll KISTI CA

Before requesting user certificate from KISTI GRID CA, you are required to enroll KISTI GRID CA.
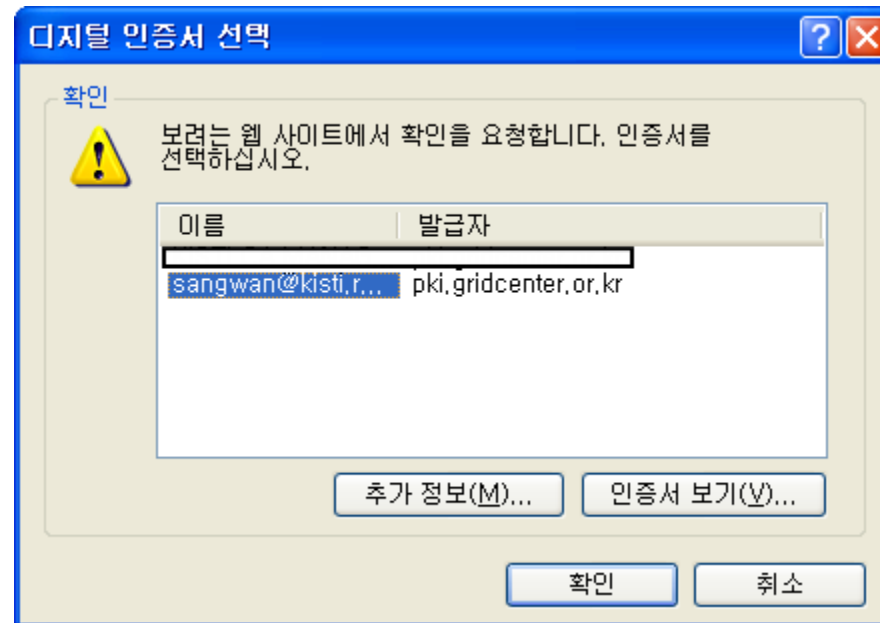
Step 2. On-line Certificate Request

Click here to request service or host certificate in the Online Request Service.
If you don't have a WACC in your browser, the access to the web page is not permitted.

Best viewed with Firefox browser.
Copyright 2006 Korea Institute of Science and Technology Information

완료   🌐 인터넷

Connect to "Online Request Service" using your WACC certificate.

KISTI Grid Certificate Authority

- Home

- Request Certificate
- My CSR List

- KISTI CA Home

Request Host Certificate

Step 1. Generate a CSR for your host.

Step 2. Upload the CSR using the following form.

Country:	KR
Organization:	KISTI
▇▇▇▇▇▇▇▇▇▇	
Organization:	[dropdown ▾]
Host FQDN:	[ ] (max. 30 characters) e.g) hostname.example.co.kr
CSR:	Copy and paste your CSR block below: [textarea]

Select Your Organization and input the FQDN of the host for which you want to get a certificate.

This CSR input textarea.

Upload CSR

How to generate CSR with **OpenSSL**

Using RSA 2048-bit and
do not encrypt the key using DES.

```
openssl req ₩
 -new -sha256 -newkey rsa:2048 -nodes ₩
 -keyout hostkey.pem ₩
 -out hostcert_request.pem ₩
 -subj "/C=KR/O=KISTI/O=ORGANIZATION/CN=host₩/grid.example.com"
```

This is common for every certificate issued by KISTI CA

Replace this your own organization and hostname.

If you use globus software, for host certificate 'host/' is prefied in the CN.

If successful, the hostkey.pem and hostcert_request.pem files are generated.

EX) a user in KISTI request a host certificate with the name 'test.kisti.re.kr'

Run like this,

```
openssl req ₩
  -new -sha256 -newkey rsa:2048 -nodes ₩
  -keyout hostkey.pem ₩
  -out hostcert_request.pem ₩
  -subj "/C=KR/O=KISTI/O=KISTI/CN=host₩/test.kisti.re.kr"
```

Check the generated CSR.

```
openssl req -in hostcert_request.pem -text -noout
```

