



FAQ

G. Pringle, D. Girou (ed.), J. Wolfrat (ed.), H. Heller (ed.)

(c) 2004 - 2010 DEISA



DEISA is funded by the European Commission in FP7 under grant agreement RI-222919

Table of contents

1 Introduction.....	1
2 General DEISA FAQ	3
3 Certificates and their usage within DEISA FAQ.....	7

1 Introduction

This document is the DEISA Frequently Asked Questions (FAQ) document and is divided into two sections. The first section contains the FAQ regarding X.509 certificates and their use within DEISA. The second section contains more general DEISA FAQs.

This FAQ is kept up-to-date and readers are encouraged to submit new FAQ questions or other improvements.

2 General DEISA FAQ

Q: How do I access my Execution Site using the DEISA network or my personal laptop?

The answer may be found at the following link: <http://www.deisa.eu/usersupport/user-documentation/interactive-access>. Alternatively, you may ask your Home Site for assistance.

Q: How can I determine the status of each component of the DEISA infrastructure?

You can view the status of each component of the DEISA infrastructure via the INCA monitoring service at <http://inca.deisa.eu>[1].

Q: I have connection problems (ssh-keys, machine not available, maintenance problems, etc.)

You can have a look at the INCA tool (<http://inca.deisa.eu>[2]) to see if the site is in maintenance or has problems with the service you are trying to use. Additionally the website of your Execution Site may have further information. If INCA does not provide an answer, please submit a query to the DEISA Trouble Ticket System (DTTS), at <http://tts.deisa.eu/UserSupport>[3]. For more information on the DTTS, please visit <http://www.deisa.eu/usersupport/primer/access-to-the-user-support>[4].

Q: How do I submit a query for support?

Rather than submitting queries to an individual DEISA site, we strongly recommend using the DEISA Trouble Ticket System. For more details, please visit <http://www.deisa.eu/usersupport/primer/access-to-the-user-support>[5].

Q: May I contact my Execution Site directly?

Please do not contact your Execution Site directly. Instead, please communicate via the DEISA Trouble Ticket System (DTTS). For more details, please visit <http://www.deisa.eu/usersupport/primer/access-to-the-user-support>[6].

Q: Why do I get “command not found” errors for almost every command?

The most probable reason is that you don't have the DEISA Common Production Environment (DCPE) loaded. In order to load the DCPE, type:

```
module load deisa
```

-
1. <http://inca.deisa.eu/>
 2. <http://inca.deisa.eu/>
 3. <http://tts.deisa.eu/UserSupport>
 4. <http://www.deisa.eu/usersupport/primer/access-to-the-user-support>
 5. <http://www.deisa.eu/usersupport/primer/access-to-the-user-support>
 6. <http://www.deisa.eu/usersupport/primer/access-to-the-user-support>

General DEISA FAQ

Indeed, every new shell must start with this command, i.e. it must be the first executable line in any batch script and the first command typed when you first log in.

Q: How can I check how many hours I have consumed?

You can check how many hours you have consumed using the DEISA Accounting Reporting Tool (DART).

For more information and for the DART FAQ, please visit <http://www.deisa.eu/usersupport/user-documentation/deisa-accounting-report-tool>[7]

To launch the tool directly, please click here: <http://www.deisa.eu/usersupport/user-documentation/deisa-accounting-report-tool/dart.jnlp>[8]

NB Some DEISA sites do report usage figures using their own tools elsewhere; however, the only official source of DEISA accounting data is given by the DART.

Q: I have platform-specific questions and problems: where can I find local documentation?

There is a link to each sites' local User Documentation via DEISA's Interactive Access User Document at <http://www.deisa.eu/usersupport/user-documentation/interactive-access/list-of-deisa-platforms-and-user-guides>[9].

Q: How do I submit a job?

This is described in DEISA's Batch System User Document, which is available via <http://www.deisa.eu/usersupport/user-documentation/deisa-batch-systems>.

Q: What is the `deisa_service` script?

