



Authentication in the NGS

John Kewley

`john.kewley@stfc.ac.uk`

NGS Support Centre Manager
STFC Daresbury Laboratory



Connecting Infrastructure

Connecting Research

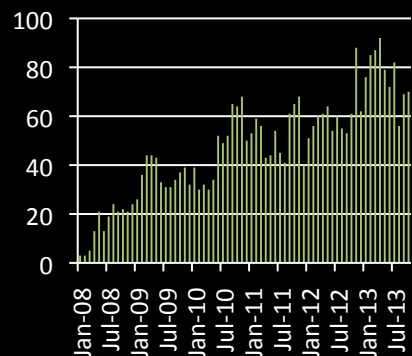


NGS

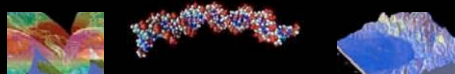
1. What is the NGS?
2. Growl: VDT installation + helper scripts
3. Some other NGS Authentication projects



>1000 cpu, ~500 db
~200 MyProxy users



> 75 applications



2nd largest e-Science CA

- 22,121 certificates issued
- 4,911 active currently

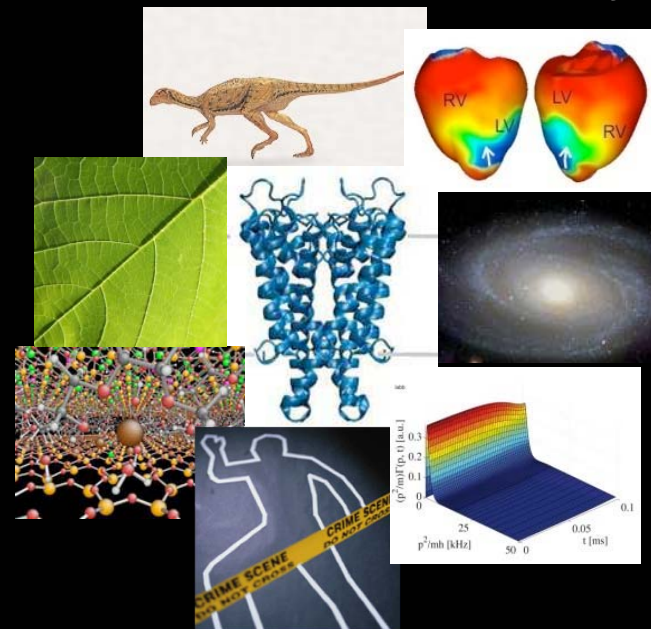
25 member institutes
33 heterogeneous resources
15,000 processing cores



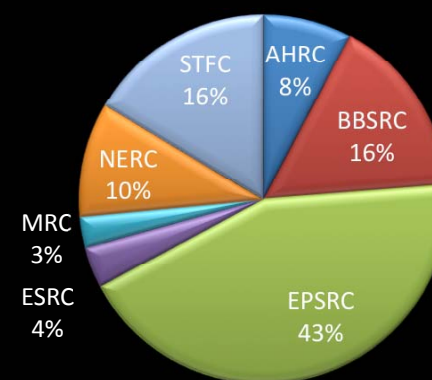
In the last 12 months

- 4,629,127 CPU hrs used
- 888,862 jobs ran

Diverse User Community



Funding Source



Connecting Infrastructure

Connecting Research

The NGS uses GSI for its Authentication

To support this we have:

- * UK e-Science CA (IGTF accredited, offline)
- * RA network across UK academia (61 RAs with 112 RA Operators)
- * 2 MyProxy servers

To support ancillary services mentioned later in this talk we also have

- * VOMS server
- * Training CA (for short-lived training certificates)
- * Test CA (for RA Training)
- * 2x SLCS online CAs (SSO and SARoNGS)



