



# Interactive access to HPC resources

H. Heller, S.H. Leong, G. Pringle (eds.)

(c) 2004 - 2011 DEISA



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



# Table of contents

1 Interactive access .....	1
2 List of DEISA platforms and User Guides .....	3
2.1 BSC: IBM Power PC (MareNostrum) .....	3
2.2 CINECA: IBM Power6-575 (SP6) .....	3
2.3 CSC: Cray XT4/XT5 (Louhi) .....	3
2.4 CSCS: Cray XT5 (Rosa) .....	4
2.5 EPCC: Cray XE6 (HECToR) .....	4
2.6 FZJ: IBM BlueGene/P (JUGENE) .....	4
2.7 FZJ: Intel Xeon X5570 QC (JuRoPa) .....	4
2.8 HLRS: NEC SX-9 .....	5
2.9 HLRS: Intel Xeon X5560 (Laki) .....	5
2.10 IDRIS: IBM BlueGene/P (BABEL) .....	5
2.11 IDRIS: IBM Power6-575 (VARGAS) .....	6
2.12 KTH: Opteron Cluster 2354 (Ekman) .....	6
2.13 LRZ: SGI-Altix Itanium (HLRBII) .....	7
2.14 RZG: IBM BlueGene/P (Genius) .....	7
2.15 RZG: IBM Power6-575 (VIP) .....	7
2.16 SARA: IBM Power6-575 (Huygens) .....	8
3 Accessing your Execution Site .....	9
3.1 Accessing your Execution Site from a Door Node using gsissh .....	9
3.2 Accessing your Execution Site from your Home Site using gsissh .....	10
4 Accessing DEISA Door Nodes using gsissh .....	13
4.1 GSISSH-Term .....	13
4.2 Preparing for GSISSH-Term .....	13
4.3 GSISSH-Term as a Java webstart application .....	14
4.4 GSISSH-Term as a web browser applet .....	17
4.5 Using GSISSH-Term .....	18
4.6 Using GSISSH-Term in DEISA environment .....	22
4.7 Hints .....	23



# 1 Interactive access

At times, it is necessary for users to access their Execution platforms interactively, to permit installation of their codes, for instance.

Within DEISA, we recommend employing `gssish` for interactive access to your Execution Site. First, employ `gssish` on your local workstation to access a DEISA Door Node (currently either CINECA, LRZ, RZG or SARA). Then, if necessary, employ `gssish` to access your Execution Site.

NB if you access your Execution Site directly from your workstation, then you will employ the public Internet; however, if you employ `gssish` on a DEISA site to access your Execution Site, using its DEISA network address (given below), then you will employ DEISA's own private network.

This document first lists of each DEISA Platform, along with the preferred method of interactive access for both Execution and Home Site users, and a link to the platform's User Guide.

The remaining part of this document describes how to access your Execution Site from either a Door Node or from your Home Site and, finally, how to access a Door Node with `GSISsh-Term`.



## 2 List of DEISA platforms and User Guides

### 2.1 BSC: IBM Power PC (MareNostrum)

If MareNostrum is your **Execution Platform**, then you gain access via gsissh from another DEISA platform, where the address is **gridftp.deisa.bsc.es:2222**. Access via ssh is also available, with your ssh public key, using the address **mn1.bsc.es**.

If MareNostrum is your **Home Site**, then you gain access via ssh, with your ssh public key, using the address **mn1.bsc.es**.

Reference: MareNostrum User Guide[1]

### 2.2 CINECA: IBM Power6-575 (SP6)

This platform is a DEISA Door Node.

If the SP6 is your **Execution site**, then you gain access via gsissh. As this is a DEISA Door Node, you can access the SP6 directly from your workstation using the address **grid.sp6.cineca.it:2222**, or from another DEISA platform using the address **grid-deisa.sp6.cineca.it:2222**. Under special circumstances, ssh is also available. Your ssh public key is required, and the address is **sp.sp6.cineca.it**

If the SP6 is your **Home Site**, then the preferred method of interactive access is gsissh, as described above. Under special circumstances, ssh is also available. You will be issued a password and you will use the address **sp.sp6.cineca.it**.

Reference: SP6 User Guide[2]

### 2.3 CSC: Cray XT4/XT5 (Louhi)

If Louhi is your **Execution Site**, then the preferred method of interactive access is gsissh, but only from another DEISA platform; the address is **louhi-deisa.csc.fi:2222**. Access with ssh is also permitted, with your ssh public key, using the address **louhi.csc.fi**. In this case, you must to install your public keys yourself, via gsissh.

Reference: Louhi User Guide[3]

- 
1. <http://www.bsc.es/media/859.pdf>
  2. <http://hpc.cineca.it/content/ibm-sp6-user-guide>

## 2.4 CSCS: Cray XT5 (Rosa)

If Rosa is your **Execution Platform**, then interactive access is available via ssh only to **ela.cscs.ch**.

If CSCS is your **Home Site**, then you cannot access Rosa to access your Execution Platform. Please consult the entry of your Execution Platform within this section for information on interactive access.

Reference: Rosa User Guide[4]

## 2.5 EPCC: Cray XE6 (HECToR)

If HECToR SE6 (phase2b) is your **Execution Site**, then you may gain accessing using gsissh, where the address is **login11b.hector.ac.uk** from your workstation, or **login11b.hector.ac.uk:2222** from another DEISA platform. You may also use ssh with a password, where the address is **login11b.hector.ac.uk**; you may install your public ssh key yourself if you wish.

If HECToR is your **Home Site**, then the methods of access are the same as above.

Reference: HECToR User Guide[5]

## 2.6 FZJ: IBM BlueGene/P (JUGENE)

If JUGENE is either your **Execution Platform** or your **Home Site**, then you gain access via gsissh, but only from another DEISA platform. The address is **jugene5d.zam.kfa-juelich.de:2222**. Access via ssh is also available, with your ssh public key. If you login from another DEISA platform, then the address is **jugene5d.zam.kfa-juelich.de** otherwise the address is **jugenedeisa.fz-juelich.de**.

