

# Introduction to Programming and Computing for Scientists

Oxana Smirnova

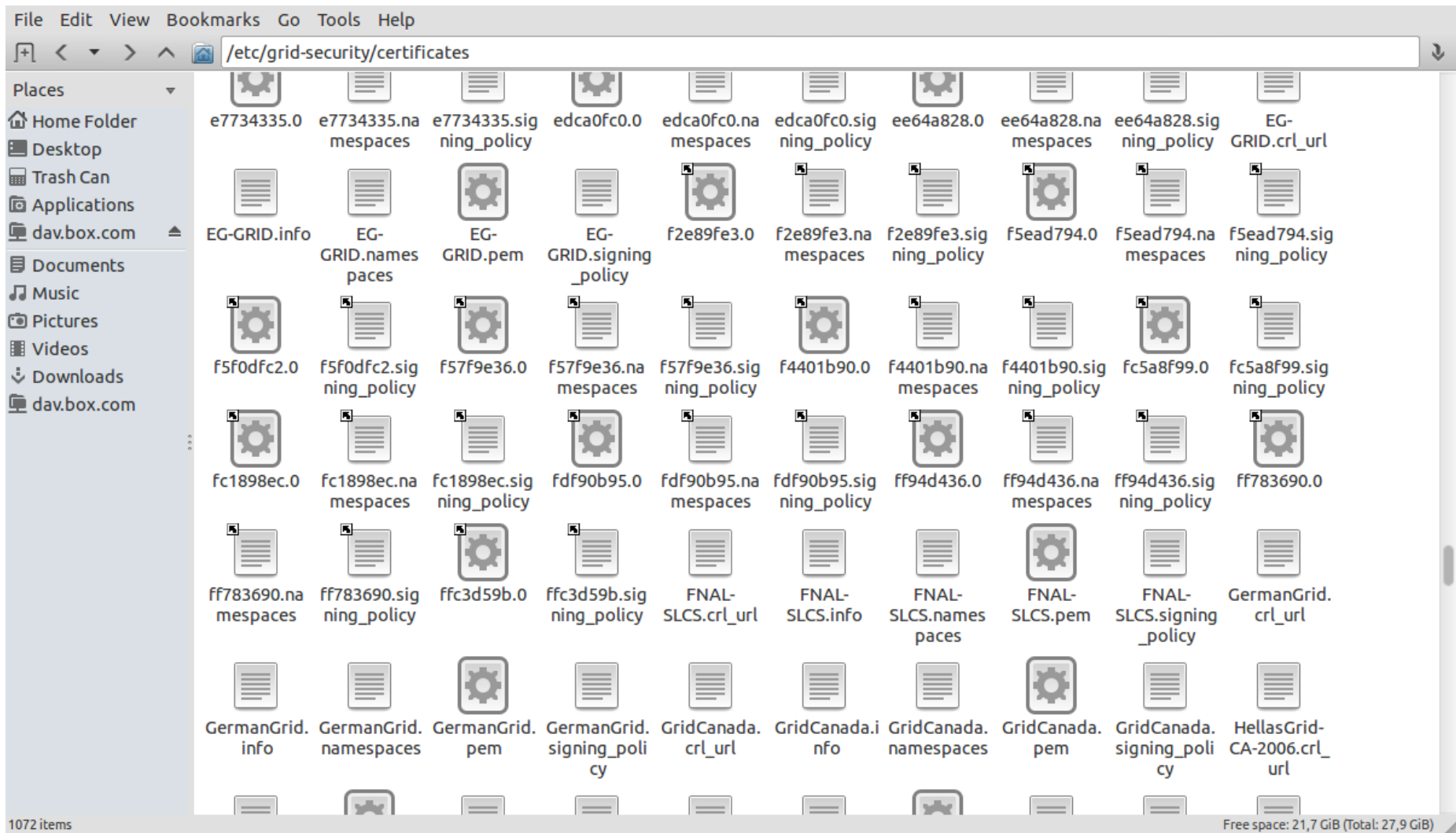
Lund University

Tutorial 4b: Grid certificates and jobs

# Step 1: Install public Certificate Authority certificates

- Before doing anything on the Grid, you will need to obtain **IGTF Certificate Authorities certificates**
  - Packages are available from IGTF and some Grid repositories
    - The packages include Certificate Revocation Lists (CRLs)
  - Regular updates for CRL and IGTF packages must be in place
    - Usually happens automatically
  - **Our virtual machines and cluster have them already**
    - Inspect **`/etc/grid-security/certificates`**
      - Hint: use **`ls -al`**

# /etc/grid-security/certificates in the course Virtual Machine



## Step 2: get your own keys and certificates

There are two main ways of storing personal certificates:

- Two files: private key and public certificate
  - Grid uses PEM encoding for keys and certificates (ASCII)
  - Standard file names: **userkey.pem** and **usercert.pem**
    - Note: public key is inside the CA-signed certificate **usercert.pem**
- Single file: PKCS#12 formatted certificate, containing private and public keys, as well as CA signature and CRL info
  - PKCS#12 certificate (**.p12**) is used mostly by browsers, but can also replace PEM files in some Grid tools
  - One can convert PKCS#12 file to PEM files and vice versa

- Private keys must not be copied over the network!
- Private keys can not be stored in public machines like ours in this class!
- Because of this, we will log in to the Iridium cluster and create the keys there

# Log in to Iridium and launch a Web browser there:

- Log in to Iridium:

```
ssh -X yourlogin@pptest-iridium.lunarc.lu.se
```

- Launch a Web browser:

```
firefox &
```

- Some useful commands – a reminder:

```
ls -al  
mkdir something  
cd something  
cp ~/dir/file1 file2  
geany &
```

# How to get a certificate

## The easy way:

Google for “TCS escience portal” and find a link to the “TCS Portal”

Log in using your university credentials

Follow the instructions

The certificate in PKCS#12 format will be stored in your browser certificate store

You can export the certificate into a file (.p12) and extract PEM files, if necessary

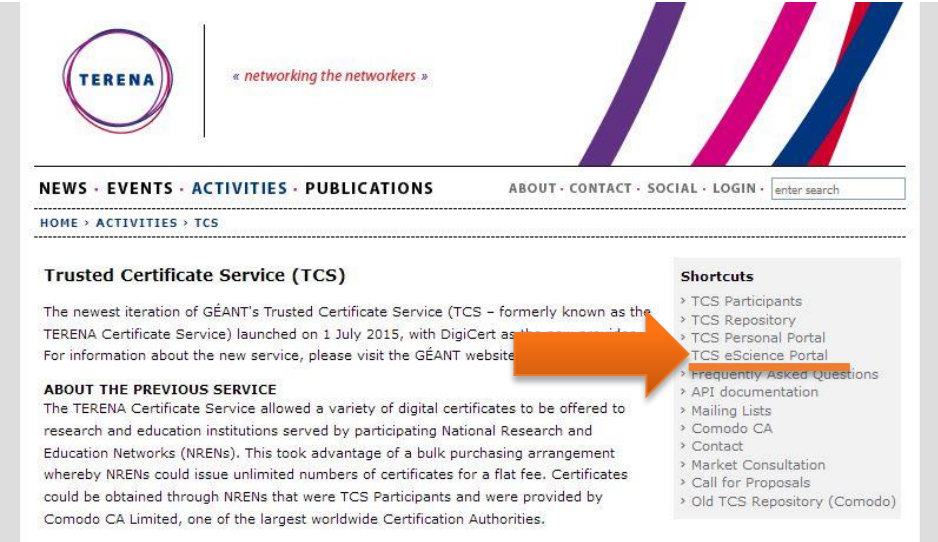
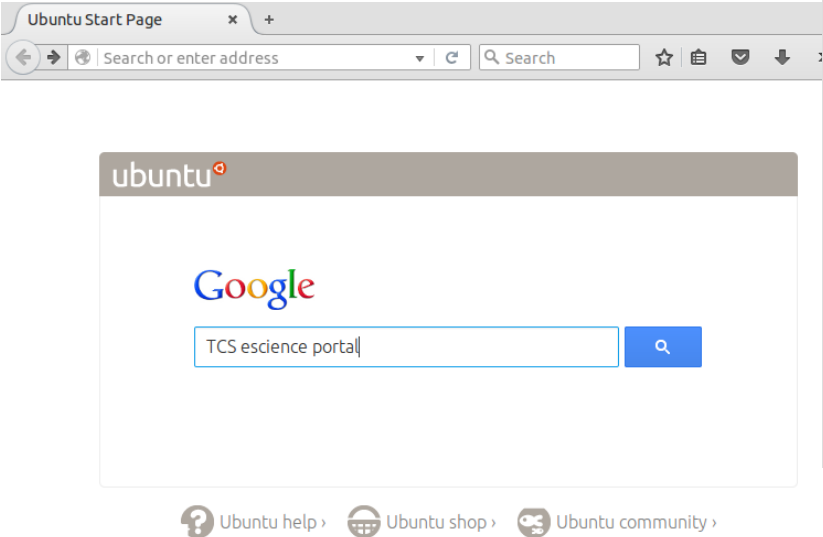
## How does it work:

Browser creates private and public keys for you

Public key is sent to TERENA CA, along with information that University provides about you

Signed public certificate is returned back to your browser, and merged with the private key to create a PKCS#12 certificate

# Google TCS e-Science portal



- Hint: Swedish SNIC Wiki has good instructions!
  - The “official” chain is rather cumbersome: 1st Google hit will be TERENA, which will direct you to GEANT, which finally will direct you to the TCS Portal

... TCS community. It is up-to-date with re-  
 portant role in signing digital certificates  
 e secure SHA-2-supported certificates that

ecure sessions with end clients.  
 GTF compliant).  
 g email communications.  
 ited over the Internet.  
 from Adobe PDF, Microsoft Office, Open-

working or being maintained. Now the only  
 still be used (solely for revocation of certifi-

play/TCSNT

**At a glance**

**Users**  
 TCS provides NRENs with cost-ef-  
 fective and easy to use manage-  
 ment of digital certificates

**Key Facts**  
 TCS is provided in partnership  
 with DigiCert one of the leading  
 Certification Authorities world-  
 wide.

