

Certificates FAQ

FAQ about certificates in general

Q: What are certificates?

IT4Innovations employs X.509 certificates for secure communication (e. g. credentials exchange) and for grid services related to PRACE, as they present a single method of authentication for all PRACE services, where only one password is required.

There are different kinds of certificates, each with a different scope of use. We mention here:

- User (Private) certificates
- Certificate Authority (CA) certificates
- Host certificates
- Service certificates

However, users need only manage User and CA certificates. Note that your user certificate is protected by an associated private key, and this private key must never be disclosed.

Q: Which X.509 certificates are recognised by IT4Innovations?

Any certificate that has been issued by a Certification Authority (CA) from a member of the IGTF (<http://www.igtf.net>) is recognised by IT4Innovations: European certificates are issued by members of the EUGridPMA (<https://www.eugridmpa.org>), which is part of the IGTF and coordinates the trust fabric for e-Science Grid authentication within Europe. Further the Czech “*Qualified certificate*” (*Kvalifikovaný certifikát*) (provided by <http://www.postsignum.cz/> or <http://www.ica.cz/Kvalifikovany-certifikat.aspx>), that is used in electronic contact with Czech public authorities is accepted.

Q: How do I get a User Certificate that can be used with IT4Innovations?

To get a certificate, you must make a request to your local, IGTF approved, Certificate Authority (CA). Usually you then must visit, in person, your nearest Registration Authority (RA) to verify your affiliation and identity (photo identification is required). Usually, you will then be emailed details on how

to retrieve your certificate, although procedures can vary between CAs. If you are in Europe, you can locate your trusted CA via <http://www.eugridpma.org/members/worldmap>.

In some countries certificates can also be retrieved using the TERENA Certificate Service, see the FAQ below for the link.

Q: Does IT4Innovations support short lived certificates (SLCS)?

Yes, provided that the CA which provides this service is also a member of IGTF.

Q: Does IT4Innovations support the TERENA certificate service?

Yes, ITInnovations supports TERENA eScience personal certificates. For more information, please visit <https://tcs-escience-portal.terena.org>, where you also can find if your organisation/country can use this service

Q: What format should my certificate take?

User Certificates come in many formats, the three most common being the 'PKCS12', 'PEM' and the JKS formats.

The PKCS12 (often abbreviated to 'p12') format stores your user certificate, along with your associated private key, in a single file. This form of your certificate is typically employed by web browsers, mail clients, and grid services like UNICORE, DART, gsissh-term and Globus toolkit (GSI-SSH, GridFTP and GRAM5).

The PEM format (*.pem) stores your user certificate and your associated private key in two separate files. This form of your certificate can be used by PRACE's gsissh-term and with the grid related services like Globus toolkit (GSI-SSH, GridFTP and GRAM5).

To convert your Certificate from PEM to p12 formats, and *vice versa*, IT4Innovations recommends using the openssl tool (see separate FAQ entry).

JKS is the Java KeyStore and may contain both your personal certificate with your private key and a list of your trusted CA certificates. This form of your certificate can be used by grid services like DART and UNICORE6.

To convert your Certificate from p12 to JKS, IT4Innovations recommends using the keytool utility (see separate FAQ entry).

Q: What are CA certificates?

Certification Authority (CA) certificates are used to verify the link between your user certificate and the authority which issued it. They are also used to verify the link between the host certificate of a IT4Innovations server and the CA which issued that certificate. In essence they establish a chain of trust between you and the target server. Thus, for some grid services, users must have a copy of all the CA certificates.

To assist users, SURFsara (a member of PRACE) provides a complete and up-to-date bundle of all the CA certificates that any PRACE user (or IT4Innovations grid services user) will require. Bundle of certificates, in either p12, PEM or JKS formats, are available from <http://winnetou.sara.nl/prace/certs/>.

It is worth noting that gsissh-term and DART automatically updates their CA certificates from this SURFsara website. In other cases, if you receive a warning that a server's certificate can not be validated (not trusted), then please update your CA certificates via the SURFsara website. If this fails, then please contact the IT4Innovations helpdesk.

Lastly, if you need the CA certificates for a personal Globus 5 installation, then you can install the CA certificates from a MyProxy server with the following command.

```
myproxy-get-trustroots -s myproxy-prace.lrz.de
```

If you run this command as 'root', then it will install the certificates into /etc/grid-security/certificates. If you run this not as 'root', then the certificates will be installed into \$HOME/.globus/certificates. For Globus, you can download the globuscerts.tar.gz packet from <http://winnetou.sara.nl/prace/certs/>.

Q: What is a DN and how do I find mine?

DN stands for Distinguished Name and is part of your user certificate. IT4Innovations needs to know your DN to enable your account to use the grid services. You may use openssl (see below) to determine your DN or, if your browser contains your user certificate, you can extract your DN from your browser.

For Internet Explorer users, the DN is referred to as the "subject" of your certificate. Tools->Internet Options->Content->Certificates->View->Details->Subject.

For users running Firefox under Windows, the DN is referred to as the "subject" of your certificate. Tools->Options->Advanced->Encryption->View Certificates. Highlight your name and then Click View->Details->Subject.

Q: How do I use the openssl tool?

The following examples are for Unix/Linux operating systems only.