Users do not need to know a particular address and/or port number when using a Globus command directly on the command-line of a DEISA machine, as DEISA has provided the `deisa_service` script. To access the `deisa_service` script, you must first load both the `deisa` and `globus` modules. The `deisa_service` script provides abbreviations for the user to employ, which encode addresses and port numbers. These abbreviations make Globus commands shorter, easier to read/write, and more robust as changes to any particular Globus address or port details need not be known by the user. For example, the command

```
gsissh `deisa_service -e -s lrz`
```

provides a shorthand for the full command of

```
gsissh -p 2222 a01.hlr2.lrz-muenchen.de
```

Note, too, that users can specify if they wish to employ the DEISA network (`-i` for internal) or the public Internet (`-e` for external). The `-s` flag informs the `deisa_service` that `gsissh` is being employed. If you call `deisa_service` without any parameters, you will get a help screen explaining all possibilities and listing example calls for `deisa_service` with frequently used Globus commands. NB to employ the `deisa_service`, users must first run the following command.

-
7. <http://www.deisa.eu/usersupport/user-documentation/deisa-accounting-report-tool>
 8. <http://www.deisa.eu/usersupport/user-documentation/deisa-accounting-report-tool/dart.jnlp>
 9. <http://www.deisa.eu/usersupport/user-documentation/interactive-access/list-of-deisa-platforms-and-user-guides>

General DEISA FAQ

```
module load deisa
```

Q: How do I increase my file space or the limit on the total number of files?

Please contact your Home Site who will then investigate the possibility of increasing your disc allocation at your Execution Site(s).

Q: Which non-DEISA tools are available on my Execution Site?

There is a link to each sites' local User Documentation via DEISA's Interactive Access User Document at <http://www.deisa.eu/usersupport/user-documentation/interactive-access/list-of-deisa-platforms-and-user-guides>^[10], where such tools will be described.

Q: How to convert binary files from little endian to big endian and visa-versa on an IBM BlueGene platform?

You can use the environment variable XLFRTEOPTS; however this does not work with files generated via MPI-IO. If you want to read or write a file in LittleEndian on unit 12 of an IBM BlueGene:

```
BlueGene>mpixlf90_r -o little_endian little_endian.f90
BlueGene>bgrun -np 64 -mode VN -env "XLFRTEOPTS=ufmt_littleendian=12" -exe little_endian
```

Q: At the end of the project, how long do I have access to my data?

Typically, each project is given up to 3 months to remove their data from their Execution Site(s), however this should be confirmed with your Home Site.

Q: At the end of the project, how do I transfer my data to a remote computer?

If you have access to the \$DEISA_DATA common file-system at both your Home Site and Execution Site, you can transfer your files into that space and access it from your Home Site. NB \$DEISA_DATA is not backed up. If you have no access to \$DEISA_DATA at one of your sites, then you will have to use GridFTP or scp. We strongly recommend using GridFTP due to its much greater performance for larger file transfers. See <http://www.deisa.eu/usersupport/user-documentation/data-transfer-with-GridFTP>^[11] for details.

Q: My registration information has changed (this may be your name, address, affiliation, e-mail, telephone number, etc). Should I tell DEISA?

Please inform DEISA via <https://tts.deisa.eu/UserSupport/>

Q: How should I acknowledge DEISA?

If you publish results which are derived from work performed using DEISA resources, then please reference DEISA in the following manner: 'We thank the DEISA Consortium (www.deisa.eu), funded through the EU FP7 project RI-222919, for support within the DEISA Extreme Computing Initiative/DEISA Virtual Community Programme*'

-
10. <http://www.deisa.eu/usersupport/user-documentation/interactive-access/list-of-deisa-platforms-and-user-guides>
 11. <http://www.deisa.eu/usersupport/user-documentation/data-transfer-with-GridFTP>

General DEISA FAQ

(* delete as applicable). Finally, please inform DEISA so that we may include a reference to your publication in our website.

3 Certificates and their usage within DEISA FAQ

Q: What are certificates?