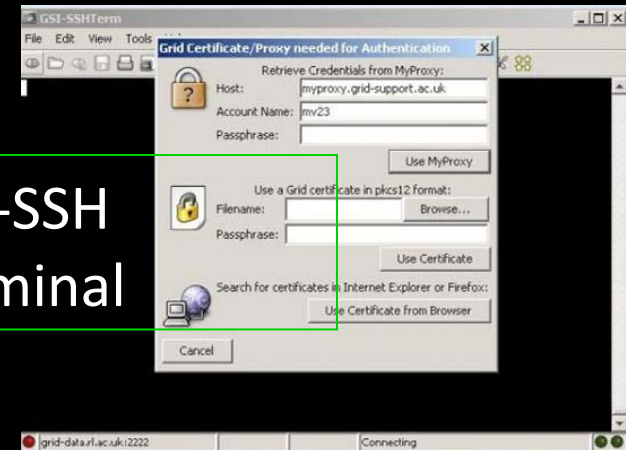
NGS Authentication



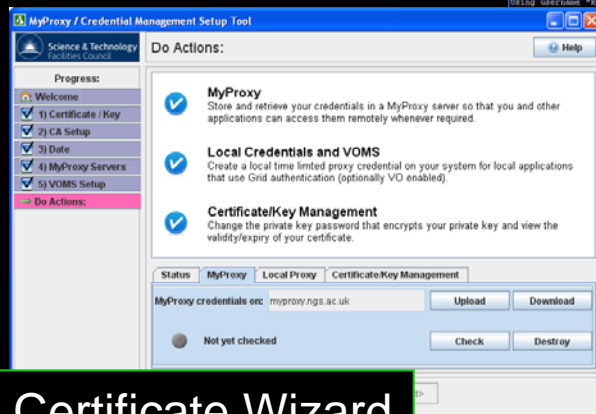
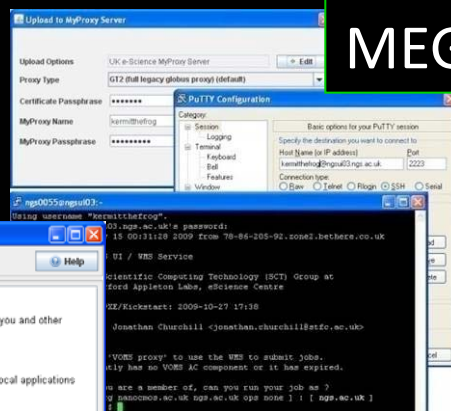
Direct access



GSI-SSH
terminal

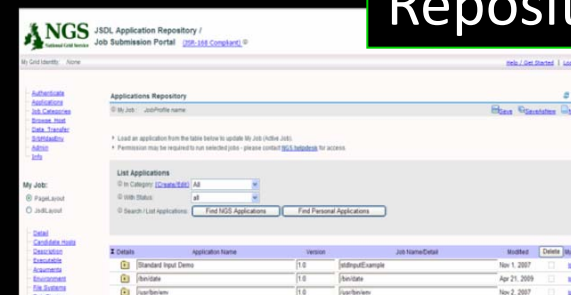


MEG



Certificate Wizard

NGS Portal/
Applications
Repository



Connecting Infrastructure

Connecting Research



3 Barriers

Three main barriers that newcomers find when using the Grid for the first time:

1. **Setting up the client-side middleware**
2. Handling of certificates
3. *[Job submission in the presence of firewalls]*



NGS

Installing Growl Scripts

1. Download GROWL Scripts

```
$ cd  
$ # possibly tell wget about http_proxy  
$ # export http_proxy=http://  
    wwwcache.dl.ac.uk:8080  
$ wget http://www.growl.org.uk/  
    GrowlScripts.tar.gz
```

2. Unpack into home directory

```
$ tar -zxvf GrowlScripts.tar.gz
```

3. "Build" VDT client

```
$ cd Growl  
$ make
```




NGS

GROWL Scripts: Contents

VDT client installation of globus, gsi-openSSH, VOMS and MyProxy

- `grid-proxy-init, grid-proxy-info`
- `globus-job-submit, globus-job-run`
- `gsissh, gsiscp, openssl`
- `myproxy-init, myproxy-info, myproxy-logon`
- `voms-proxy-init, voms-proxy-info`

Certificate helper scripts

- `mk-cert`
- `growl-info, growl-login, growl-logout`

GROWL wrapper scripts

- `growl-submit, growl-status, growl-get-output,`
- `growl-sh, growl-cp, growl-mkdir, growl-rm,,`
- `growl-pwd, growl-which, growl-get-jobmanager`
- `growl-queue`

Note: there is also a globus source build for non-VDT-supported platforms



3 Barriers

Three main barriers that newcomers find when using the Grid for the first time:

1. Setting up the client-side middleware
2. **Handling of certificates**
3. *[Job submission in the presence of firewalls]*