**Quick Links**  
[TCS Wiki](#)  
[TCS Portal](#)



# Login to TCS eScience Portal



## IDP Selection

Please enter the Identity Provider to authenticate with:

Lund University

Start single sign-on

- If asked whether to remember Lund University as Identity Provider, feel free to answer “yes”



# Enter your LU credentials



SVENSKA

## LUND UNIVERSITY

Please enter your userid without "@lu.se" at the end.

Username:

Password:

**LOGIN**

This is Lund University Central Authentication Service (CAS). For privacy and security reasons, you should always log out and close all browser windows when you are done accessing services that require authentication. If you use Apple Mac OS X, you must also shut down the entire browser, not just the windows. If you use a public computer, it is especially important that you close all browser windows before you leave your computer.

# Request “Grid Premium” certificate



## Request a Certificate

Choose a product



Product:

CSR:  
(optional)

Common Name: Oxana Smirnova quar-osm@lu.se

Email: oxana.smirnova@hep.lu.se

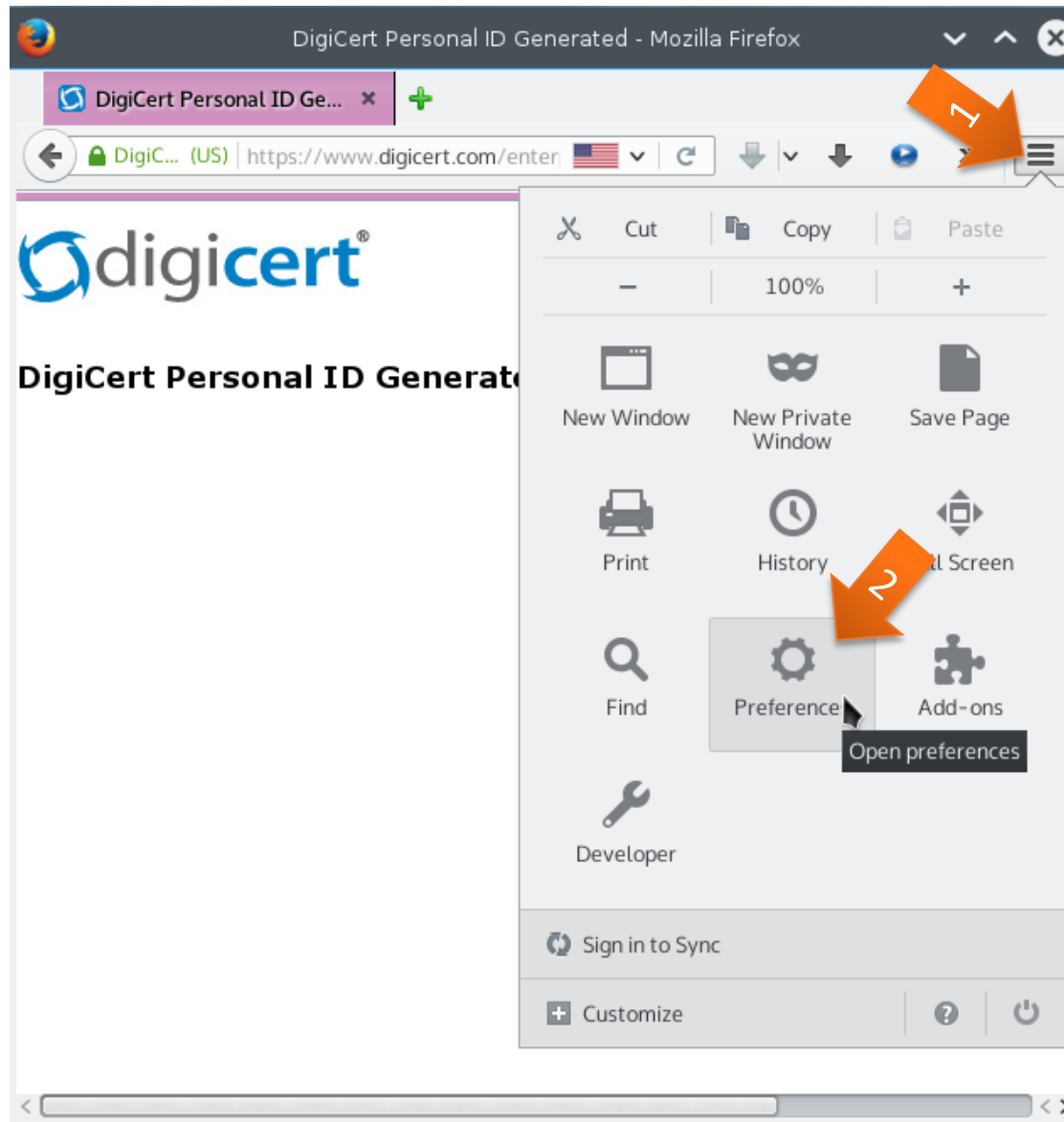
Organization: Lunds universitet



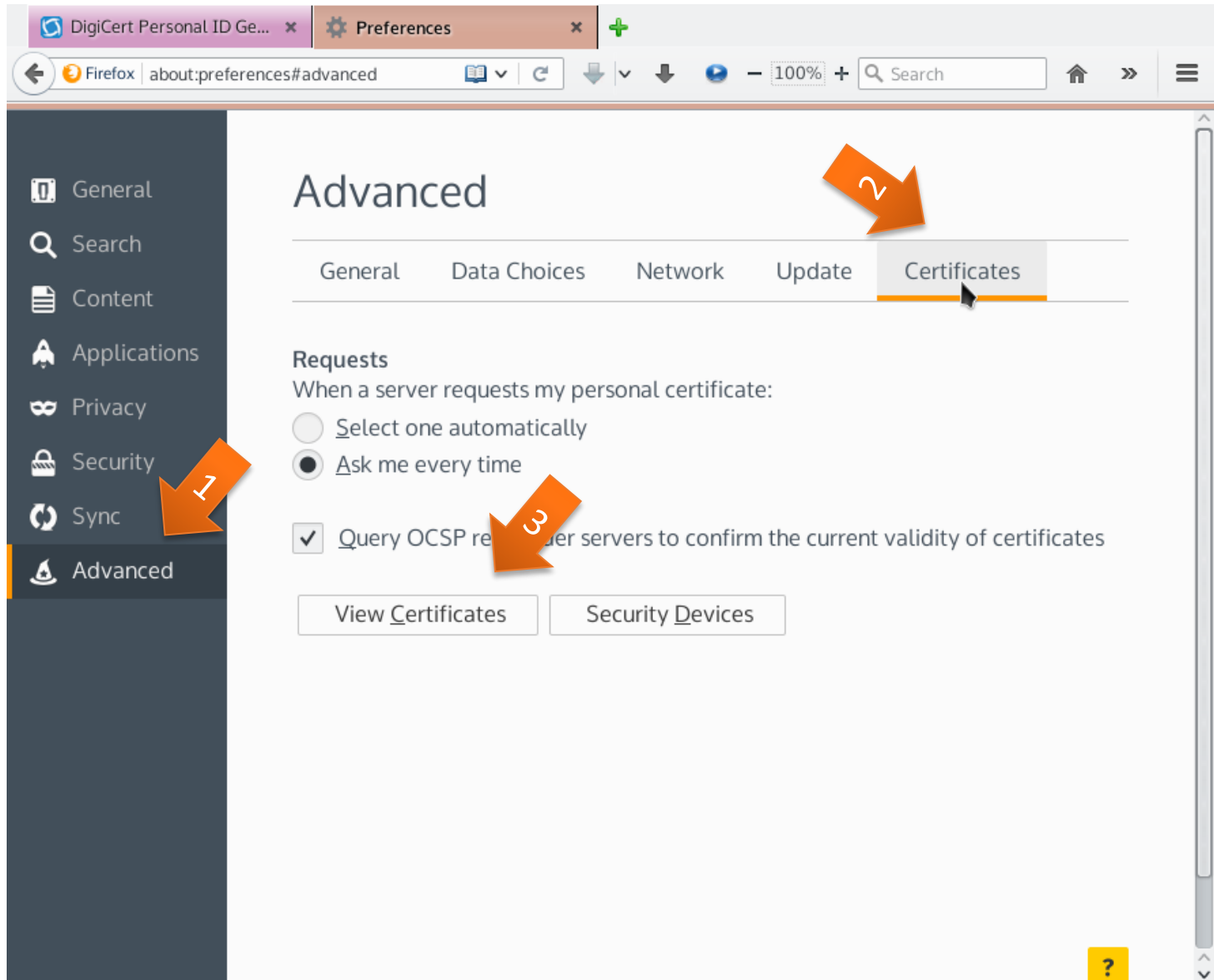
- If asked whether to trust the CA, feel free to tick “yes” everywhere