Reference: JUGENE User Guide[6]

## 2.7 FZJ: Intel Xeon X5570 QC (JuRoPa)

- 
3. [http://www.csc.fi/english/pages/louhi\\_guide](http://www.csc.fi/english/pages/louhi_guide)
  4. <http://www.cscs.ch/350.0.html>
  5. <http://www.hector.ac.uk/support/documentation/userguide>
  6. <http://www.fz-juelich.de/jsc/jugene/usage>

## List of DEISA platforms and User Guides

If JuRoPa is either your **Execution Platform** or your **Home Site**, then the preferred method of interactive access is ssh with your ssh public key. If you login from a DEISA platform, i.e. over the DEISA network, then the address is **juropagpfs01d.zam.kfa-juelich.de**. If you login from a non-DEISA platform, i.e. over the public Internet, then the address is **juropagpfs01.fz-juelich.de**.

Access via gsissh is also available, but only from other DEISA platforms. The address is **juropagpfs01d.zam.kfa-juelich.de:2222**.

Reference: JuRoPa User Guide[7]

### 2.8 HLRS: NEC SX-9

If the SX-9 is either your **Execution Platform** or your **Home Site**, then the only method of interactive access is ssh, using only your ssh public key. Further, you must also register your IP address. The address is either **ontake.hww.de** or, if that is unavailable, **yari.hww.de**.

Reference: SX-9 User Guide[8]

### 2.9 HLRS: Intel Xeon X5560 (Laki)

If Laki is either your **Execution Platform** or your **Home Site**, then the only method of interactive access is ssh, using only your ssh public key. Further, you must also register your IP address.

The address is **cl3fr1.hww.de** or, if that is unavailable, **cl3fr2.hww.de**.

Reference: Laki User Guide[9]

### 2.10 IDRIS: IBM BlueGene/P (BABEL)

If BABEL is your **Execution Platform**, then you gain access via gsissh, but only from other DEISA platforms. The address is **ulam-d.idris.fr:2222**. Once logged in, you then type 'rlogin babel-d.idris.fr' to access BABEL. Access via ssh is also available, using your ssh public key. You can employ either another DEISA platform, from where the address is then **babel-d.idris.fr**, or your own workstation, from where the address is **babel.idris.fr**.

---

7. <http://www.fz-juelich.de/jsc/juropa/usage>

8. <http://www.hlr.de/systems/platforms/nec-sx-9-12m192>

9. <http://www.hlr.de/systems/platforms/nec-nehalem-cluster>

## List of DEISA platforms and User Guides

If BABEL is your **Home Site**, then the preferred method of access is ssh with either a password or your ssh public key. The address is **babel.idris.fr**.

NB if employing your workstation to access BABEL directly, then you must first register its IP address with IDRIS.[10]

Reference: BABEL User Guide[11]

### 2.11 IDRIS: IBM Power6-575 (VARGAS)

If VARGAS is your **Execution Platform**, then you gain access via gsissh, but only from other DEISA platforms. The address is **ulam-d.idris.fr:2222**. Once logged in, you then type 'rlogin vargas-d.idris.fr' to access VARGAS. Access via ssh is also available, using your ssh public key. You can either login from another DEISA platform, where the address is then **vargas-d.idris.fr**, or login from your own workstation, from where the address is **vargas.idris.fr**.

If VARGAS is your **Home Site**, then the preferred method of access is ssh with either a password or your ssh public key. The address is **vargas.idris.fr**.

NB if employing your workstation to access VARGAS directly, then you must first register its IP address with IDRIS.[12]

Reference: VARGAS User Guide[13]

### 2.12 KTH: Opteron Cluster 2354 (Ekman)

If Ekman is your **Execution Platform**, then interactive access is available via ssh with Kerberos. You may access from your own workstation with a ticket by employing **kinit --forwardable yourusername@NADA.KTH.SE** (NB the capital letters are required) and then employ the address **ekman.pdc.kth.se**.

For an overview of login software with Kerberos, please visit this website[14], and for detailed information on access via ssh with Kerberos, please visit this website[15].

If KTH is your **Home Site**, then you cannot access Ekman to access your Execution Platform. Please consult the entry of your Execution Platform within this section for information on interactive access.

Reference: Ekman User Guide[16]

---

10. <http://www.idris.fr/eng/Forms/ftip-Eng.pdf>

11. [http://www.idris.fr/eng/User\\_Support/bg\\_support.html](http://www.idris.fr/eng/User_Support/bg_support.html)

12. <http://www.idris.fr/eng/Forms/ftip-Eng.pdf>

13. <http://www.idris.fr/su/Scalaire/vargas/>

14. <http://www.pdc.kth.se/resources/software/login-1>

15. <http://www.pdc.kth.se/resources/software/login-1/linux/ssh-with-kerberos-gssapi-on-ubuntu>

## 2.13 LRZ: SGI-Altix Itanium (HLRBII)

This platform is a DEISA Door Node.

If HLRBII is either your **Execution Site** or your **Home Site**, then the only method of interactive access is via gsissh. You may login using your workstation, where the address is **a01.hlrb2.lrz-muenchen.de**, or from another DEISA platform, where the address is then **a01-deisa.hlrb2.lrz-muenchen.de**. Please note that must register your IP address via LRZ.

Reference: HLRBII User Guide<sup>[17]</sup>

## 2.14 RZG: IBM BlueGene/P (Genius)

If Genius is your **Execution Platform**, then interactive access is available via gsissh only. You may log in directly from another DEISA platform, where the address is **genius1-fun.rzg.mpg.de:2223**, or you may log in using your workstation, where you must gsissh into a Door Node first. For instance, you can gsissh into RZG:VIP first, using the address **vip.rzg.mpg.de:2222**, and then gsissh from VIP into **genius.rzg.mpg.de**.

Reference: Genius User Guide<sup>[18]</sup>

## 2.15 RZG: IBM Power6-575 (VIP)

This platform is a DEISA Door Node.