NGS

How many passwords

- Request Certificate
 1. Request certificate **PIN**
 2. [Confirm **PIN**]
 3. Present **PIN** at photoID check
 4. [**Master** Password if on FF]
- Export Certificate
 5. [**Master** Password if on FF]
 6. Backup/export password (**.p12**)
 7. Re-confirm backup/export password (**.p12**)
- Setup .pem files
 8. Unpack **.p12** for userkey
 9. Set **.pem** password
 10. Confirm **.pem** password
 11. Unpack **.p12** for usercert
- MyProxy Setup
 12. `myproxy-init (.pem)`
 13. [set **myproxy** pwd]
 14. [Confirm **myproxy** pwd]
- Obtain Grid proxy
 15. `myproxy-logon (myproxy pwd)`



Installation

GROWL scripts provide a simple way of installing Grid middleware on your client Linux machine:

Advantages:

- Don't need to be a privileged user
- Will download client middleware packages for your system (if supported by VDT)
- Will build client middleware (if not)
- Minimal setup/configuration
- About 10–15 mins (if all goes well !)



NGS

Credential conversion

~~\$ openssl -clcerts -nokeys -in JK.p12 -out userkey.pem~~

~~\$ openssl -nocerts -in JK.p12 -out usercert.pem~~

~~\$ openssl pkcs12 -clcerts -nokeys -in JK.p12 -out userkey.pem~~

~~\$ openssl pkcs12 -nocerts -in JK.p12 -out usercert.pem~~

\$ openssl pkcs12 -clcerts -nokeys -in JK.p12 -out usercert.pem

\$ openssl pkcs12 -nocerts -in JK.p12 -out userkey.pem

\$ chmod 444 usercert.pem

\$ chmod 400 userkey.pem





NGS

mk-cert

```
$ openssl pkcs12 -clcerts \  
  -nokeys -in usercred.p12 \  
  -out usercert.pem  
  <Pass1>  
  
$ openssl pkcs12 -nocerts \  
  -in usercred.p12 \  
  -out userkey.pem  
  <Pass1>  
  <Pass2>  
  <Pass2> [confirm]  
  
$ chmod 444 usercert.pem  
$ chmod 400 userkey.pem  
  
$ mv userkey.pem ~/.globus  
$ mv usercert.pem ~/.globus  
$ chmod 700 ~/.globus
```

```
$ mk-cert mykey.p12  
  <Pass1>  
  [<Pass2>]
```



NGS

Proxy helper scripts

- **growl-login** wraps `grid-proxy-init`, `myproxy-init` and `myproxy-logon`
- **growl-logout** wraps `grid-proxy-destroy` and `myproxy-destroy`
- **growl-info** wraps `grid-cert-info`, `myproxy-info` and `grid-proxy-info` and `openssl` and can be used with certificates in several formats



NGS

growl-logon

Only does what is needed

Generates a local proxy (if there isn't a valid one there already)

Options:

- -m : Uploads a credential to the myproxy server (but only if required)
- -v myVO : proxies generated or uploaded will contain a VOMS Attribute Certificate for myVO (VDT only - not in source build yet)
- -f : force generation / upload
- -D : debugging information



NGS

Uses of growl-login

1. Generation of a proxy credential from a grid certificate (c.f. `grid-proxy-init`)
2. Uploading a proxy credential to a MyProxy server for use from other clients or portals (c.f. `myproxy-init`)
3. Retrieving a proxy credential without a grid certificate (c.f. `myproxy-login`)



NGS

Uses of `growl-login`

1. Generation of a proxy credential from a grid certificate
- 2. Uploading a proxy credential to a myproxy server for use from other clients or portals**
3. Retrieving a proxy credential without a grid certificate (using myproxy)