- If request is denied, skip to slide 17

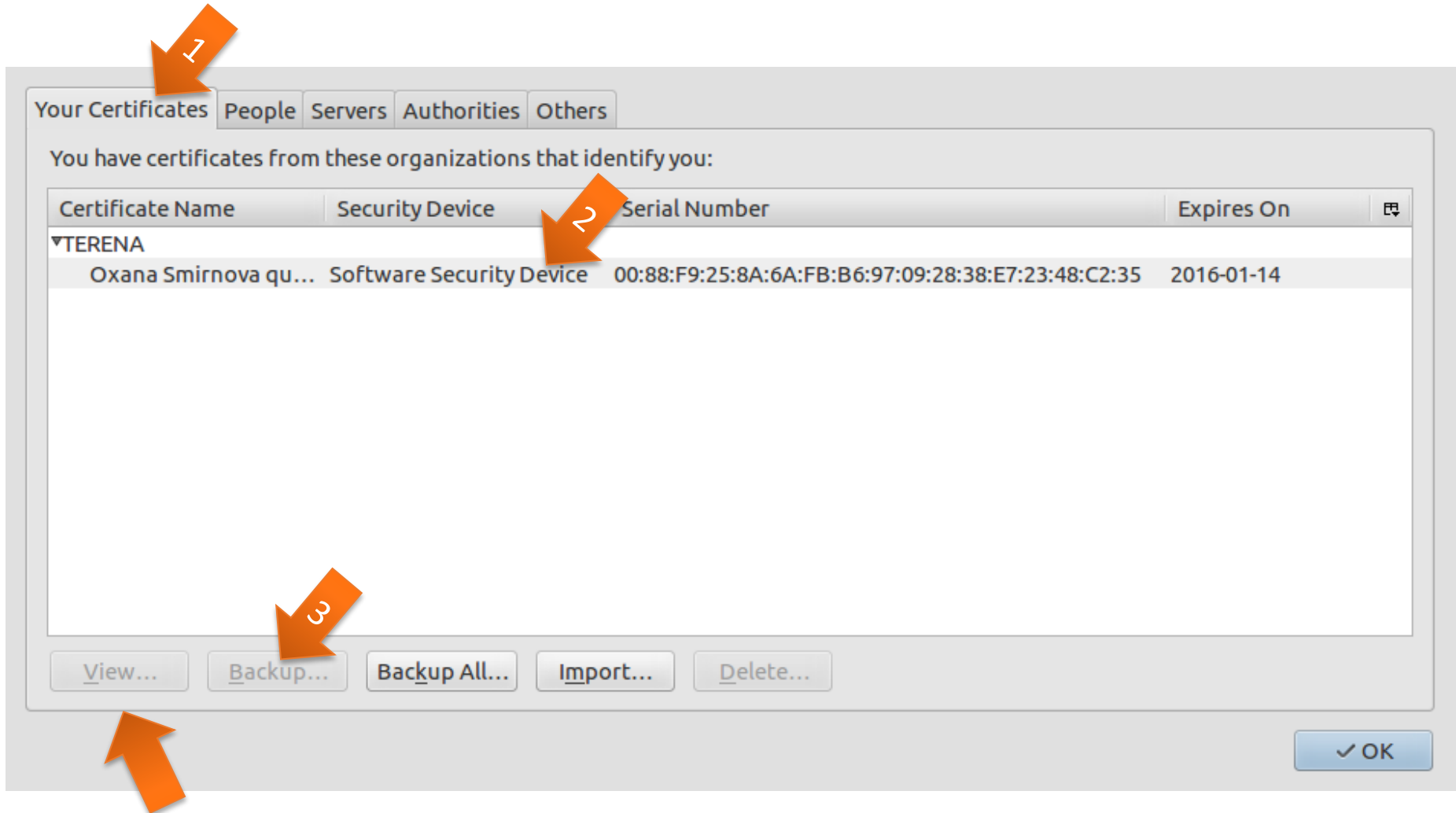
# Backup the certificate as a file



# Go to Advanced – Certificates – View Certificates

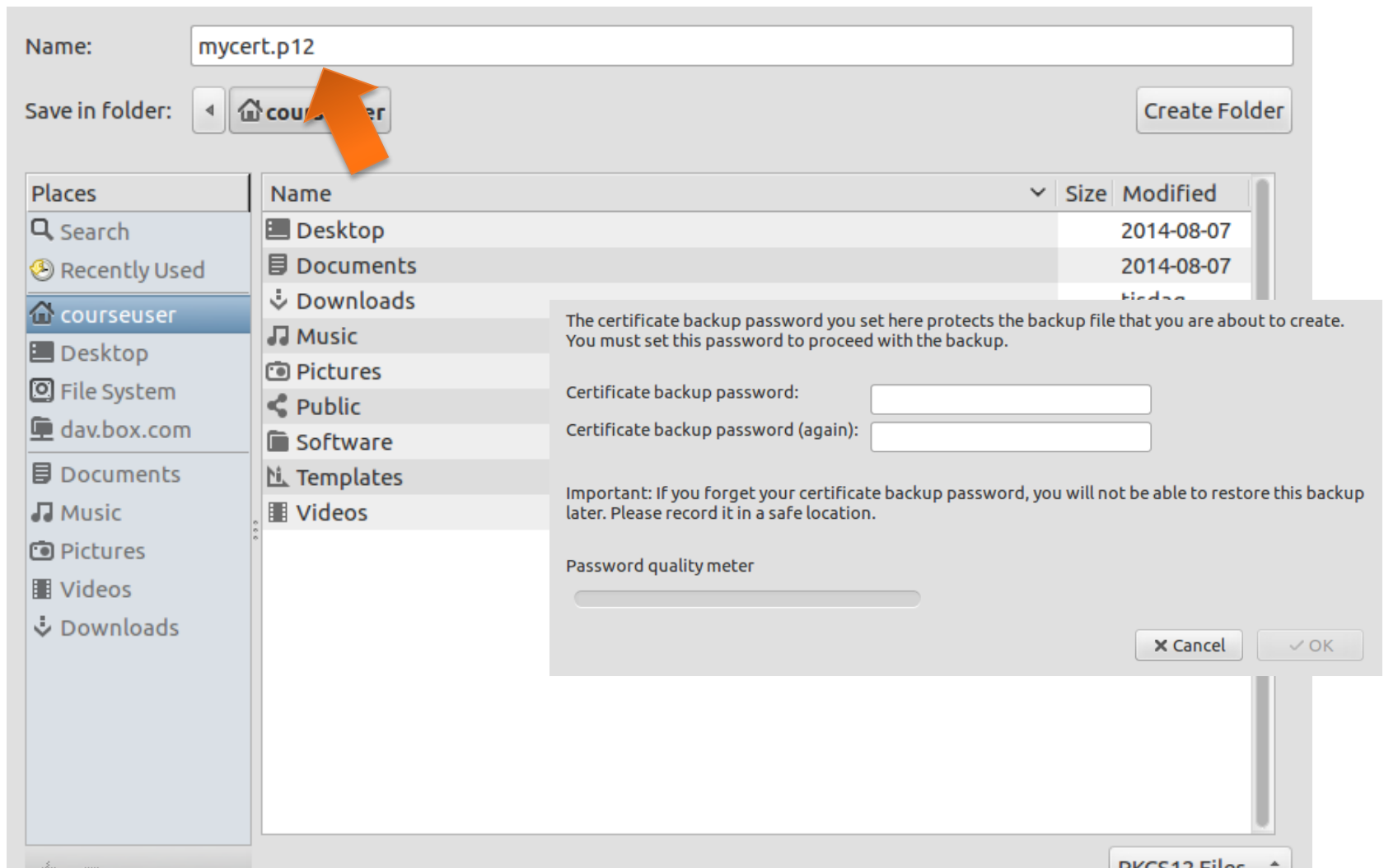


# In Your Certificates, find yours, and use Backup to save it



Take some time to view the certificate content

# Backup the certificate as a file with extension .p12



- Choose any password you like

# Extract private and public keys

- Create a hidden directory `~/ .globus`
  - This is the default location for Grid certificates
- Use `openssl` command to extract the keys inside `~/ .globus` :
  - Private key:

```
openssl pkcs12 -nocerts -in mycert.p12 -out userkey.pem
```
  - Public key:

```
openssl pkcs12 -clcerts -nokeys -in mycert.p12 -out usercert.pem
```
  - Hint: Google for “grid certificate howto” to find where to copy-and-paste from
  - “*Import Password*” is the one you used to backup `mycert.p12` from the browser
  - “*pass phrase*” for PEM key is your own choice
    - You can use the same password in both cases
- Copy the files to `userkey.pem` and `usercert.pem` into `~/ .globus`
  - Make sure that `userkey.pem` is readable only by you!
    - Hint: use `ls -al` and `chmod`

# Summary of the steps:

```
oxana@bornholm:~/globus >
oxana@bornholm:~/globus >
oxana@bornholm:~/globus > openssl pkcs12 -nocerts -in terena-15.p12 -out userkey-terena15.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
oxana@bornholm:~/globus > openssl pkcs12 -clcerts -nokeys -in terena-15.p12 -out usercert-terena15.pem
Enter Import Password:
MAC verified OK
oxana@bornholm:~/globus > ls -al *terena15*
-rw-rw-r-- 1 oxana oxana 2279 нояб. 25 01:33 usercert-terena15.pem
-rw-rw-r-- 1 oxana oxana 2018 нояб. 25 01:32 userkey-terena15.pem
oxana@bornholm:~/globus > chmod 400 userkey-terena15.pem
oxana@bornholm:~/globus > ls -al *terena15*
-rw-rw-r-- 1 oxana oxana 2279 нояб. 25 01:33 usercert-terena15.pem
-r----- 1 oxana oxana 2018 нояб. 25 01:32 userkey-terena15.pem
oxana@bornholm:~/globus > █
```

- Skip to slide 27



## In case TCS request fails:

- Backup solution: we can use pre-installed certificates on the Iridium cluster
  - We issued the certificates ourselves, so they are **not good** for any real purpose: we are not a trusted Certificate Authority