If VIP is your **Execution Platform**, then access is via gsissh. You may login via your own workstation, as this is a DEISA Door Node, where the address is then **vip.rzg.mpd.de:2222**, or from another DEISA platform, where the address is then **vip001s.rzg.mpg.de:2223**.

If VIP is your **Home Site**, then you may employ either gsissh or ssh with a password. If you wish to employ gsissh, you may login via your own workstation, where the address is then **vip.rzg.mpd.de:2222**, or from another DEISA platform, where the address is then **vip001s.rzg.mpg.de:2223**. If you wish to employ ssh, then the address is **vip.rzg.mpg.de**.

Reference: VIP User Guide<sup>[19]</sup>

---

16. <http://www.pdc.kth.se/resources/computers/ekman/ekman-how-to/ekman-run>

17. <http://www.lrz-muenchen.de/services/compute/hlrb/>

18. <http://www.rzg.mpg.de/computing/hardware/BGP>

19. <http://www.rzg.mpg.de/computing/hardware/Power6/the-ibm-power6-system>

## 2.16 SARA: IBM Power6-575 (Huygens)

This platform is a DEISA Door Node

If Huygens is either your **Execution Site** or your **Home site**, then interactive access is via `gsissh`. You may log in from another DEISA platform, where the address is **p6012-deisa.huygens.sara.nl:2222**, or, as this is a DEISA Door Node, directly from your workstation using the address is then **p6012.huygens.sara.nl:2222**

Under special circumstances, `ssh` is also available using your `ssh` public key.

Reference: Huygens User Guide<sup>[20]</sup>

---

20. <https://subtrac.sara.nl/userdoc/wiki/huygens/usage>

## 3 Accessing your Execution Site

### 3.1 Accessing your Execution Site from a Door Node using gsissh

The fundamental steps are as follows:

#### 1) Users who have installed Globus or Cog-Kits

```
grid-proxy-init
```

Enter the passphrase that has been used when exporting the PKCS12-keystore.

Next, gsissh to one of the door nodes, e.g. SARA. The `-p` flag is optional, depending on your local configuration.

```
gsissh p6012.huygens.sara.nl -p 2222
```

SITE	Hostname	Port
CINECA	grid.sp6.cineca.it	2222
SARA	p6012.huygens.sara.nl	2222
LRZ (with firewall)	a01.hlr2.lrz-muenchen.de	2222
RZG	vip.rzg.mpg.de	2222

Table 1: *Door nodes in DEISA*

Now, you should be logged on to one of the door node sites. To log on to your execution site, e.g. LRZ

```
module load deisa globus
gsissh `deisa_service -i -s lrz`
```

The `-i` flag is network service flag to request for internal DEISA private network information. The `-s` flag is a service flag to request for gsissh service information. The final argument is the site/machine option. Available options are "lrz lrz-rvs sara rzg rzg-bg ecmwf idris csc fzj fzj-bg bsc hlrs epcc cineca-bcx cineca cea". For more information, please invoke command `deisa_service` on any of the deisa machines without options to get the help manual.

N.B. if you have multiple DEISA accounts, you can specify the specific account you would like to access with the `-l` option,

e.g. `gsissh `deisa_service -i -s sara` -l <deisa-username>`

#### 2) Users who are using GSISSH-Term

Please refer to the following page for more information.

### 3.2 Accessing your Execution Site from your Home Site using gsissh

Note, this process might involve placing your certificate's encrypted private key, as part of your keystore, on a networked system if you login to your Home Site using ssh. This is permitted by EUGridPMA but is currently not permitted by the Italian CA and by at least one German CA. If this process is not permitted by your CA, then your certificate may be revoked. We advise users to remove their personal certificates from the networked system once the proxy has been generated. Please note that you will have to upload your personal certificate to create new proxy certificate once the old one has expired (typically 12 hours). Alternatively, you can use DEISA's myProxy service to store and retrieve a copy of your proxy certificate (without having to transfer your private key to a networked system) or you can simply use gsissh, using e.g. GSISsh-Term, directly from your local workstation to avoid having to create proxy certificates on a networked system. GSISsh-Term will help you create the required proxy certificate and transfer it to the respective machines you gsissh to.

The fundamental steps are as follows.:

**1) If your Home Site is a DEISA door node, then follow the method listed above in section 3.1.**

**2) If your Home Site is not a DEISA door node and you are using ssh to login to your homesite.**

Login to your homesite. Create a directory `.globus` in your home directory (you only have to do this once).

```
mkdir $HOME/.globus
```

Export your certificate keystore, i.e. from your web browser on your local workstation, and copy it (e.g. scp) to your `$HOME/.globus` at your homesite. N.B. you have to name it as `usercred.p12`. Now, modify the access rights of your keystore for security.

```
chmod 600 $HOME/.globus/usercred.p12
```

Next, invoke the following commands to login to e.g. SARA.

```
module load deisa globus
grid-proxy-init
```

Enter the passphrase of your `usercred.p12` keystore.

```
gsissh `deisa_service -i -s sara`
```

The `-i` flag is network service flag to request for internal DEISA private network information. The `-s` flag is a service flag to request for `gsissh` service information. The final argument is the site/machine option. Available options are "`lrz lrz-rvs sara rzg rzg-bg ecmwf idris csc fzj fzj-bg bsc hlrs epcc cineca-bcx cineca cea`". For more information, please invoke command `deisa_service`

on any of the deisa machines without options to get the help manual.