NGS

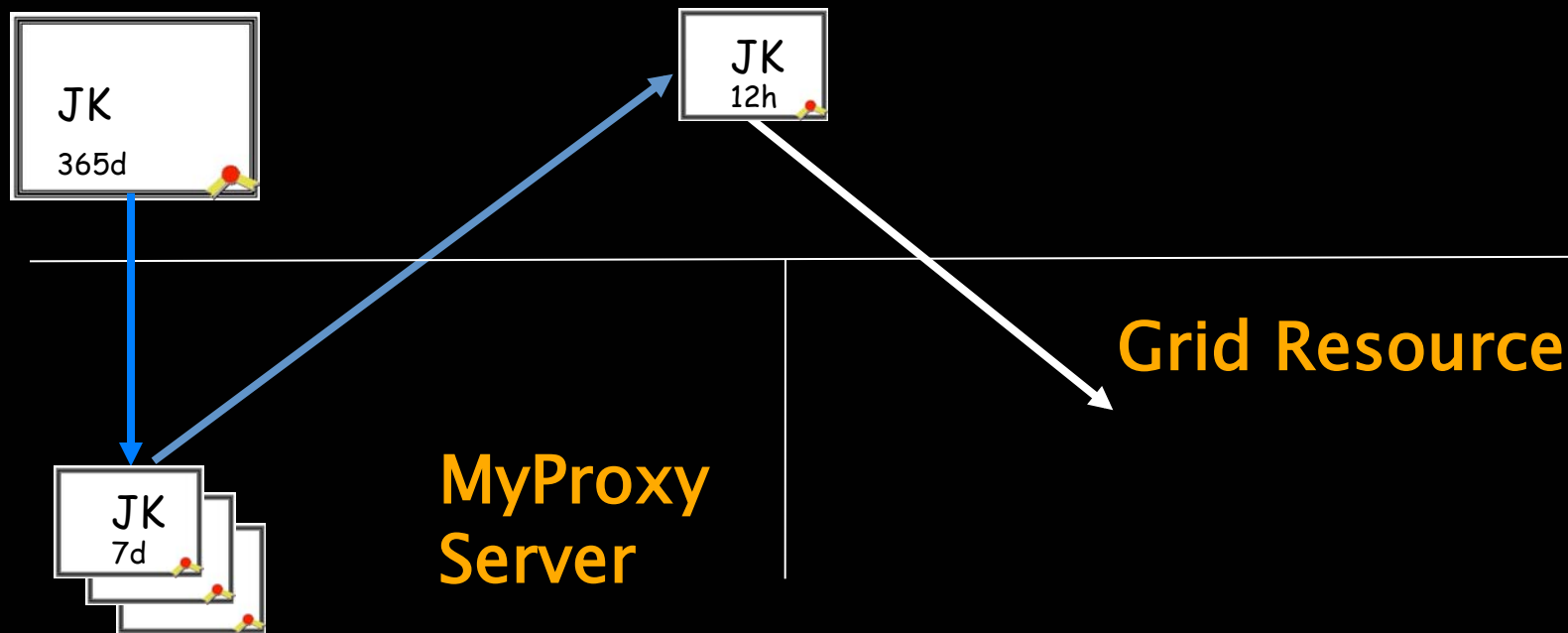
Use Case 2

```
$ myproxy-init  
<Grid Pass Phrase>  
<MyProxy Password>  
<MyProxy Password>  
$ myproxy-logon  
<MyProxy Password>
```

```
$ myproxy-init -L  
<Grid Pass Phrase>  
<MyProxy Password>  
<MyProxy Password>
```

Client

```
$ growl -login -m  
<Grid Pass Phrase>  
<MyProxy Password>
```



Connecting Infrastructure

Connecting Research



NGS

growl -i nfo

- Combines certificate info into one package
 - `grid-cert-info`
 - `myproxy-info`
 - `grid-proxy-info`
 - `voms-proxy-info`
- Reports on only certs and credentials it finds
- Issues warnings
- Notes when other certs are present (but are not the ones that `growl-login` would use)
- Can also be used with any certificate file to display its DN and validity and so can be used to check host, CA and VOMS-issuing certificate



growl -l logout

- Removes local proxy
- With `-m` option will also remove MyProxy credential from MyProxy server.



Advantages

- Symmetry
growl -l o g i n vs growl -l o g o u t
c.f. myproxy-l o g o n vs gri d-proxy-destroy
- Generally less passwords to type
- Single command automagically "*does the right thing™*"
 - Does nothing if no need
 - Utilises myproxy if credential present and valid
 - Uses existing proxy credential if still valid



Java Webstart Apps

Users have several options to logon to our resources including:

- * gsissh from globus, VDT or Growl on Linux
- * GSI-SSHTERM to logon to a head node
- * Using any ssh client (PuTTY, ssh) with MEG
- * The NGS Portal