Plan B

# Work with the public and private keys: browser gymnastics

- Create a hidden directory `~/ .globus`
  - This is the default location for Grid certificates
- Find the directory called `certs` in your home: it will contain two keys:  
`userkey-<username>.pem`  
`usercert-<username>.pem`
- Copy these files to `userkey.pem` and `usercert.pem` in `~/ .globus`
  - Check that `userkey.pem` is readable only by you!
    - Hint: use `ls -al`
- Use `openssl` command to create a `.p12` certificate (one line):  

```
openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out cert.p12 -name "My toy certificate"
```

  - Hint: Google for “grid certificate howto” to find where to copy-and-paste from
  - “*pass phrase*” for PEM key: `gridcourse2015`
  - “*Export password*” is the one you will use in the browser
    - You can use the same password in both cases

Plan B

# Summary of the steps:

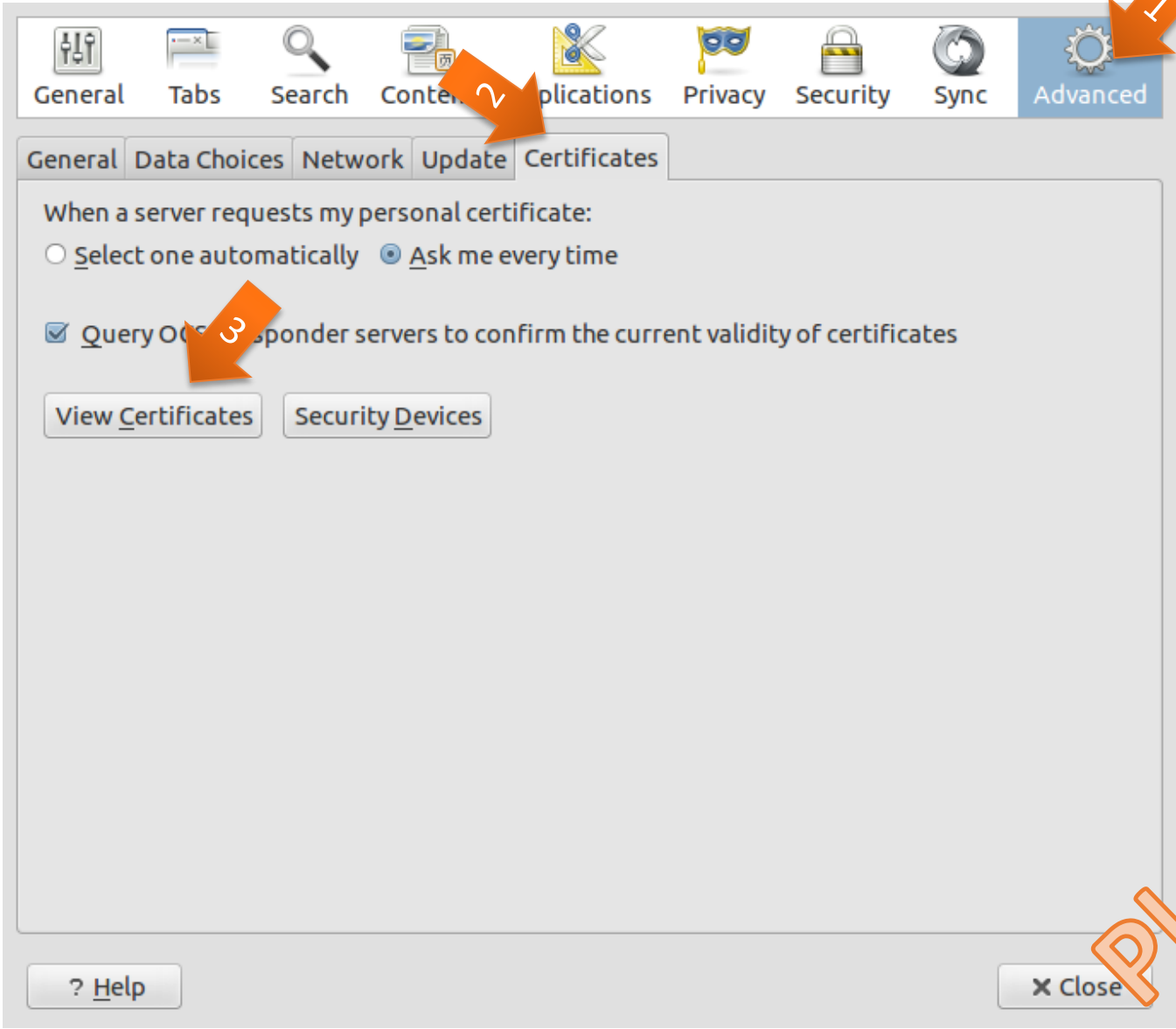
```
File Edit Tabs Help
courseuser@Lubuntu-VirtualBox:~$ mkdir .globus
courseuser@Lubuntu-VirtualBox:~$ cd .globus
courseuser@Lubuntu-VirtualBox:~/globus$ cp ~/certs/usercert-progcourse7.pem usercert.pem
courseuser@Lubuntu-VirtualBox:~/globus$ cp ~/certs/userkey-progcourse7.pem userkey.pem
courseuser@Lubuntu-VirtualBox:~/globus$ ls -al
total 16
drwxrwxr-x  2 courseuser courseuser 4096 dec 18 21:44 .
drwxr-xr-x 24 courseuser courseuser 4096 dec 18 21:43 ..
-rw-r--r--  1 courseuser courseuser 2085 dec 18 21:44 usercert.pem
-r-----  1 courseuser courseuser 2022 dec 18 21:44 userkey.pem
courseuser@Lubuntu-VirtualBox:~/globus$ openssl pkcs12 -export -in usercert.pem -inkey userkey
.pem -out cert.p12 -name "My toy certificate"
Enter pass phrase for userkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
courseuser@Lubuntu-VirtualBox:~/globus$ ls -al
total 20
drwxrwxr-x  2 courseuser courseuser 4096 dec 18 21:45 .
drwxr-xr-x 24 courseuser courseuser 4096 dec 18 21:43 ..
-rw-rw-r--  1 courseuser courseuser 2986 dec 18 21:45 cert.p12
-rw-r--r--  1 courseuser courseuser 2085 dec 18 21:44 usercert.pem
-r-----  1 courseuser courseuser 2022 dec 18 21:44 userkey.pem
courseuser@Lubuntu-VirtualBox:~/globus$ □
```

Plan B

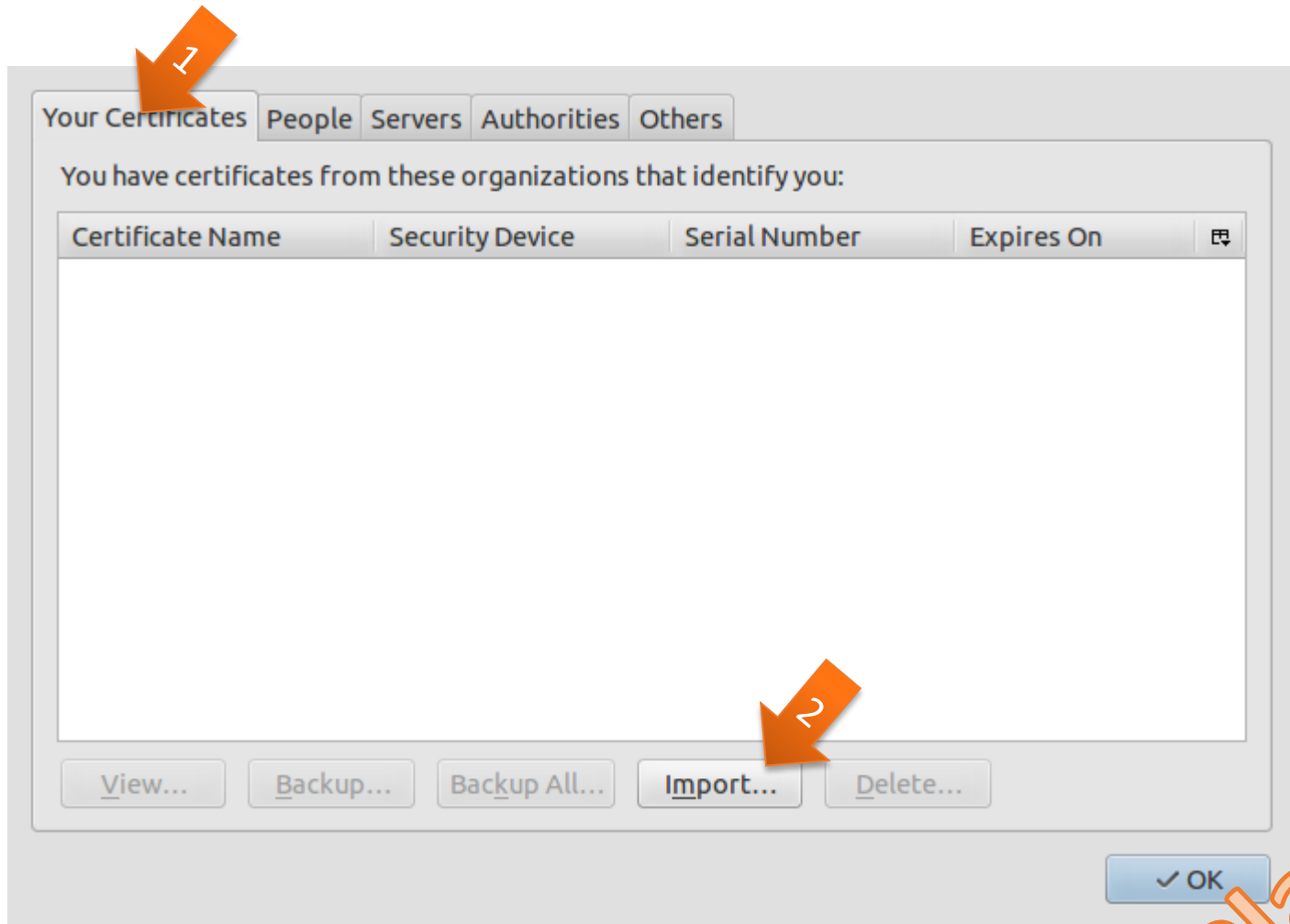
# Load the certificate into the browser (start firefox)

The screenshot shows a Firefox browser window with the address bar at `www.nordugrid.org/documents/certificate_howto`. The page content includes instructions for converting certificates and extracting keys, with terminal commands in code blocks. An orange arrow labeled '1' points to the browser's menu icon in the top right corner. The menu is open, showing options like Cut, Copy, Paste, New Window, New Private Window, Save Page, Print, History, Screen, Find, Preferences, Add-ons, Developer, Sign in to Sync, and Customize. An orange arrow labeled '2' points to the 'Preferences' option, which is highlighted with a black box containing the text 'Open preferences'. A large orange watermark 'Plan B' is visible in the bottom right corner of the browser window.