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=KR, O=KISTI, O=KISTI, CN=host/test.kisti.re.kr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ce:e1:6a:bf:1e:28:1a:00:ee:8e:55:5f:37:5f:
                    c0:98:37:c8:63:85:1a:ce:b6:52:88:41:3c:bf:eb:
                    8c:fb:0b:31:7a:ec:e4:e6:fd:57:5c:5c:04:bb:74:
                    03:cd:2b:c5:25:4b:b6:b2:21:d3:3c:c6:ee:db:14:
                    d3:0f:ba:74:5d:ea:e0:d6:3a:a4:fa:c8:79:5b:59:
                    ea:e2:32:a3:fe:79:37:3e:9b:9f:55:ec:4e:c0:32:
                    98:f0:1b:aa:01:2c:42:b7:43:70:e7:3f:6b:f0:b5:
                    b3:38:b8:37:16:6a:a9:32:e8:21:10:67:29:d5:f7:
                    d7:1f:9f:96:26:61:6f:eb:21:6b:32:1e:9b:13:80:
                    37:14:ce:97:74:e6:98:2d:2c:0c:e0:d1:e2:be:37:
                    90:67:28:f5:79:2a:b6:05:3b:7c:11:ee:5b:be:ec:
                    be:15:d7:5f:83:e5:12:d7:d5:01:e0:08:a8:ac:1c:
                    a0:fc:c9:95:4b:b3:f7:c0:6e:1d:a9:5f:04:9b:8e:
                    34:4d:b1:31:cb:ce:50:0d:3e:1a:40:fa:f7:34:de:
                    11:9b:ad:d3:e5:26:b9:62:13:34:3d:98:d7:90:17:
                    42:9b:ba:97:aa:11:be:15:78:e8:2e:5f:50:55:7c:
                    4d:3c:20:cf:c5:ad:ef:96:0b:fe:c0:90:a5:6b:90:
                    f6:0f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
        a1:a6:d0:21:b7:f3:8c:72:e6:3d:cb:c6:b8:77:56:bf:74:ed:
        61:68:d2:28:8c:e5:01:46:e1:7e:be:d7:1d:1b:8a:6a:85:0f:
```

Check the subject of the CSR

Check the RSA key size.

If the CSR have no problem,
You can input the CSR text block in the previous step.

Copy the content of the hostcert_request.pem file.

```
K0840P2:igtf-policy-installation-bundle-1.83 sahn$ more hostcert_request.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICkjCCAXoCAQAwTTELMAkGA1UEBhMCS1IxDjAMBgNVBAoTBUtJU1RJMQ4wDAYD
VQQKEwVLSVNUSTEeMBwGA1UEAxMVaG9zdC90ZXN0Lmtpc3RpLnJlLmtyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzuFqvx4oGgDujlVfN1/AmDfIY4Ua
zrZSiEE8v+uM+wsxeuzk5v1XXFwEu3QDzSvFJUu2siHTPMbu2xTTD7p0Xerg1jqk
+sh5W1nq4jKj/nk3PpufVexOwDKY8BuqASxCt0Nw5z9r8LWzOLg3FmqpMughEGcp
1ffXH5+WJmFv6yFrMh6bE4A3FM6XdOaYLSwM4NHivjeQZyj1eSq2BTt8Ee5bvuy+
Fddfg+US19UB4AiorByg/MmVS7P3wG4dqV8Em440TbExy85QDT4aQPr3NN4Rm63T
5Sa5YhM0PZjXkBdCm7qXqhG+FXjoLl9QVXxNPCDPxa3vlgv+wJCla5D2DwIDAQAB
oAAwDQYJKoZIhvcNAQELBQADggEBAKGm0CG384xy5j3Lxrh3Vr907WFo0iiM5QFG
4X6+1x0bimqFD5TuOEtKhhDUn9f+8mhGj53FhBpAPIQtHgbdvUkktzji+56Hjf4Q
B62dtW1X6vlsILDrB6MHuDpsiaksCXRcHP+9u1e6F1WgQKHT+/7oK21yd3Rc+lVW
Ox5N65pchBNtFqmNhFem2rB9Qm11+z/4HP7bnM7GWF8tvLd8dQpdTPKNuU3hMOQC
PUsEaJWUEqIMBnHpsv6Hln3SMFNsznHroqrEfGygTGhectBgRupPGOWMUcJzm+ss
YNC9L19CakFj0U5eya8v8giq21+M0N8cNxExtOsmSSQgwCOvtxI=
-----END CERTIFICATE REQUEST-----
K0840P2:igtf-policy-installation-bundle-1.83 sahn$
```

KISTI Grid Certificate Authority

- Home

- Request Certificate
- My CSR List

- KISTI CA Home

Your CSR has been requestd to KISTI CA.

KISTI CA will review your CSR, before issuing your certificate.

Your CSR is sent to your email **sangwan@kisti.re.kr**.

After KISTI CA issue your certificate, a notification e-mail will be sent to you.

CSR information has been stored and the page show
that an email message has been sent.

KISTI Grid Certificate Authority

KISTI Grid Certificate Authority

- Home
- Request Certificate
- My CSR List
- KISTI CA Home

My Certificate Signing Request List

ID	Type	Form Information	Date	Status	View
1	user	O=KISTI CN=80864141 Sangwan Kim	2007-07-21 15:44:39	issued	[show] / [hide]
14	host	O=KISTI CN=test.kisti.re.kr	2007-10-02 11:25:03	upload	[show] / [hide]

Request CSR information is shown in the left size menu
' My CSR List'

KISTI Grid Certificate Authority

After finishing CSR upload process,
for notification, please send an email to <u>kisti-grid-ca@kisti.re.kr</u>
containing the following message.

To KISTI CA manager,

I have uploaded my host certificate request,

please sign the CSR.

FROM: <u>Your Name</u>