e.g. `gsissh `deisa_service -i -s sara` -l <deisa-username>`

## Accessing your Execution Site

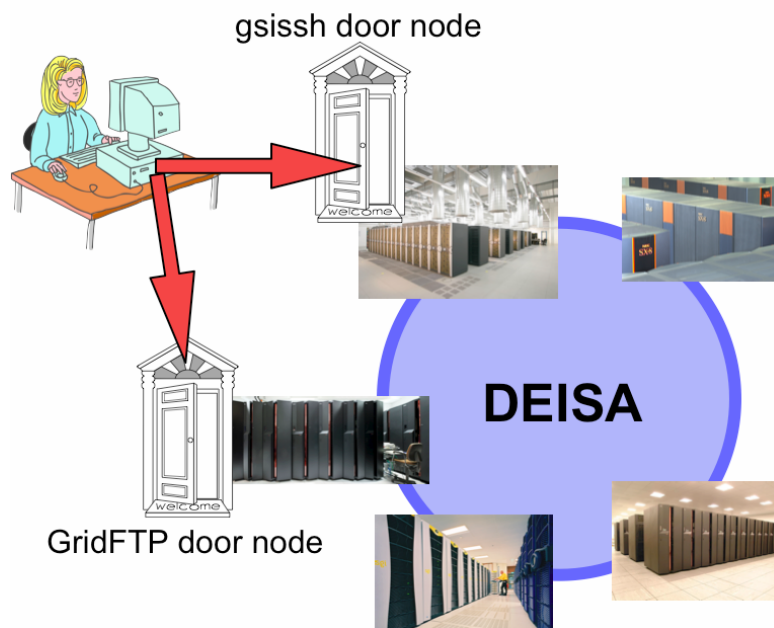
Finally, please remember to remove your *usercred.p12* if your CA does not permit you to store your certificate on a networked system.

```
rm $HOME/.globus/usercred.p12
```



## 4 Accessing DEISA Door Nodes using gsissh

For security and administrative reasons, not all DEISA sites are open worldwide for access via either gsissh or ssh. In most cases, gsissh (as well as gridFTP services) are only available on the private DEISA network. A few DEISA sites provide access to gsissh (and gridFTP) from the public Internet: we call them *Door Nodes*. Figure 1 shows that there can be different Door Nodes for different services. In this section, we explain how to use access a DEISA *Door Node* from your local workstation.



*Figure 1: DEISA door nodes for gsissh and gridFTP providing access from the public Internet.*

### 4.1 GSISSH-Term

GSISSH-Term is a Java based terminal client application for accessing the Grid created by the UK's NGS. It supports the use of grid certificates for authentication. Since this application is written in Java, it is supported on most platforms (e.g. Windows, MAC and Linux). DEISA provides a customised version of GSISSH-Term which includes DEISA users' customisations and additional bug fixes.

### 4.2 Preparing for GSISSH-Term

# Accessing DEISA Door Nodes using gsissh

## Setting up Grid Certificates

Users have to place the required grid certificates (CA certificates and personal certificates) appropriately on their machine before they can access DEISA's grid. Please follow the following steps:

- Ensure that your grid certificates (usercert.pem and userkey.pem) are in ".globus" folder in your home directory. For Linux/Unix user, the ".globus" folder should be in \$HOME. For Windows user (for more information, please refer to the section "*Hints*"), the ".globus" folder should be in following directory %HOMEPATH%.  
**Hint:** Please kindly ensure that your certificate and private key are named "usercert.pem" and "userkey.pem" respectively.
- DEISA customised version of GSISSH-Term that automatically retrieve from the server and update the required CA certificates into the appropriate local folders. As such, users do not have to be concerned with the set up of the CA certificates.

## Setting up Java

Since GSISSH-Term as a Java based application, you will need Java[1] Runtime Environment (JRE) 1.5 or higher installed. You should also install "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" which are not included in the default distribution of JRE due to import control restrictions. Please download the files from the following links:

- [Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0[2]] for JRE 1.5
- [Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6[3]] for JRE 1.6

Extract the two jar files, "*local\_policy.jar*" and "*US\_export\_policy.jar*", and copy them to

- {JRE\_HOME}/lib/security

Note that there are files with identical names but different content in the folder. This is because JRE supports by default up to 512 bit security. JCE provides additional support for 1024 bits.

## 4.3 GSISSH-Term as a Java webstart application

Before continuing, you should have set up your grid certificates and Java. If you have not done so, please refer to the previous section "Preparing for GSISSH-Term" before proceeding any further.

To install and start GSISSH-Term via Java Web Start, please click on this link[4] and open it with Java webstart (javaws).

- 
1. <http://java.sun.com>
  2. [https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS\\_Developer-Site/en\\_US/-/USD/ViewProductDetail-Start?ProductRef=jce\\_policy-1.5.0-oth-JPR@CDS-CDS\\_Developer](https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jce_policy-1.5.0-oth-JPR@CDS-CDS_Developer)
  3. [https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS\\_Developer-Site/en\\_US/-/USD/ViewProductDetail-Start?ProductRef=jce\\_policy-6-oth-JPR@CDS-CDS\\_Developer](https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jce_policy-6-oth-JPR@CDS-CDS_Developer)
  4. <http://www.grid.lrz-muenchen.de/res/globus/gsissh-term/applet/jws.jnlp>

## Accessing DEISA Door Nodes using gsissh

For your security, GSISsh-Term webstart application is signed with 2 certificates. A "Warning - Security" window, similar to the one here will be displayed.



Figure 2: GSISsh-Term digital signature security window

To verify that you are indeed using and downloading the version from DEISA (hosted at LRZ), please click on the "More Information ..." link. Depending on the version of Java you are using, the user interface may differ slightly. Another window will appear, please click on the "Certificate Details ..." link. Verify that the certificate information is as such:

```
Issuer: CN=DFN-Verein PCA Grid - G01, OU=DFN-PKI, O=DFN-Verein, C=DE
Subject: CN=Siew Hoon Leong, OU=Leibniz-Rechenzentrum, O=GridGermany, C=DE
```

The second certificate prompt will request for you to accept a certificate from "The Legion of the Bouncy Castle".



Figure 3: Bouncy Castle digital signature security window

To verify, make sure that the certificate information is as such:

```
Issuer: CN=JCE Code Signing CA, OU=Java Software Code Signing, O=Sun Microsystems Inc,
L=Palo Alto, ST=CA, C=US
Subject: CN=The Legion of the Bouncy Castle, OU=Java Software Code Signing, O=Sun
Microsystems Inc
```

You should see the following window when GSISsh-Term is initiated successfully.