# Go to Advanced – Certificates – View Certificates

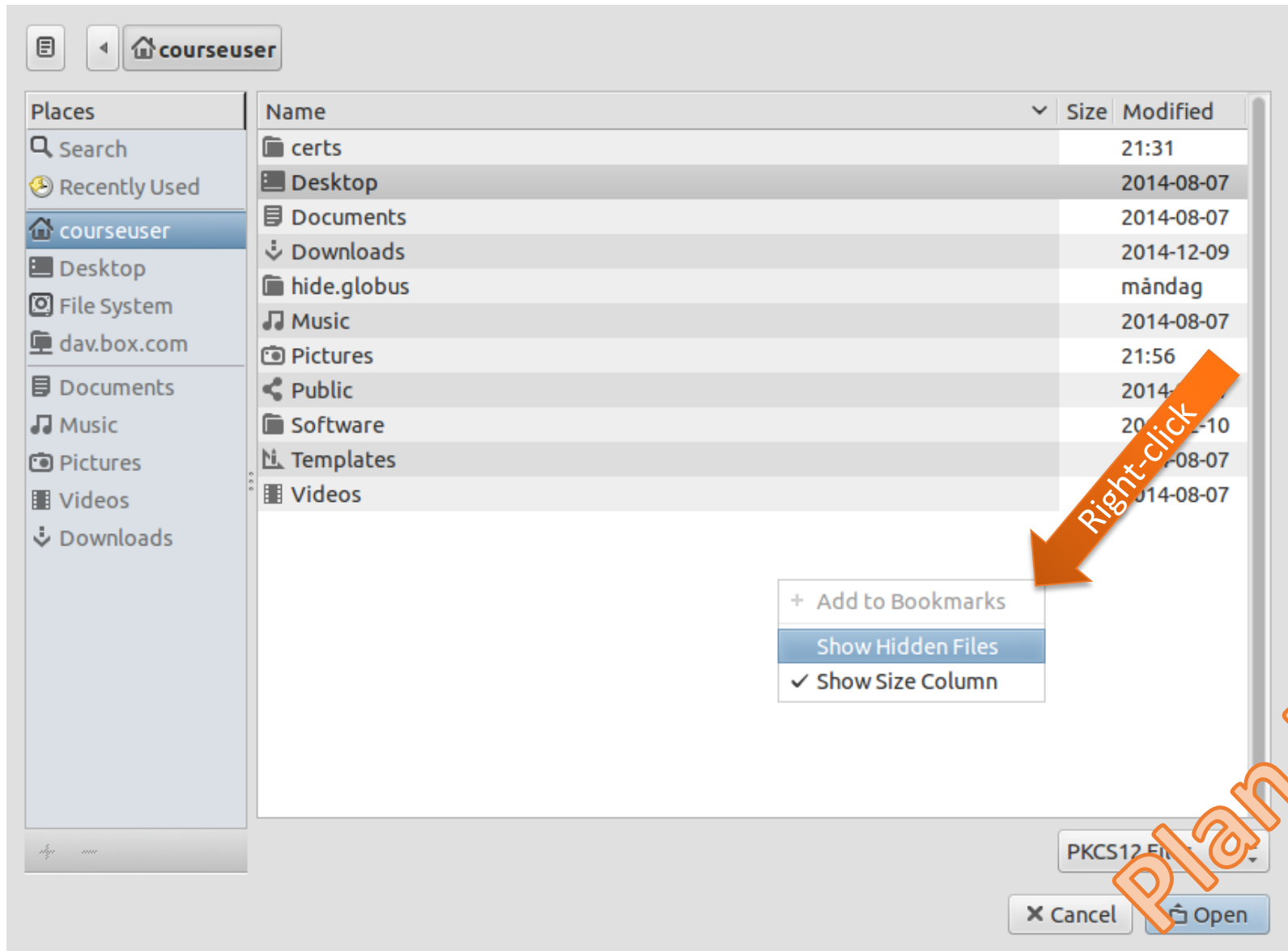


# In Your Certificates, find yours, and use Import to load one

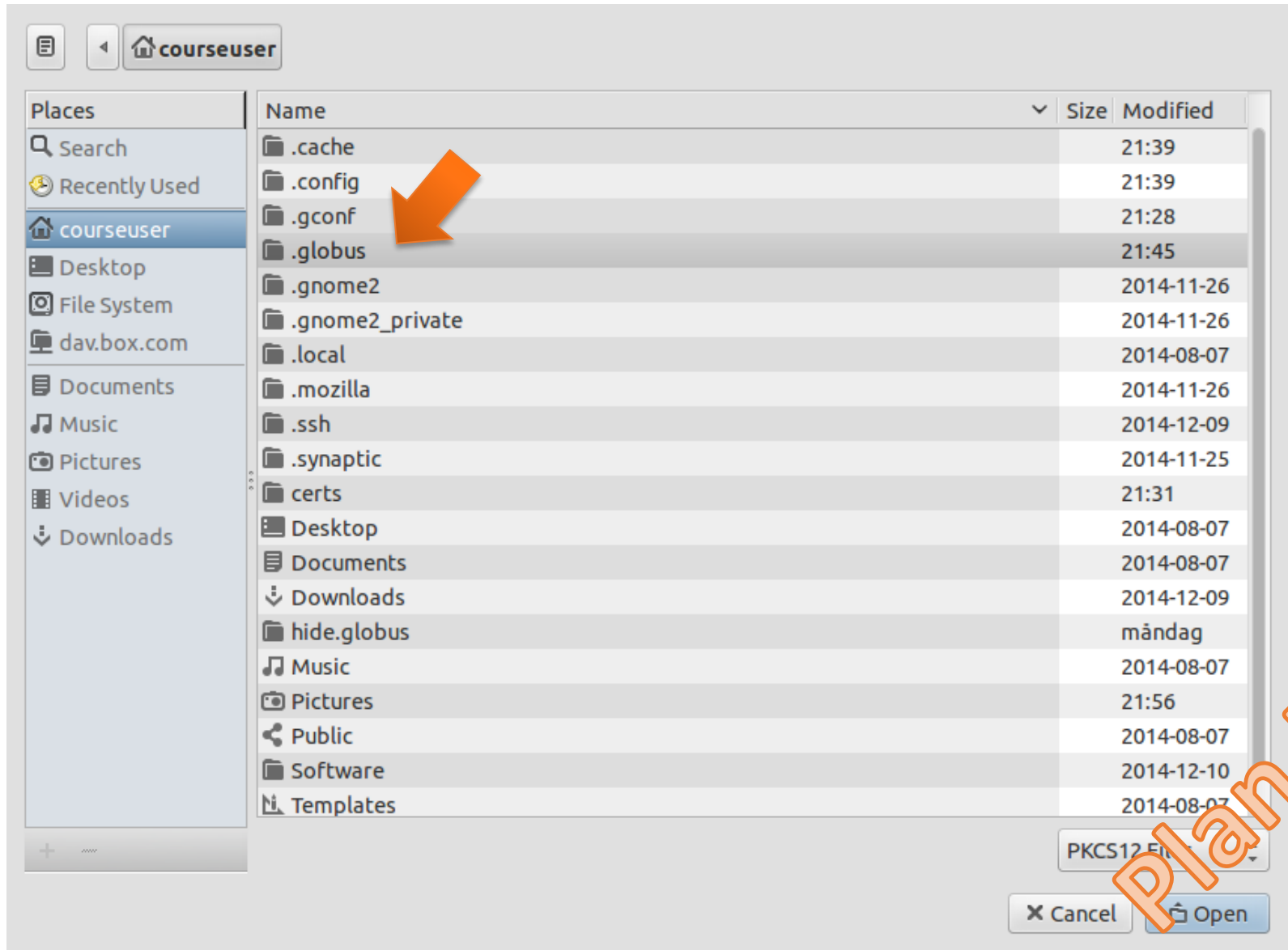


Plan B

# Make sure you can see hidden files: right-click and tick

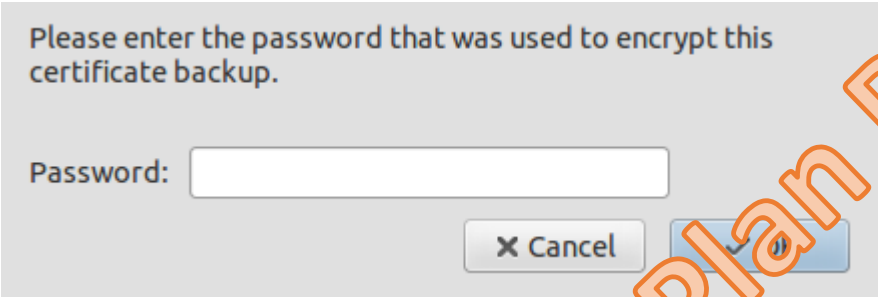


