

How to Request User Certificate

사용자 인증서 신청 방법

KISTI Certification Authority

- Home
- CA Certificates
- Documents
 - CP/CPS
 - Minimum CA Requirement
- Request Certificates
- Issued Certificates (v3.0)
- Issued Certificates (obsolete)
- Contact Information
- Related Sites

Introduction

Welcome to KISTI Certification Authority web site.

KISTI Certification 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.

Certification Authority(CA) is a mandatory component of public key infrastructure(PKI).

Please read ["Overview of the Grid Security Infrastructure"](#) from Globus site.

Global Science experimental Data hub Center
National Institute of Supercomputing and Networking
Korea Institute of Science and Technology Information
245 Daehak-ro, Yuseong-gu 3414 Daejeon, Republic of Korea



4. Please send an notification e-mail to kisti-grid-ca@kisti.re.kr after sending a FAX.
5. KISTI CA staff will respond immediately when we receive your request form.
6. KISTI 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.
Read the following insturction to install the web access certificate(WACC) in your browser.

[How to Install Web Access Client Certificate in the Browser](#)

Step 2. Request a Grid Certificate from KISTI CA

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

Click [User Certificate Request](#)

 [How to Request User Certificate \(Korean\)](#)

 [How to Request User Certificate \(English\)](#)

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

Click [Host/Service Certificate Request](#)

 [How to Request Host Certificate \(Korean\)](#)

 [How to Request Host Certificate \(English\)](#)

Global Science experimental Data hub Center
National Institute of Supercomputing and Networking
Korea Institute of Science and Technology Information
245 Daehak-ro, Yuseong-gu 3414 Daejeon, Republic of Korea



KISTI Certification Authority

- Home
- CA Certificates
- Documents
 - CP/CPS
 - Minimum CA Requirement
- Request Certificates
- Issued Certificates (v3.0)
- Issued Certificates (obsolete)
- Contact Information
- Related Sites

Instruction for requesting an User 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 (Secion 1.3.3) specified in the document.

Step 1. Enroll KISTI CA

Before requesting user certificate from KISTI CA, you are required to enroll KISTI CA.

Step 2. On-line Certificate Request

[Click here to request user 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.

* NOW This function **SUPPORT ALL KIND OF BROWSERS** such as *Google Chrome, Edge, FireFox and Safari, etc. IE(Internet Explorer) mode of Edge no longer necessary.*

** **[DO NOT FORGET!]** After uploading your CSR, you can **download PIN-protected ZIP file** of your private key file (file name is like "#csrid_privateKey.zip") from the result page.

*** The ZIP file contains sensitive information and is encrypted for security. You'll find the **PIN number in the email** "[KISTI CA] User registration completed".

You can UNZIP the private key zip file using the command below:

```
# unzip -P PIN_NUMBER /path/to/csrid_privateKey.zip
```

It is crucial to back up your privatekey.pem file in a secure location. If you want to protect it with a password, use the following command:

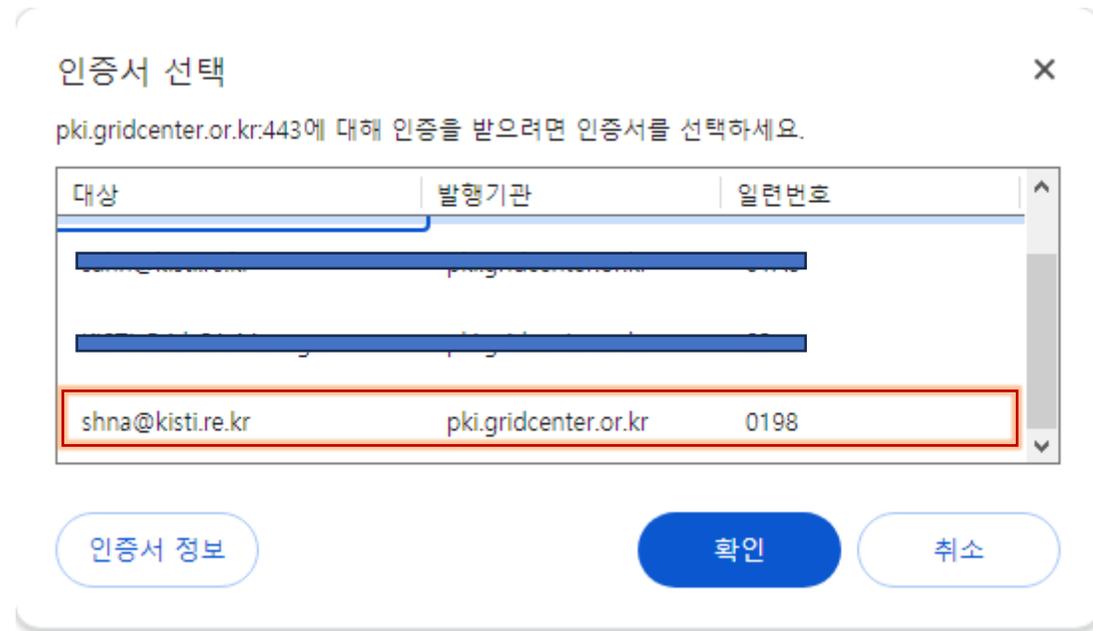
```
# openssl rsa -aes256 -in your_private_key.pem -out your_private_key_with_password.pem
```

(For maximum security, we strongly recommend using a passphrase of at least 12 characters.)

Please read these instructions carefully before proceeding.

Step 3. Download and Import Certificate

Once your certificate is issued, we'll publish it on the [Issued Certificates](#) and send out a confirmation to inform your certificate is ready. You can simply download your certificate via the link provided in the e-mail and import it into your browser.



- Select your WACC (Web Access Control Certificate) issued when you register.
- 사용자 등록 시 발급받은 WACC를 선택하세요

KISTI Certification Authority

- Home

- Request Certificate (v3.0)

- My CSR List (v3.0)

- My CERT List (v3.0)

- KISTI CA Home

Request Certificate

KISTI CA (v3.0)

- If you are applying for a **user certificate**, [User Certificate Request](#)

* NOW This function SUPPORT ALL KIND OF BROWSERS such as *Google Chrome, Edge, FireFox and Safari, etc.*
IE(Internet Explorer) mode of Edge no longer necessary.

** [DO NOT FORGET!] After uploading your CSR, you can download your private key file (csrid_privateKey.pem) from the result page.

- If you are applying for a **host/service certificate**, [Host Certificate Request](#)

KISTI Certification Authority

- Home
- Request Certificate (v3.0)
- My CSR List (v3.0)
- My CERT List (v3.0)
- KISTI CA Home

Request User Certificate

User Certificate Information:

* You don't have any valid user certificate. You can proceed Step 1 and 2.

Step 1. Check the following form, and click the 'Generate CSR' button.
KISTI CA server will create a CSR, which will be shown in the CSR text area of the step 2.

* NOW This function SUPPORT ALL KIND OF BROWSERS such as *Google Chrome, Edge, FireFox and Safari, etc.*
** IE(Internet Explorer) mode of Edge no longer necessary.

Country: KR
Organization: KISTI
Organization: KISTI
Common Name: 60115390 causer GSDC

Generate CSR

Step 2. Upload CSR

[Important] You can download private key(pem) from the CSR upload result page.

KISTI Certification Authority

- Home
- Request Certificate (v3.0)
- My CSR List (v3.0)
- My CERT List (v3.0)
- KISTI CA Home

Request User Certificate

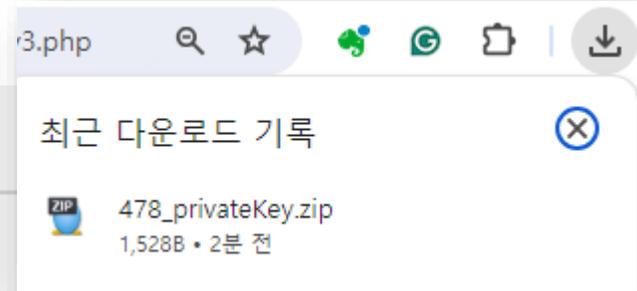
Your CSR has been requestd to KISTI CA.