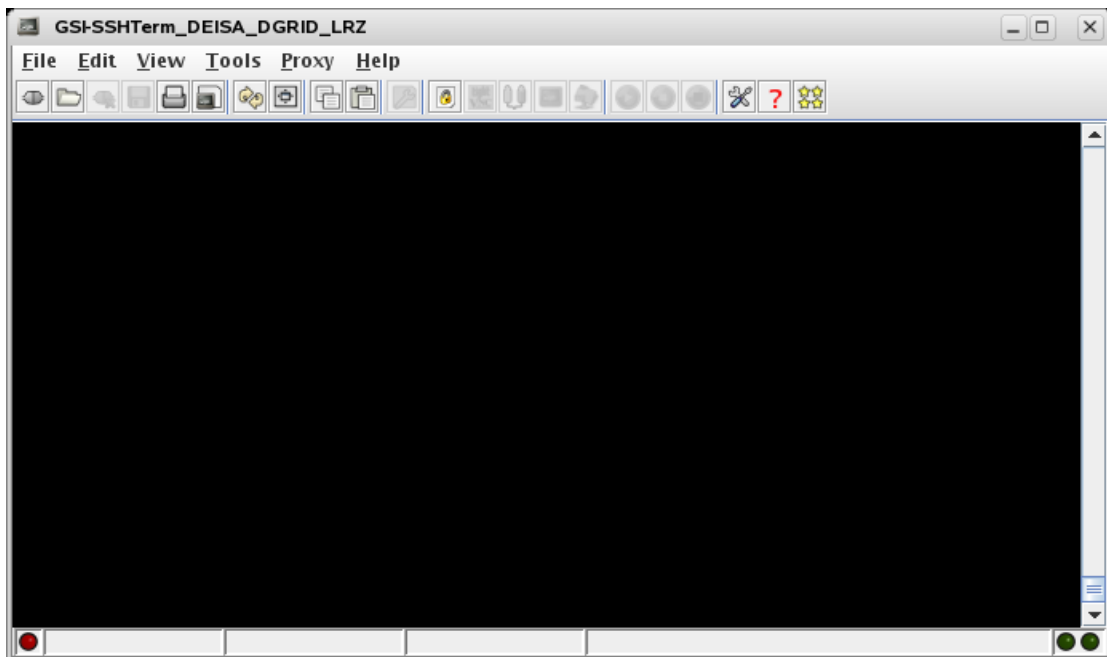


Figure 4: GSISsh-Term main window

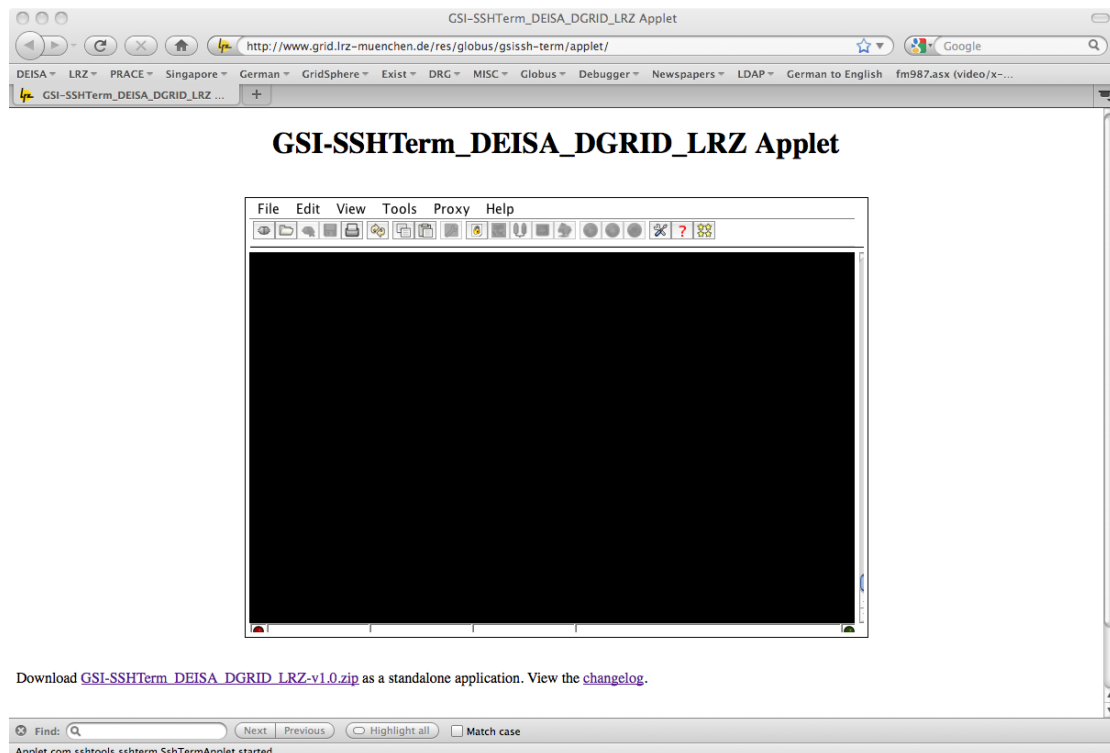
## Accessing DEISA Door Nodes using gsissh

For instructions on how to use GSISsh-Term, proceed to the section "Using GSISsh-Term" below.

### 4.4 GSISsh-Term as a web browser applet

Before continuing, you should have set up your grid certificates and Java. If you have not done so, please refer to the previous section "Preparing for GSISsh-Term" before proceeding any further.

For new users who would simply like to try GSISsh-Term and have an idea how it looks like and how it works, you can start GSISsh-Term as a browser applet.[5]All you need to do is to open this link in your web browser[6]. You should see the following window when GSISsh-Term is initiated successfully.



Download [GSI-SSHTerm\\_DEISA\\_DGRID\\_LRZ-v1.0.zip](#) as a standalone application. View the [changelog](#).

Figure 5: GSISsh-Term as a web browser applet

For instructions on how to use GSISsh-Term, proceed to the section "Using GSISsh-Term" below.