# Browse down to .globus



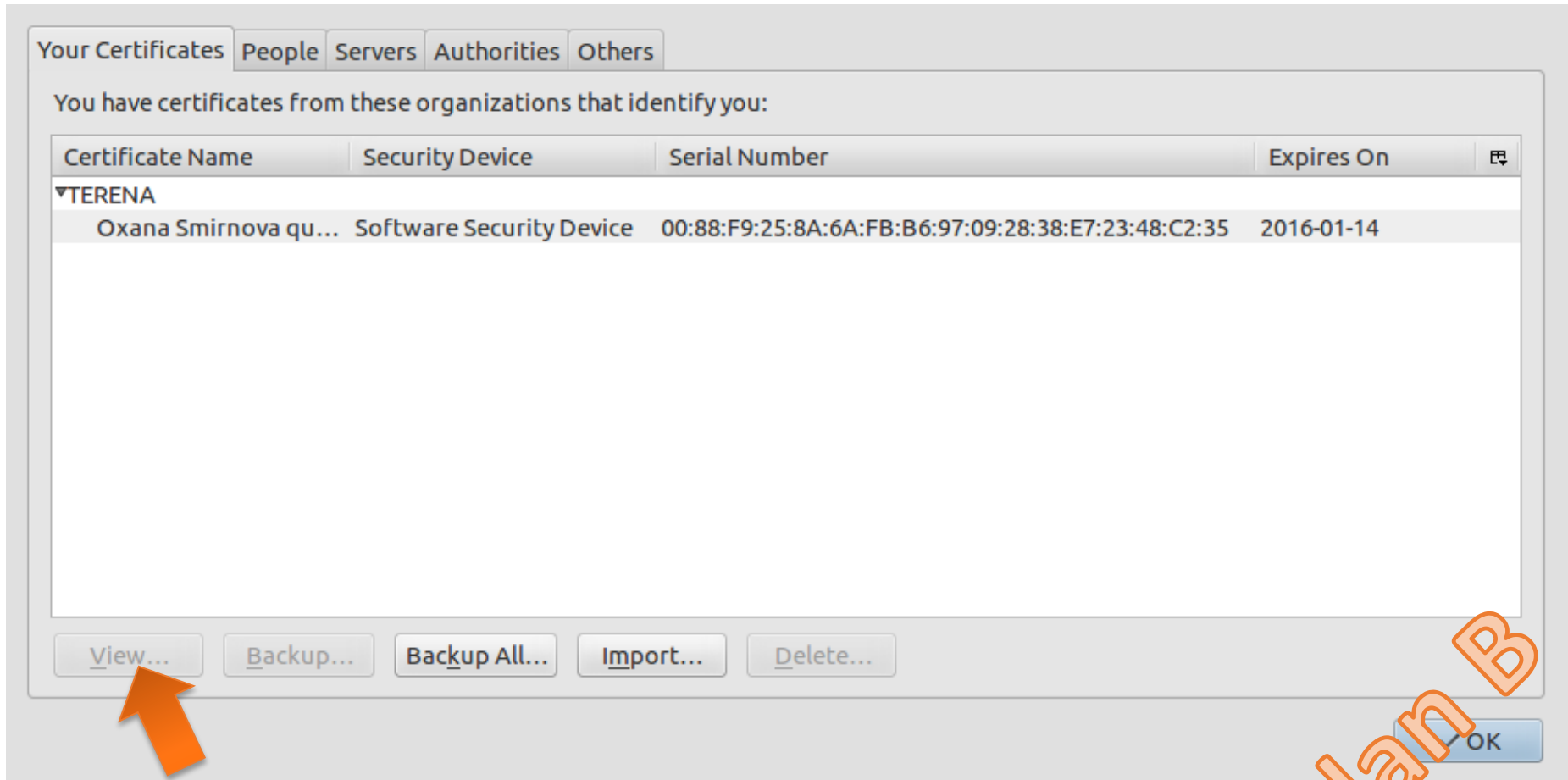


Select the .p12 file, use the password you used to create it



Plan B

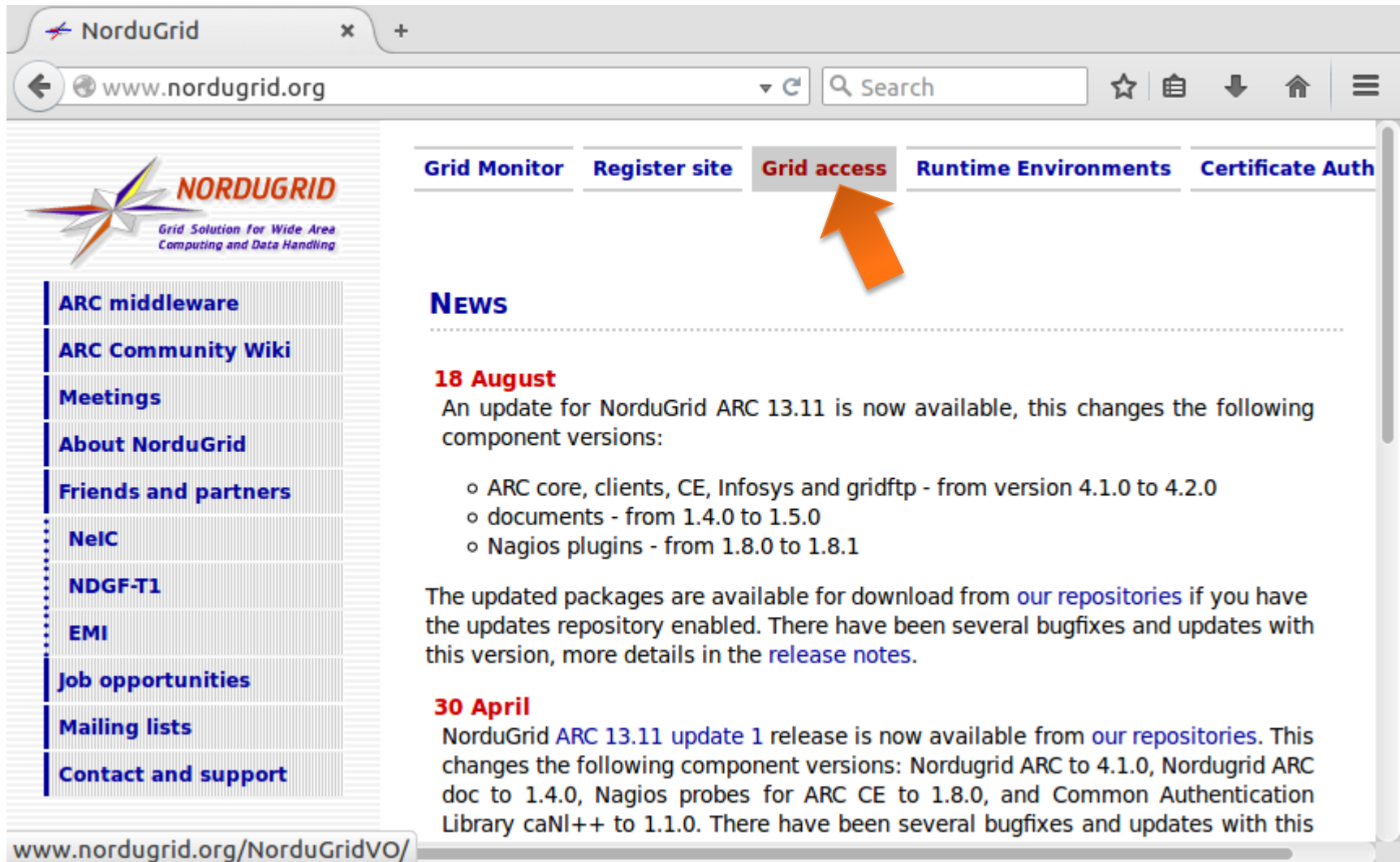
# You should now be able to view your certificate