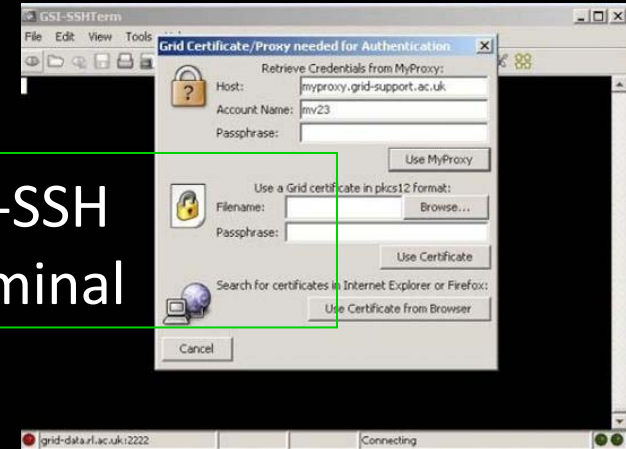
NGS Authentication



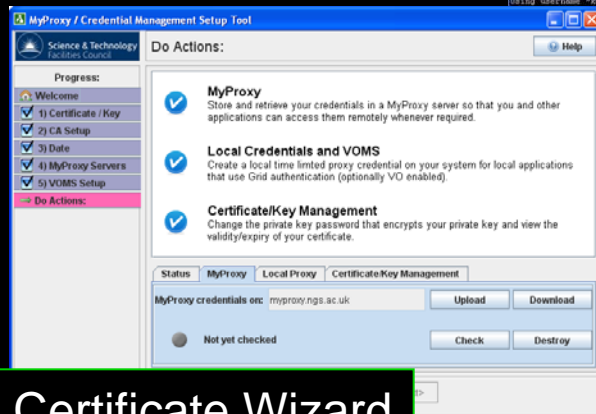
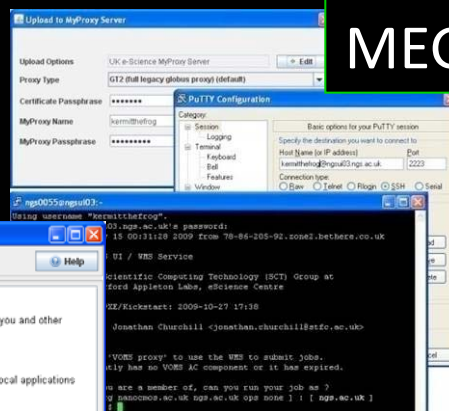
Direct access