DEISA employs X.509 certificates for grid services, as they present a single method of authentication for all DEISA 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 DEISA?

Any certificate that has been issued by a Certification Authority (CA) from a member of the IGTF (<http://www.igtf.net>[1]) is recognised by DEISA: European certificates are issued by members of the EUGridPMA (<https://www.eugridpma.org>), which is part of the IGTF and coordinates the trust fabric for e-Science Grid authentication within Europe.

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

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 DEISA trusted CA via <http://www.eugridpma.org/members/worldmap>.

For more information, please see Section 2.4 of The Primer, which may be found at <http://www.deisa.eu/usersupport/primer/access-to-the-deisa-infrastructure>.

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

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

Q: Does DEISA support the TERENA certificate service?

Yes.

1. <http://www.igtf.net/>

Certificates and their usage within DEISA FAQ

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, UNICORE, DART, gsissh-term and Globus toolkit (GSI-SSH, GridFTP, RFT and WS-GRAM).

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 DEISA's gsissh-term and with the Globus toolkit (GSI-SSH, GridFTP, RFT, and WS-GRAM).

To convert your Certificate from PEM to p12 formats, and *visa versa*, DEISA 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 DART, the DESHL, and UNICORE6.

To convert your Certificate from p12 to JKS, DEISA 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 DEISA 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 DEISA services, users must have a copy of all the DEISA CA certificates.

To assist DEISA users, SARA provides a complete and up-to-date bundle of all the CA certificates that any DEISA user will require. Bundle of certificates, in either p12, PEM or JKS formats, are available from <http://winnetou.sara.nl/deisa/certs/>.

It is worth noting that gsissh-term and DART automatically updates their CA certificates from this SARA 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 SARA website. If this fails, then please contact the DEISA 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.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 4 you can download the globuscerts.tar.gz packet from <http://winnetou.sara.nl/deisa/certs/>.

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

DN stands for Distinguished Name and is part of your user certificate. DEISA needs to know your DN to create your DEISA account. 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.

Certificates and their usage within DEISA FAQ

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?

DEISA 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://download-llnw.oracle.com/javase/1.3/docs/tool-docs/win32/keytool.html>

Certificates and their usage within DEISA FAQ

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

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

If employing DEISA Trouble Ticket System (DTTS) or INCA (both Web Applications), then the certificate must be in the p12 format and must be manually loaded into your browser for each computer you intend to employ. (Some Certification Authorities deliver the certificate directly into your browser.)

If employing the DART (a Java Web Start Application), then you may use either the p12 format or JKS. For more information, please visit <http://www.deisa.eu/usersupport/user-documentation/deisa-accounting-report-tool>.

If employing the DEISA 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 DEISA CA certificates.

If the DEISA 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 <http://www.deisa.eu/usersupport/user-documentation/unicore>.

If the DEISA service is the DESHL then your personal certificate must be contained in a JKS (Java KeyStore), which also contains the DEISA CA certificates. An up-to-date DEISA JKS containing the necessary certificates can be downloaded from SARA, via <http://winnetou.sara.nl/deisa/certs>. You can add your personal certificate to this JKS using a keystore editor, such as Portecle, which may be downloaded from <http://portecle.sourceforge.net>. NB if you have already installed the UNICORE6 Rich Client, then the JKS created during installation can be used by DESHL without any further modification. For more information, please visit <http://www.deisa.eu/usersupport/user-documentation/deshl>.

If the DEISA service is part of Globus, such as GSI-SSH, GriFTP or WS-GRAM, 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%\globus\certificates. (If you are using GSISSH-Term from deisa.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.

Certificates and their usage within DEISA FAQ

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_u{uid}` but can be set via the `$X509_USER_PROXY` environment variable.

Q: What is the MyProxy service?

The MyProxy service, <http://www.deisa.eu/usersupport/user-documentation/deisa-myproxy-service>, can be employed by `gssh-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 DEISA via <https://tts.deisa.eu/UserSupport/>.