Take some time to view the certificate content

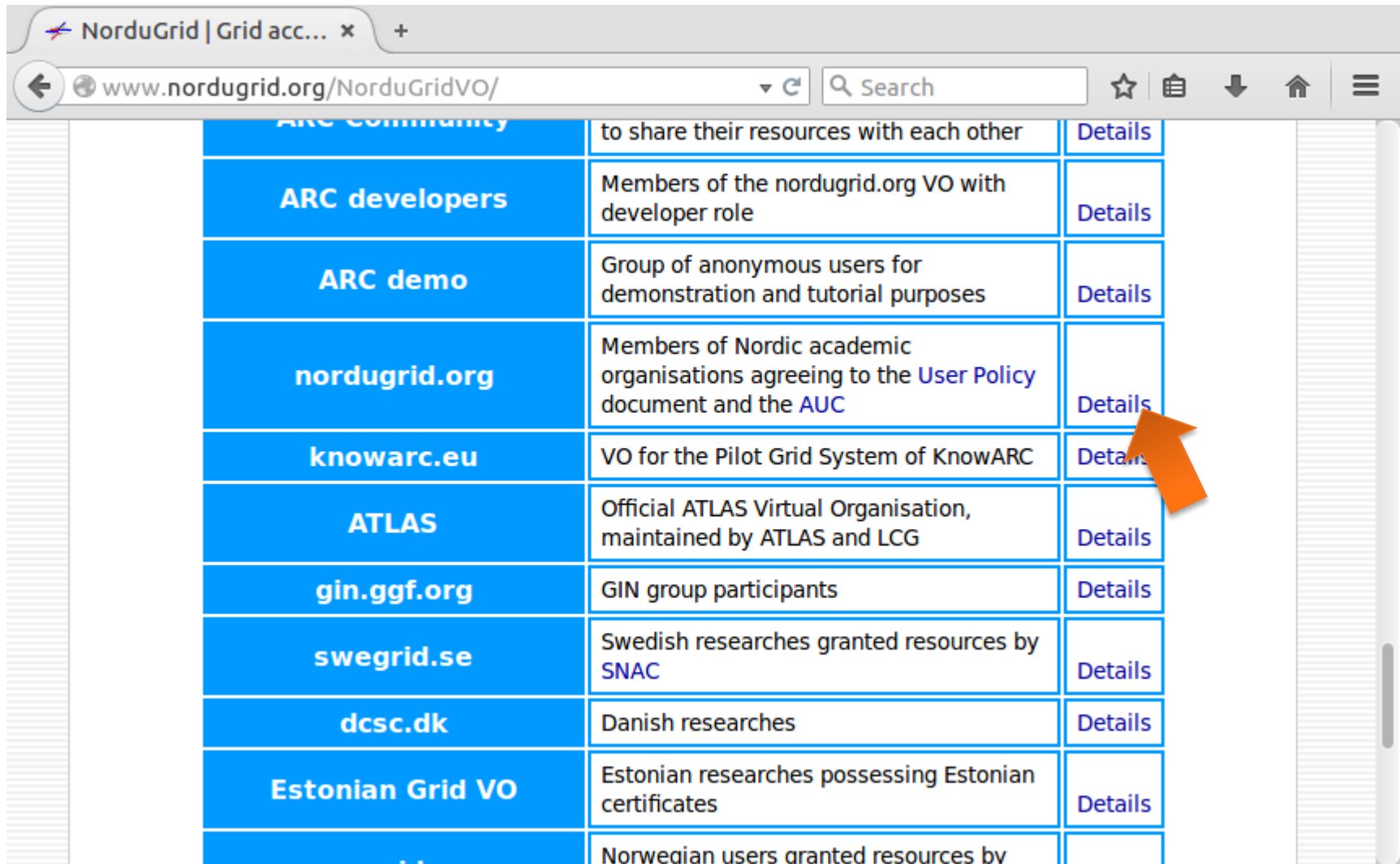
Plan B

# Step 3: Join a Virtual Organisation (Google for NorduGrid)



The screenshot shows a web browser window with the address bar displaying [www.nordugrid.org](http://www.nordugrid.org). The page features a navigation menu with the following items: [Grid Monitor](#), [Register site](#), [Grid access](#) (highlighted with an orange arrow), [Runtime Environments](#), and [Certificate Auth](#). On the left side, there is a sidebar with a logo and a list of links: [ARC middleware](#), [ARC Community Wiki](#), [Meetings](#), [About NorduGrid](#), [Friends and partners](#), [NeIC](#), [NDGF-T1](#), [EMI](#), [Job opportunities](#), [Mailing lists](#), and [Contact and support](#). The main content area is titled **NEWS** and contains two news items. The first item, dated **18 August**, announces an update for NorduGrid ARC 13.11 and lists the following component versions: ARC core, clients, CE, Infosys and gridftp (4.1.0 to 4.2.0), documents (1.4.0 to 1.5.0), and Nagios plugins (1.8.0 to 1.8.1). The second item, dated **30 April**, announces the NorduGrid ARC 13.11 update 1 release and lists the following component versions: Nordugrid ARC (4.1.0), Nordugrid ARC doc (1.4.0), Nagios probes for ARC CE (1.8.0), and Common Authentication Library caNI++ (1.1.0). The address bar at the bottom of the browser shows [www.nordugrid.org/NorduGridVO/](http://www.nordugrid.org/NorduGridVO/).

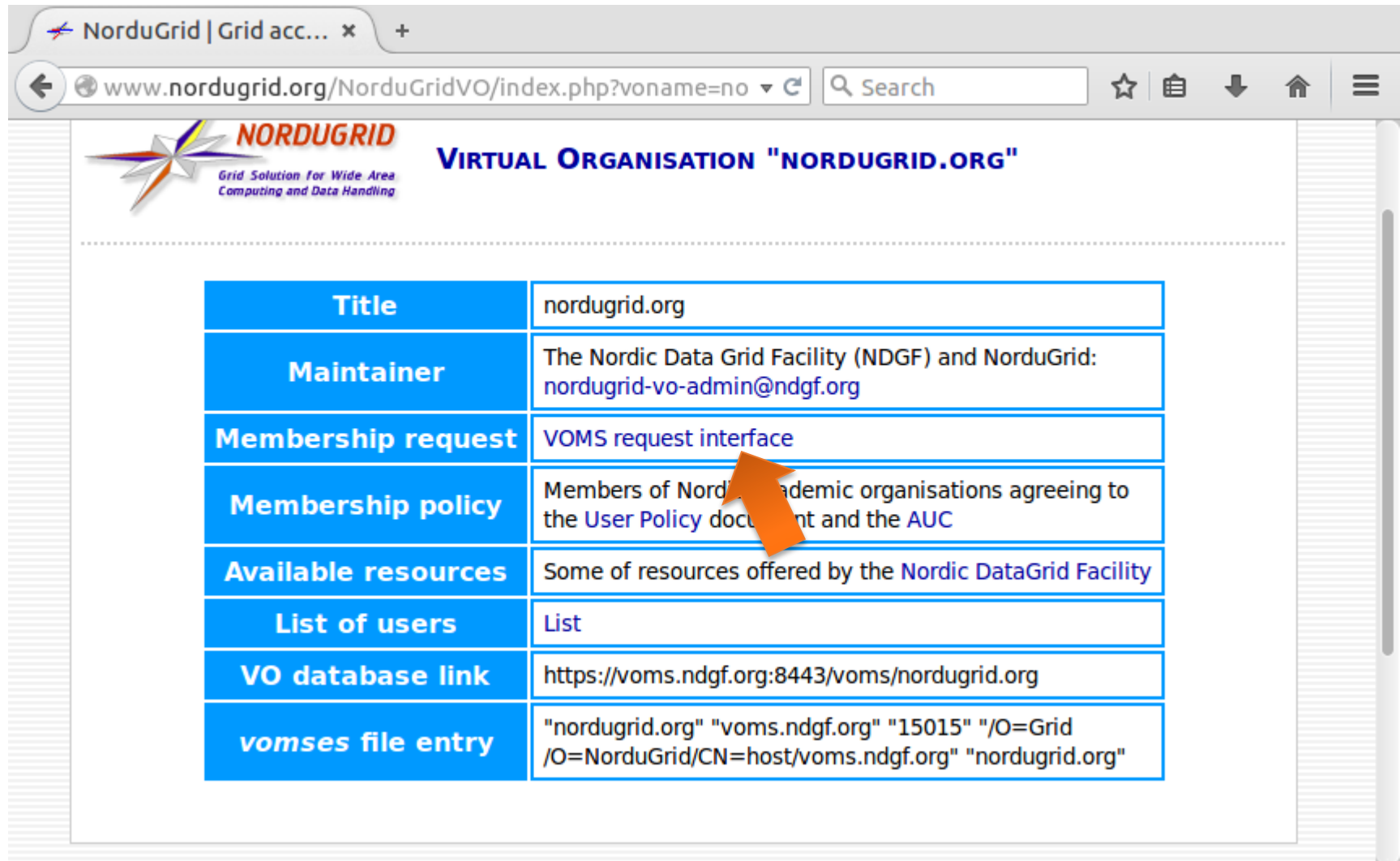
# Find nordugrid.org and click Details



The screenshot shows a web browser window with the address bar displaying `www.nordugrid.org/NorduGridVO/`. The page content is a table listing various Virtual Organizations (VOs) with their descriptions and links to their details.

ARC community	to share their resources with each other	<a href="#">Details</a>
<b>ARC developers</b>	Members of the nordugrid.org VO with developer role	<a href="#">Details</a>
<b>ARC demo</b>	Group of anonymous users for demonstration and tutorial purposes	<a href="#">Details</a>
<b>nordugrid.org</b>	Members of Nordic academic organisations agreeing to the <a href="#">User Policy</a> document and the <a href="#">AUC</a>	<a href="#">Details</a>
<b>knowarc.eu</b>	VO for the Pilot Grid System of KnowARC	<a href="#">Details</a>
<b>ATLAS</b>	Official ATLAS Virtual Organisation, maintained by ATLAS and LCG	<a href="#">Details</a>
<b>gin.ggf.org</b>	GIN group participants	<a href="#">Details</a>
<b>swegrid.se</b>	Swedish researches granted resources by SNAC	<a href="#">Details</a>
<b>dcsc.dk</b>	Danish researches	<a href="#">Details</a>
<b>Estonian Grid VO</b>	Estonian researches possessing Estonian certificates	<a href="#">Details</a>
	Norwegian users granted resources by	

# Click "VOMS request interface"



The screenshot shows a web browser window with the URL `www.nordugrid.org/NorduGridVO/index.php?voname=no`. The page header includes the NorduGrid logo and the text "VIRTUAL ORGANISATION 'NORDUGRID.ORG'". Below the header is a table with the following content:

Title	nordugrid.org
Maintainer	The Nordic Data Grid Facility (NDGF) and NorduGrid: nordugrid-vo-admin@ndgf.org
Membership request	<a href="#">VOMS request interface</a>
Membership policy	Members of Nordic academic organisations agreeing to the <a href="#">User Policy document</a> and the AUC
Available resources	Some of resources offered by the <a href="#">Nordic DataGrid Facility</a>
List of users	<a href="#">List</a>
VO database link	<a href="https://voms.ndgf.org:8443/voms/nordugrid.org">https://voms.ndgf.org:8443/voms/nordugrid.org</a>
vomses file entry	"nordugrid.org" "voms.ndgf.org" "15015" "/O=Grid /O=NorduGrid/CN=host/voms.ndgf.org" "nordugrid.org"

An orange arrow points to the "VOMS request interface" link in the "Membership request" row.