GSI-SSH
terminal

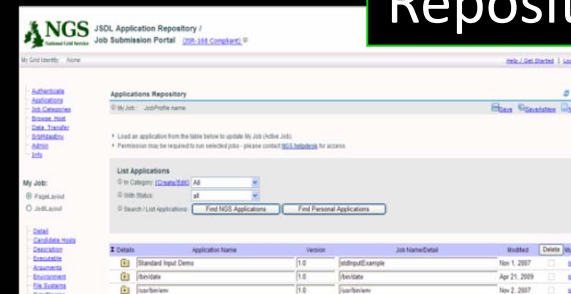


MEG



Certificate Wizard

NGS Portal/
Applications
Repository



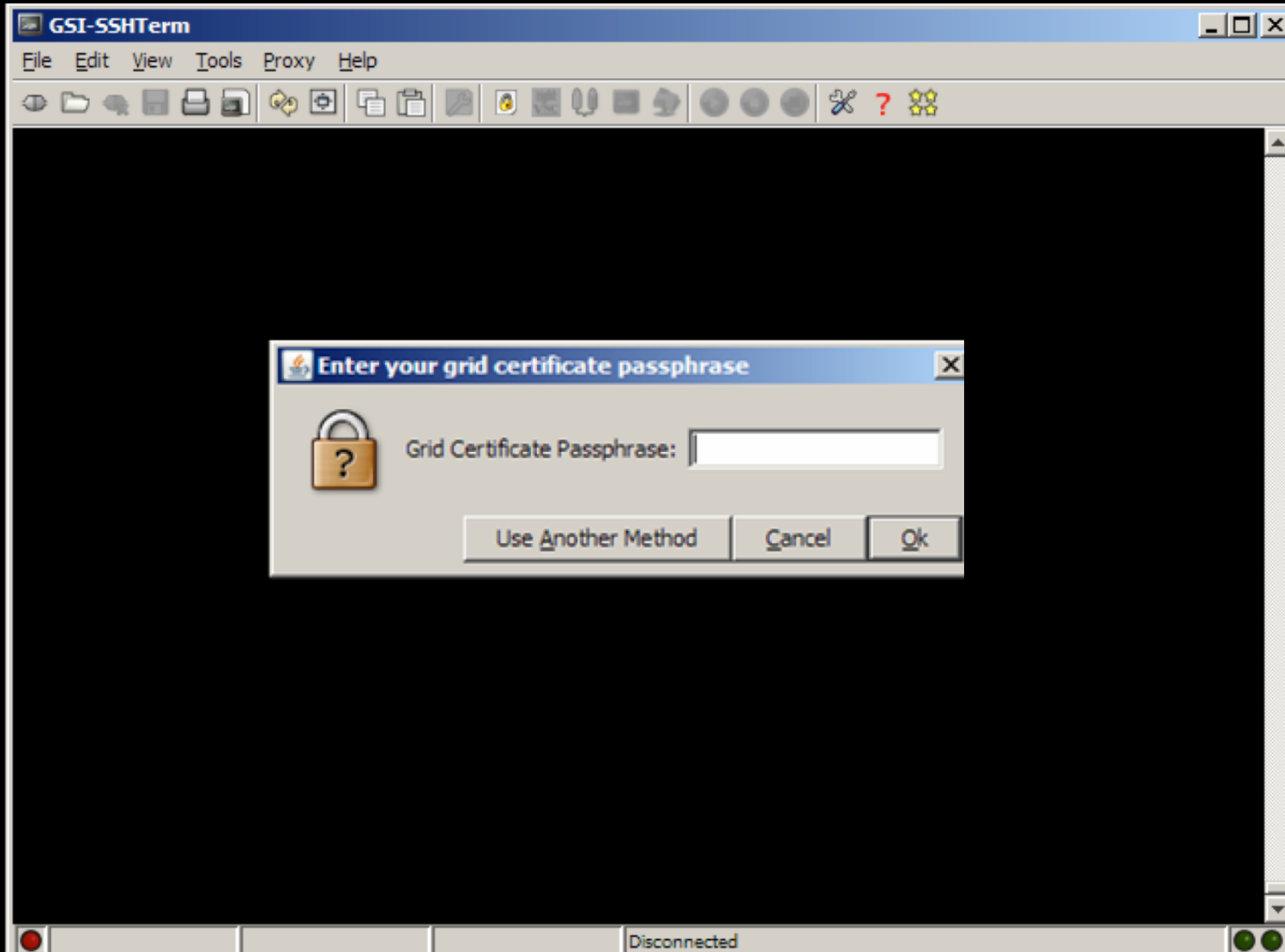
Connecting Infrastructure

Connecting Research



NGS

GSI-Enabled SShTERM



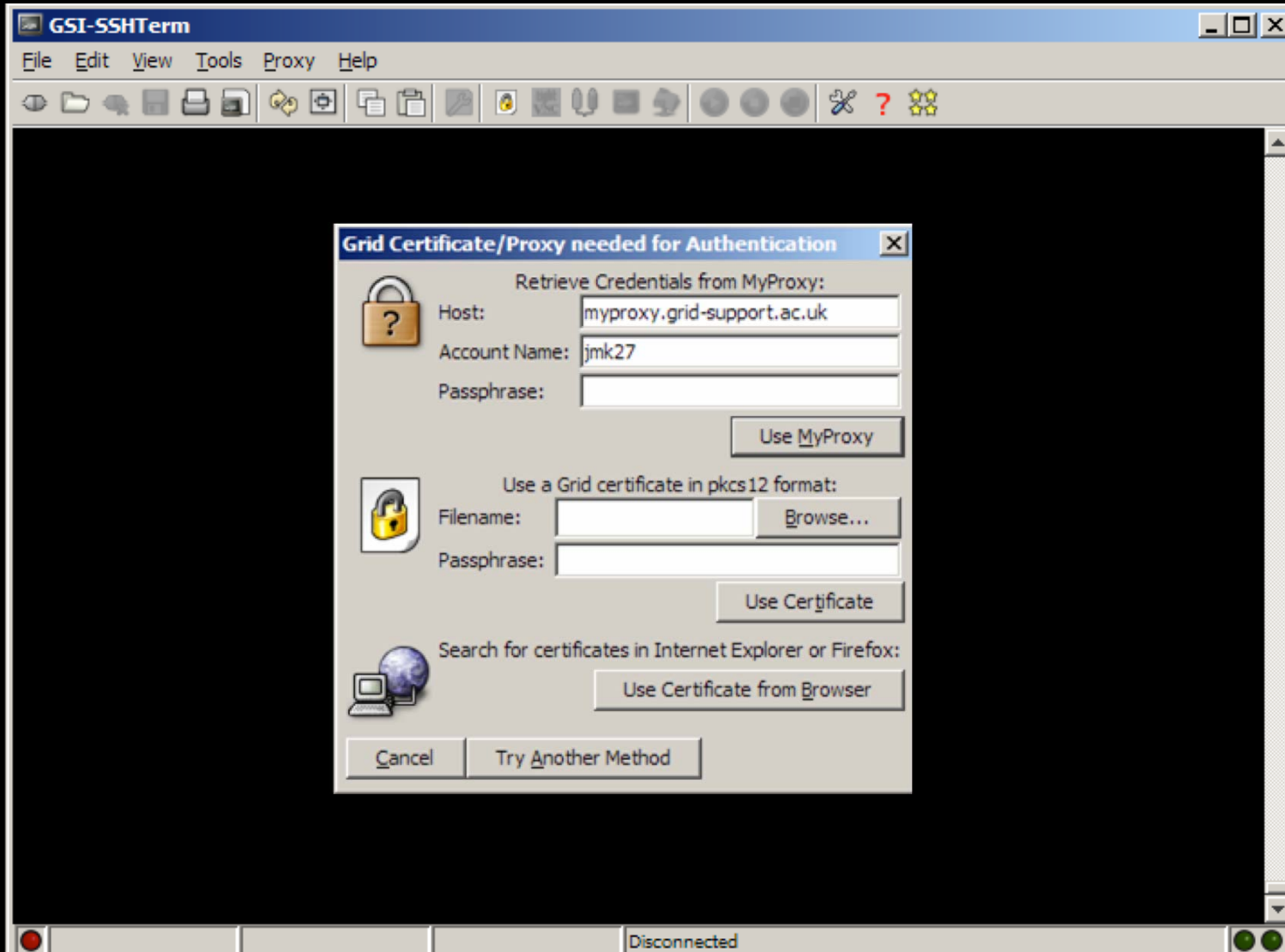
Connecting Infrastructure

Connecting Research



NGS

GSI-Enabled SShTERM



Connecting Infrastructure

Connecting Research



NGS

Certificate Wizard

MyProxy / Credential Management Setup Tool

Science & Technology Facilities Council

Progress:

- Welcome
- ☒ 1) Certificate / Key
- ☒ 2) CA Setup
- ☒ 3) Date
- ☒ 4) MyProxy Servers
- ☒ 5) VOMS Setup
- Do Actions:**

Do Actions: [Help](#)

☒ **MyProxy**
Store and retrieve your credentials in a MyProxy server so that you and other applications can access them remotely whenever required.

☒ **Local Credentials and VOMS**
Create a local time limited proxy credential on your system for local applications

Upload to MyProxy Server

Upload Options: UK e-Science MyProxy Server [Edit](#)

Proxy Type: GT2 (full legacy globus proxy) (default)

Private Key Password:

MyProxy Name: foo

MyProxy Password:

☐ Save Default Local Proxy

[OK](#) [Cancel](#)

[Send to Tray](#) [<Previous](#) [Next>](#)

Connecting Infrastructure

Connecting Research



NGS

NGS Member Institutions, Autumn 2009



MANCHESTER
1824



Imperial College
London

Royal Holloway
University of London

HPC
CAPABILITY COMPUTING



Science & Technology Facilities Council
Rutherford Appleton Laboratory

University of Westminster



UNIVERSITY OF
Southampton

CARDIFF
UNIVERSITY



University
of Glasgow



The University of Reading



Brunel
UNIVERSITY
WEST LONDON



KEELE
UNIVERSITY



Durham
University



UNIVERSITY OF
BIRMINGHAM



UNIVERSITY OF
LIVERPOOL



The
University
Of
Sheffield.

THE UNIVERSITY of York

wellcome trust
sanger
institute

Connecting Infrastructure

Connecting Research