5. <http://www.grid.lrz-muenchen.de/res/globus/gsissh-term/applet/>
6. <http://www.grid.lrz-muenchen.de/res/globus/gsissh-term/applet/>

## 4.5 Using GSISsh-Term

To create a new connection, select "File → New Connection" or the shortcut icon "Create a New Connection" (first icon from the left). The following window will be displayed:

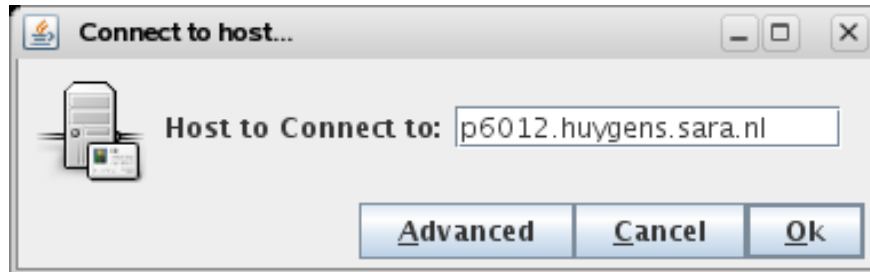


Figure 6: Connect to host dialog

Now, you can simply enter the host name of one of the DEISA Gsissh Door nodes in the textbox "Host to Connect to:" and click on the "Ok" button. The following table shows the door nodes in DEISA which offer access from public Internet. For direct access to LRZ, the IP number of the external PC must first be registered (please submit a request to the DEISA Helpdesk service<sup>[7]</sup>).

SITE	Hostname	Port
CINECA	grid.sp6.cineca.it	2222
SARA	p6012.huygens.sara.nl	2222
LRZ (with firewall)	a01.hrb2.lrz-muenchen.de	2222
RZG	vip.rzg.mpg.de	2222

Table 2: Door nodes in DEISA

**Note:** If your Home site or Execution sites are not offering public gsissh access, you can access the required site from one of the door node sites via gsissh hops. A description on how to do that is available in the next section "Using GSISsh-Term in DEISA environment".

For users who are accessing multiple DEISA accounts via a single user certificate, you can configure which account to login to by clicking on the "Advanced" button. The "Connection Profile" will be opened. Select the "Host" tab. By default, the "Username" textbox is left empty. If you want to login to a specific account that you owned, you should then fill in the "Username" textbox. You can leave the rest of the options as they are.

---

7. <https://tts.deisa.eu/UserSupport/>

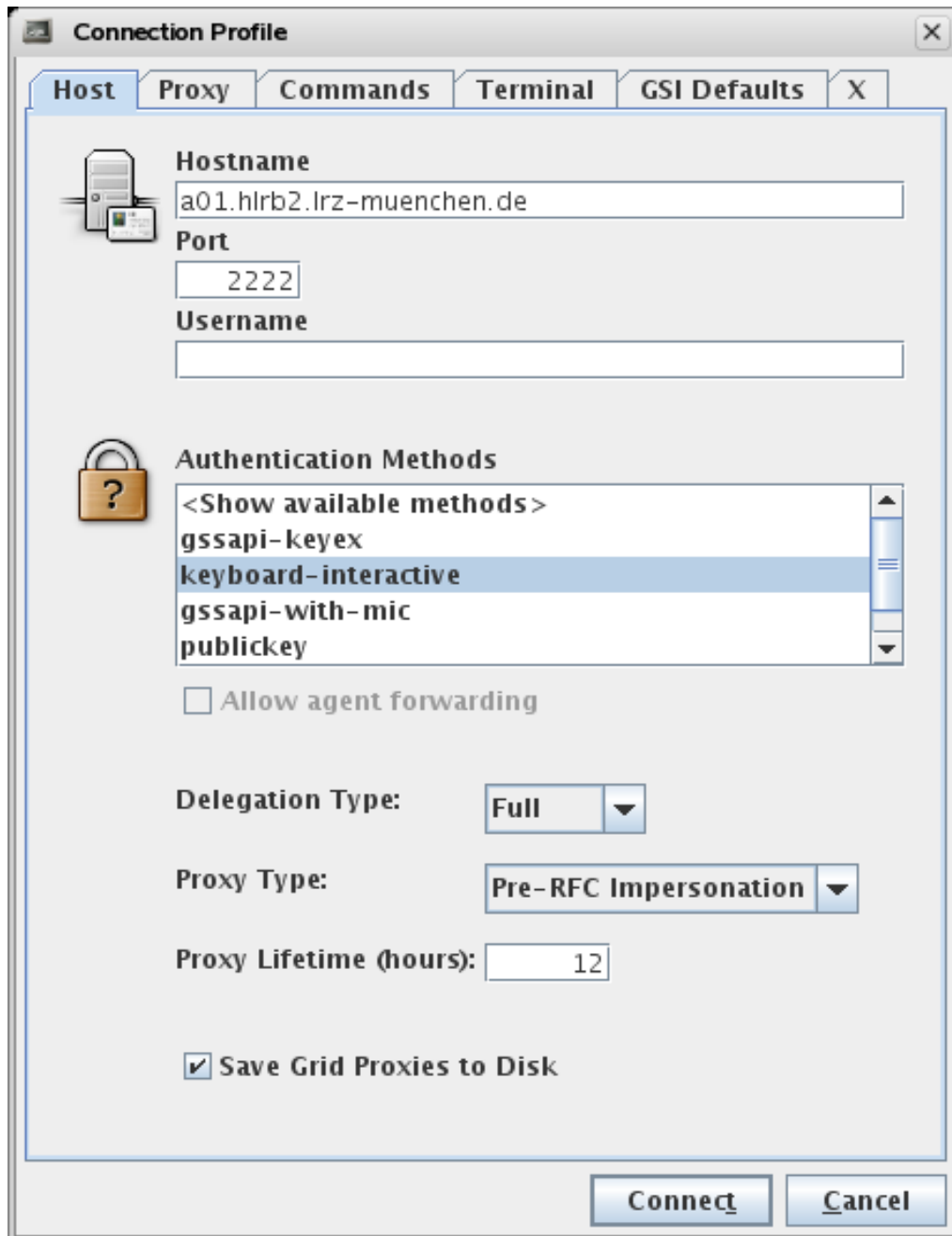


Figure 7: Connection Profile window

Now, select the "Connect" button.