To convert from PEM to p12, enter the following command:

```
openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out
username.p12
```

To convert from p12 to PEM, type the following *four* commands:

```
openssl pkcs12 -in username.p12 -out usercert.pem -clcerts -nokeys
openssl pkcs12 -in username.p12 -out userkey.pem -nocerts
chmod 444 usercert.pem
chmod 400 userkey.pem
```

To check your Distinguished Name (DN), enter the following command:

```
openssl x509 -in usercert.pem -noout -subject -nameopt
RFC2253
```

To check your certificate (e.g., DN, validity, issuer, public key algorithm, etc.), enter the following command:

```
openssl x509 -in usercert.pem -text -noout
```

To download openssl for both Linux and Windows, please visit <http://www.openssl.org/related/binaries.html>. On Macintosh Mac OS X computers openssl is already pre-installed and can be used immediately.

Q: How do I create and then manage a keystore?

IT4innovations recommends the java based keytool utility to create and manage keystores, which themselves are stores of keys and certificates. For example if you want to convert your pkcs12 formatted key pair into a java keystore you can use the following command.

```
keytool -importkeystore -srckeystore $my_p12_cert -destkeystore
$my_keystore -srcstoretype pkcs12 -deststoretype jks -alias
$my_nickname -destalias $my_nickname
```

where \$my_p12_cert is the name of your p12 (pkcs12) certificate, \$my_keystore is the name that you give to your new java keystore and \$my_nickname is the alias name that the p12 certificate was given and is used also for the new keystore.

You also can import CA certificates into your java keystore with the tool, e.g.:

```
keytool -import -trustcacerts -alias $mydomain -file $mydomain.crt -keystore $my_keystore
```

where \$mydomain.crt is the certificate of a trusted signing authority (CA) and \$mydomain is the alias name that you give to the entry.

More information on the tool can be found at:<http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html>

Q: How do I use my certificate to access the different grid Services?

Most grid services require the use of your certificate; however, the format of your certificate depends on the grid Service you wish to employ.

If employing the PRACE version of GSISSH-term (also a Java Web Start Application), you may use either the PEM or p12 formats. Note that this service automatically installs up-to-date PRACE CA certificates.

If the grid service is UNICORE, then you bind your certificate, in either the p12 format or JKS, to UNICORE during the installation of the client on your local machine. For more information, please visit UNICORE6 in PRACE

If the grid service is part of Globus, such as GSI-SSH, GriFTP or GRAM5, then the certificates can be in either p12 or PEM format and must reside in the “\$HOME/.globus” directory for Linux and Mac users or %HOMEPATH%.globus for Windows users. (Windows users will have to use the DOS command ‘cmd’ to create a directory which starts with a ‘.’). Further, user certificates should be named either “usercred.p12” or “usercert.pem” and “userkey.pem”, and the CA certificates must be kept in a pre-specified directory as follows. For Linux and Mac users, this directory is either \$HOME/.globus/certificates or /etc/grid-security/certificates. For Windows users, this directory is %HOMEPATH%.globuscertificates. (If you are using GSISSH-Term from prace-ri.eu then you do not have to create the .globus directory nor install CA certificates to use this tool alone).

Q: How do I manually import my certificate into my browser?

If you employ the Firefox browser, then you can import your certificate by first choosing the “Preferences” window. For Windows, this is Tools->Options. For Linux, this is Edit->Preferences. For Mac, this is Firefox->Preferences. Then, choose the “Advanced” button; followed by the “Encryption” tab. Then, choose the “Certificates” panel; select the option “Select one automatically” if you have only one certificate, or “Ask me every time” if you have more than one. Then click on the “View Certificates” button to open the “Certificate Manager” window. You can then select the “Your Certificates” tab and click on button “Import”. Then locate the PKCS12 (.p12) certificate you wish to import, and employ its associated password.

If you are a Safari user, then simply open the “Keychain Access” application and follow “File->Import items”.

If you are an Internet Explorer user, click Start->Settings->Control Panel and then double-click on Internet. On the Content tab, click Personal, and then click Import. In the Password box, type your password. NB you may be prompted multiple times for your password. In the “Certificate File To Import” box, type the filename of the certificate you wish to import, and then click OK. Click Close, and then click OK.

Q: What is a proxy certificate?

A proxy certificate is a short-lived certificate which may be employed by UNICORE and the Globus services. The proxy certificate consists of a new user certificate and a newly generated proxy private key. This proxy typically has a rather short lifetime (normally 12 hours) and often only allows a limited delegation of rights. Its default location, for Unix/Linux, is /tmp/x509_undefined but can be set via the \$X509_USER_PROXY environment variable.

Q: What is the MyProxy service?

The MyProxy Service, can be employed by gsissh-term and Globus tools, and is an online repository that allows users to store long lived proxy certificates remotely, which can then be retrieved for use at a later date. Each proxy is protected by a password provided by the user at the time of storage. This is beneficial to Globus users as they do not have to carry their private keys and certificates when travelling; nor do users have to install private keys and certificates on possibly insecure computers.

Q: Someone may have copied or had access to the private key of my certificate either in a separate file or in the browser. What should I do?

Please ask the CA that issued your certificate to revoke this certificate and to supply you with a new one. In addition, please report this to IT4Innovations by contacting the support team.