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

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

!Important! You can not back to this page. Please DO NOT MISS to download your private key zip file!
!Important! The ZIP file contains sensitive information and is encrypted for security. You'll find the PIN number in the email "[KISTI CA] User registration completed".

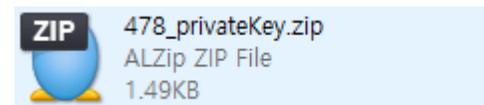
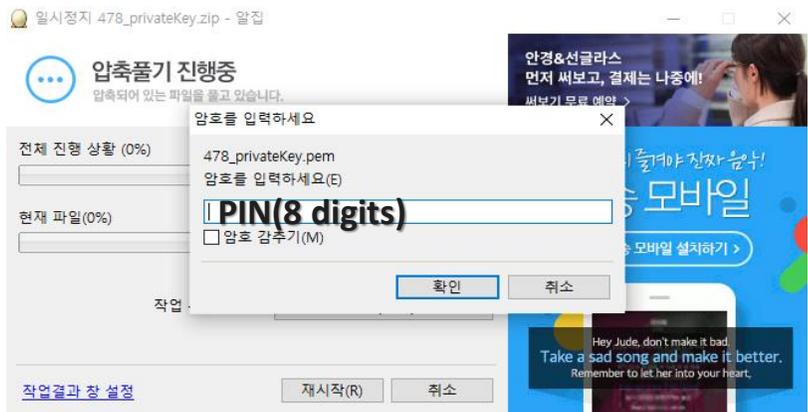
Private Key



PIN-protected zip file of your private key.

개인키 압축 풀기 Extract Private Key

Window



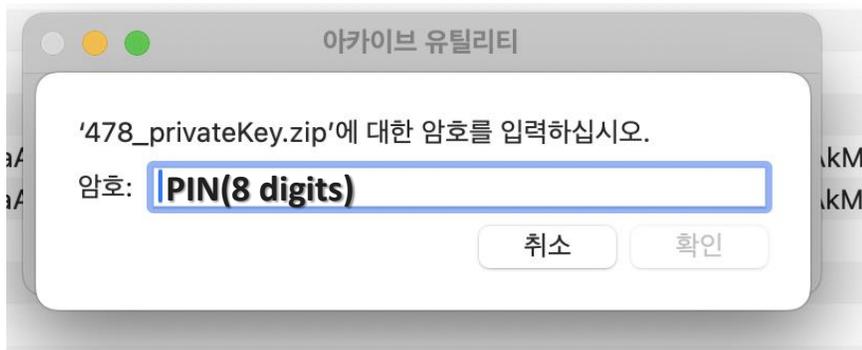
PIN(8 digits) ↓



Linux

```
# unzip -P PIN_NUMBER /path/to/csrid_privateKey.zip
```

MAC



Set password for private key

개인키 비밀번호 설정

```
# openssl rsa -aes256 -in your_private_key.pem -out your_private_key_with_password.pem
```

Convert format of certificate between der and pem

der - pem 간 인증서 포맷 변환하기

```
# openssl x509 -inform der -in your_certificate.der -out your_certificate.pem
```

```
# openssl x509 -outform der -in your_certificate.pem -out your_certificate.der
```

Combine your private key (privateKey.pem) and certificate (cert.pem) into a PKCS#12 (PFX) file.

개인키(privateKey.pem)와 인증서(cert.pem)를 pfx 포맷으로 합치기

```
# openssl pkcs12 -export -out output.pfx -inkey privatekey.pem -in your_certificate.pem
```

For Globus Toolkit,

you can copy `your_certificate.pem` and `your_private_key.pem` in `~/ .globus` directory.