You will be prompted to enter your "Grid Certificate Passphrase". Enter the passphrase of your grid certificate and click "Ok" or hit the "Enter" key of your keyboard.

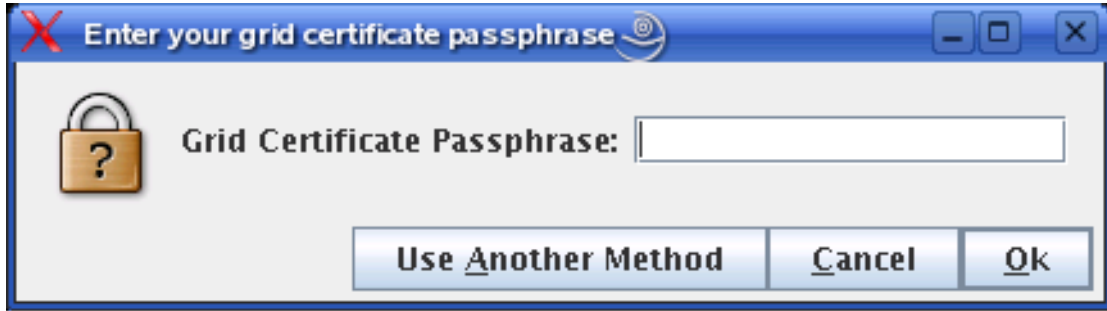


Figure 8: Enter your grid certificate passphrase dialog

If you do not have your \*.pem files and is using the grid certificate imported in the browser instead, you will be prompted to select the web browser where your grid certificate is imported. On Linux, only Firefox/Mozilla is supported. On Windows, Firefox/Mozilla and Internet explorer are supported. On Mac OS X, Safari and Chrome are supported via Keychain Access (only for DEISA customised version).



Figure 9: Web browser selection for authentication

In the case of Mozilla/Firefox, please enter your Mozilla/Firefox master password as your certificate store passphrase and select the "Ok" button.

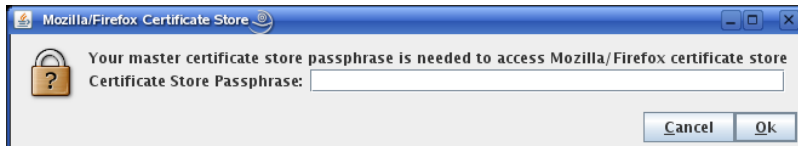


Figure 10: Mozilla/Firefox certificate store

In the case of Safari/Chrome on Mac OS X via Keychain access. If your certificate is not locked, you should be prompted with the following window. Select either "Allow" or "Always Allow" based on your personal preference. If your certificate is locked, you will be prompted an additional dialog to enter the password to unlock the particular keychain in Keychain Access.



Figure 11: Mac OS X security warning window

## Accessing DEISA Door Nodes using gsissh

If both authentication methods mentioned above are unavailable or unsuccessful, you can also access the grid resource via your \*.p12 keystore file. In the following window, in the section "Use a Grid certificate in pkcs12 format:", you will now be asked to specify the location of your pkcs12 keystore file: Click the "Browse" button and select the keystore file. Enter the keystore passphrase in the "Passphrase" textbox and select the "Use Certificate" button

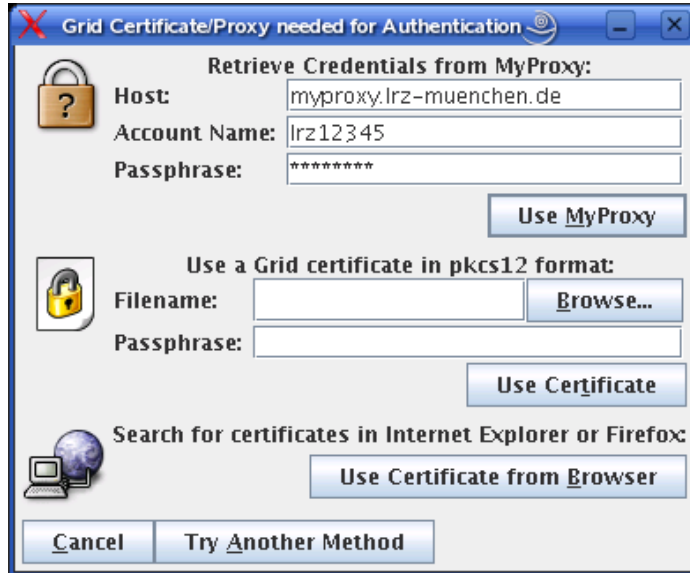


Figure 12: Grid certificate/proxy needed for authentication

You should now be logged on to the door node:

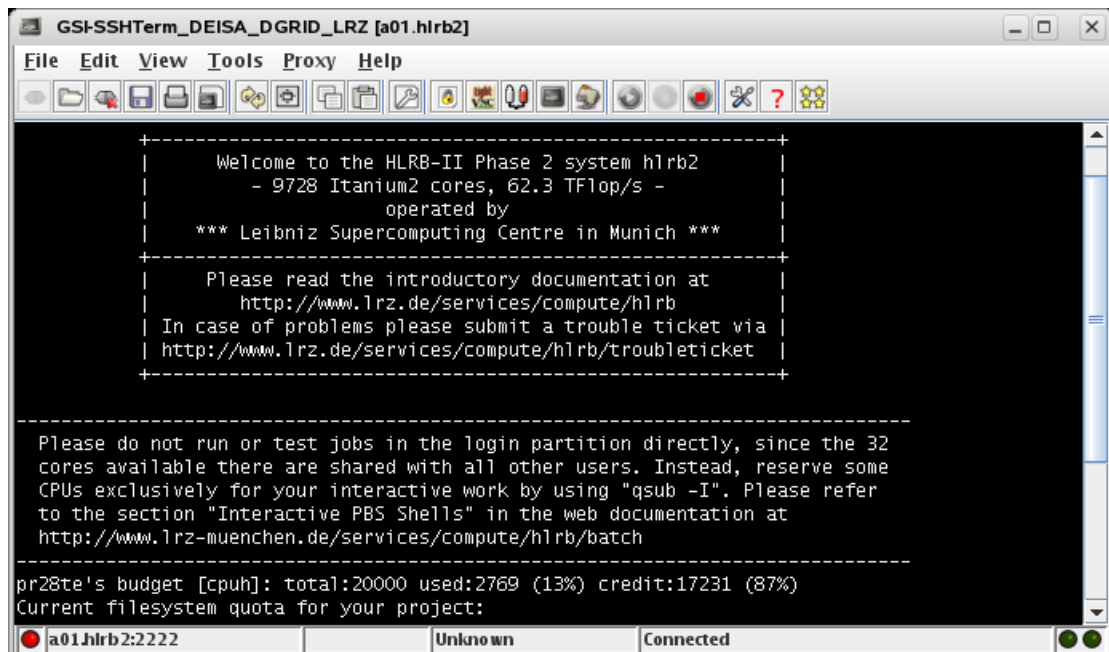


Figure 13: Welcome screen upon successful login

### 4.6 Using GSISSH-Term in DEISA environment

**To set up the proper DEISA and Globus environment, you have to load two *modulefiles*:**

```
module load deisa
module load globus
```

Alternatively, both modules can be loaded using the following sequence:

```
module load deisa globus
```

Only after issuing the “module load globus” command will you have access to the Globus client commands, such as gsissh. Other vital parameters that are needed to work with Globus are also set by “module load globus”, thus Globus commands will only work properly after this *modulefile* is loaded.

If the door node you used is not your Execution Site, then you have to use gsissh from the door node to the Execution Site via the internal DEISA network. This can be done very easily using the program `deisa_service`[4] (using the correct kind of inverted commas is essential!):

```
gsissh `deisa_service -i -s <execution site>`
```

For example, if SARA is the target the command is:

```
gsissh `deisa_service -i -s sara`
```

If you are not sure whether an Execution Site supports the service you require, you can also call `deisa_service` directly on the command line. If the service is not available, you will be notified.:

```
deisa_service -e -s <execution site>
```

Simply invoke

```
deisa_service
```

to obtain a list of valid options and their meaning.

gsissh (and gsissh-TERM) automatically transfer your proxy credentials (a short-lived copy of your credentials) to the target system, so that you do not have to type your passphrase a second time when using gsissh on the target machine to log into another remote machine. There is also no need to put your credentials (`usercert.pem` and `userkey.pem`) directly on any DEISA machine. For security reasons it is advisable to keep the `userkey.pem` file only on your private, local workstation. `$HOME` file systems (or the `$HOME/.globus` directory) on DEISA supercomputers may be mounted via NFS and storing your private key on an NFS file system may violate the policy of the Certification Authority that issued your personal certificate.

---

[1] If you only have your keystore file `cert.p12` (as used by UNICORE), then you can use the `cert.p12` file instead, however, it must not contain CA certificates, only your key and your public certificate. Your keystore passphrase should only contain printable ASCII characters. If you experience difficulties using your keystore file, use your `*.pem` files instead.

## Accessing DEISA Door Nodes using gsissh

[2] A word of caution: on networked Windows systems we observed that a different location on a shared drive is sometimes used. The exact path depends on the specifics of the respective local installation. In case of problems, please report them to the DEISA Helpdesk service.

[3] See <http://www.deisa.eu/usersupport/user-documentation/faq/CertificatesFAQ>

[4] Using `deisa_service` without parameters produces a short help screen:

```
deisa_service <network flag> <service flag> <site>
```

where the network flag distinguishes internal private DEISA network and external public Internet, the service flag identifies the Globus service, e.g., `gsissh`, `gridftp` or `WS-GRAM`, and the site acronym names the Execution Site.

## 4.7 Hints

- To check Java version, in your Linux/Unix/OS X terminal or Windows command prompt, please use the following command:

```
java -version
```

- To create a ".globus" directory in Windows, simply use the following command in your command prompt:

```
md .globus  
or  
mkdir .globus
```

- For your security, it is encouraged that you modify the access rights of your ".globus" directory and PEM certificates as follows.:

```
Unix/Linux/OS X:  
chmod 700 ~/.globus  
chmod 400 ~/.globus/*.pem
```

- Please use only printable ASCII characters for your certificate(keystore) passphrase. If you have used unprintable characters, please kindly change your passphrase and replace your "*userkey.pem*" with the following commands on a Unix/Linus/OS X machine:

```
mv userkey.pem userkey.pem.old  
openssl rsa -in userkey.pem.old -des3 -out userkey.pem
```

## Accessing DEISA Door Nodes using gsissh

- To convert your "*userkey.pem*" and "*usercert.pem*" to pkcs12 format, use the following commands on a Unix/Linux/OS X machine:

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

- To convert your pkcs12 keystore (e.g. keystore.p12) to PEM format, use the following commands on a Unix/Linux/OS X machine:

```
openssl pkcs12 -in keystore.p12 -out usercert.pem -clcerts -nokeys
openssl pkcs12 -in keystore.p12 -out userkey.pem -nocerts
```

- If you notice strange characters while using the delete and/or backspace keys on some machines, e.g. IBM AIX OS, in your shell, you can set your "*\$HOME/.inputrc*" as such

```
"\e[3~": delete-char
# this is actually equivalent to "\C-?": delete-char
# VT
"\e[1~": beginning-of-line
"\e[4~": end-of-line
# kvt
"\e[H":beginning-of-line
"\e[F":end-of-line
# rxvt and konsole (i.e. the KDE-app...)
"\e[7~":beginning-of-line
"\e[8~":end-of-line
```

More information is available at the following site<sup>[8]</sup>.

---

8. <http://www.ibb.net/%7Eanne/keyboard.html>