# The server requires your certificate:

**This site has requested that you identify yourself with a certificate:**  
host/voms.ndgf.org (:8443)  
Organization: "Grid"  
Issued Under: "Grid"


**Choose a certificate to present as identification:**

Oxana Smirnova quar-osm@lu.se's TERENA ID [00:88:F9:25:8A:6A:FB:B6:97:09:28:38:E7:23:48:C2:35] ▾

Details of selected certificate:

Issued to: CN=Oxana Smirnova quar-osm@lu.se,O=Lunds Universitet,C=SE,DC=tcs,DC=terena,DC=org  
Serial Number: 00:88:F9:25:8A:6A:FB:B6:97:09:28:38:E7:23:48:C2:35  
Valid from 2014-12-14 01:00:00 to 2016-01-14 00:59:59  
Certificate Key Usage: Signing,Key Encipherment  
Email: oxana.smirnova@hep.lu.se  
Issued by: CN=TERENA eScience Personal CA,O=TERENA,C=NL  
Stored in: Software Security Device

Remember this decision



# You have to establish trust with the server

Untrusted Connection x +

https://voms.ndgf.org:8443/voms/nordugrid.org

## This Connection is Untrusted

You have asked Firefox to connect securely to **voms.ndgf.org**. This connection is secure.

Normally, when you try to connect securely, sites will prove they are going to the right place. However, this site's identity is not trusted.

### What Should I Do?

If you usually connect to this site without problems, they may be impersonating the site, and you shouldn't continue.

Get me out of here!

- ▶ **Technical Details**
- ▼ **I Understand the Risks**

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error should mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

You are about to override how Firefox identifies this site.  
**Legitimate banks, stores, and other public sites will not ask you to do this.**

Server  
Location: https://voms.ndgf.org:8443/voms/r Get Certificate

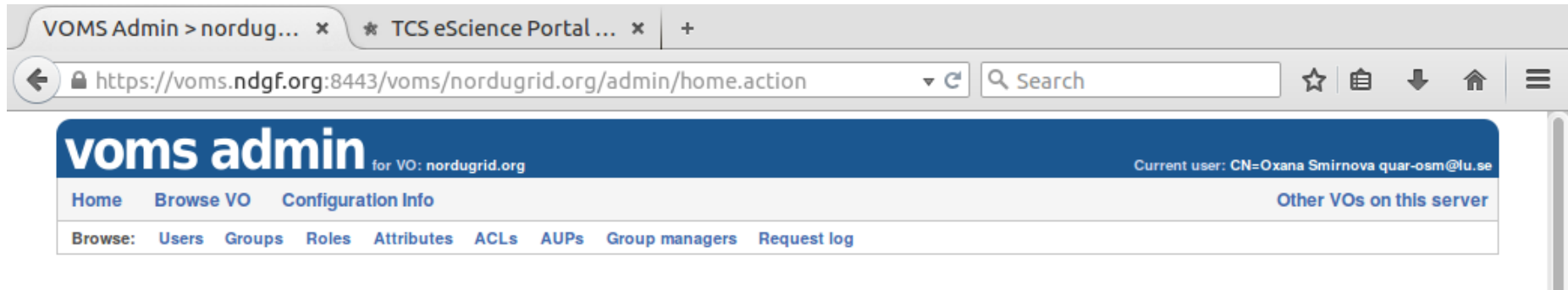
Certificate Status  
This site attempts to identify itself with invalid information. View...

Unknown Identity  
Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

Permanently store this exception

Confirm Security Exception Cancel

# Fill in your details and request VO membership



- Check your e-mail: VOMS will ask to confirm the request
  - Give teacher a moment to approve the request
- Ask the teacher if something is unclear
- What happens if your certificate is issued by a non-trusted CA?



# On to Grid: create a proxy!

```
File Edit Tabs Help
courseuser@Lubuntu-VirtualBox:~$ arcproxy
Enter pass phrase for private key:
Your identity: /DC=org/DC=terena/DC=tcs/C=SE/O=Lunds Universitet/CN=Oxana Smirnova quar-osm@lu.se
Proxy generation succeeded
Your proxy is valid until: 2014-12-15 12:32:44
courseuser@Lubuntu-VirtualBox:~$
```

- Simply type **arcproxy** and enter your Grid password (*PEM pass phrase* for the private key)

# What actually `arcproxy` does?

- A **new** private/public key pair is created for each proxy
  - When a proxy expires, a new one must be created to continue working
    - Default expiration time is 24 hours
- A proxy is then constructed of:
  1. Public certificate (with public key embedded)
    - Certificate contains modified owner's Distinguished Name (has "*proxy*" appended to the name)
      - Owner's DN:  
`/C=UK/O=Grid/OU=CenterA/L=LabX/CN=john doe`
      - Proxy DN:  
`/C=UK/O=Grid/OU=CenterA/L=LabX/CN=john doe/CN=proxy`
    - Certificate is signed by the proxy owner's **real** private key
    - Certificate contains validity period
  2. Private key
  3. Optionally, Attribute Certificates – extensions containing additional information

# The tale of two proxies

- A user always has to create a proxy certificate **P1**
  - Technically, it can be sent to the server, but it is a security breach
- Any Grid server (e.g. a Computing Element) creates itself a delegated proxy **P2** for each user request:
  1. Server generates a **new** private/public key pair (yes, that's a 3<sup>rd</sup> one...)
  2. Server returns the generated public key as a certificate request to the user
  3. User's tool signs that public key and inserts user information (DN etc), thus generating a public certificate. It uses the private key of proxy P1 for performing signing operation.
    - It can also use the actual private key, but that will require entering password every time!
  4. User's tool sends the signed public certificate back to the server
  5. Server adds generated private key to that certificate and creates a delegated proxy **P2**

# What's the use of VOMS

- A Grid user must become a member of a VO
  - VOMS is the most common VO management system
- A Grid cluster administrator gets the list of authorised users from the VOMS database
- VOMS can add extra VO information to your proxy, if necessary
  - For example, your VO role, group etc
  - You should use **arcproxy** with special command-line options to request such extra information to be added
    - We won't try it today

# Summary of the proxies

- Luckily, all authentication and delegation procedures are a part of the protocol, you only need to create a proxy
- You have to create a proxy before every Grid activity
- Proxies expire quickly!
  - Resist temptation to create long-living proxy: this will undermine your security
- Proxies may have special extensions, specific to Virtual Organisations
- If you forget your Grid password (PEM pass phrase), and even the browser Import Password, you will have to request a new certificate

# Workflow: Grid vs PC/cluster

## PC/cluster

Log in via SSH

- Different logins on different machines

Familiarize with the environment

- OS, installed software, storage space, batch system, sysadmin etc

Customize the environment

- Pathes, environment variables, own software, scripts, data files etc

Prepare for batch submission

- Interactive execution of short jobs, optimization of batch scripts

Submit jobs to the batch system, check their status

- Different batch systems (or none) on different machines

Log out

Log in later to fetch the output

## Grid

Create proxy

- One for all machines

Create a Grid job description document

- Generalization of batch scripts, plus input/output data location etc

Test a couple of jobs, fix job description

Submit jobs to the Grid, check their status

- Same commands for all machines

Watch output appearing in the desired location

- Or fetch it manually

# Simplest Grid job submission

- Your Grid client should:

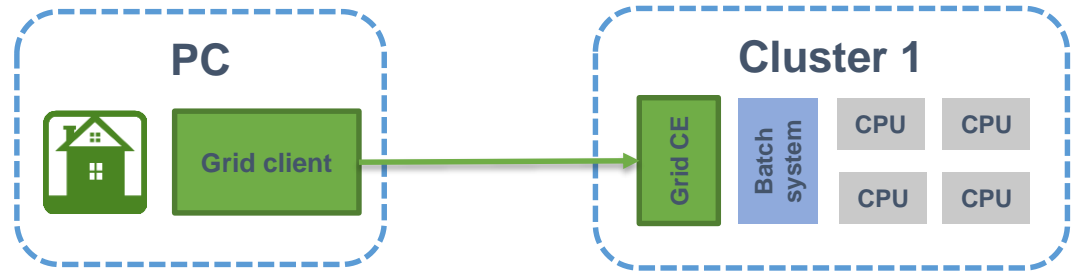
- Create a proxy:

- **arcproxy**

- Submit the job description document to the cluster:

- **arcsub -c arc-iridium.lunarc.lu.se hello\_grid.xrsl**

- **arcsub** will refuse submission if the cluster does not meet job requirements



See the *ARC Clients manual* for info about all ARC client commands:  
<http://www.nordugrid.org/documents/arc-ui.pdf>

- The CE on the cluster should:

- Check whether you are authorised
- Fetch input file (if requested)
- Convert job description to a batch script and start a batch job
- Upload output file (if requested)

# Simplest Grid job description: hello\_grid.xrsl

```
&( executable = "/bin/echo" )
  ( arguments = "hello grid" )
  ( stdout = "stdout_file" )
  ( stderr = "error_file" )
  ( cputime = "13" )
  ( gmlog = "grid_log" )
  ( jobname = "hello_grid" )
```

attribute

value

- Yes, this is yet another language:  
**XRSL – eXtended Resource Specification Language**
  - File extension is **.xrsl**
- XRSL is not a standard language, but no standard exists
  - There are many other Grid languages and meta-languages
  - XRSL is an ARC extension of the original Grid language by Globus
    - It was actually modelled on the LDAP database query language
    - Is a list of attribute-value pairs



# Main attributes of job description

Job attribute description	Attribute name (XRSL)	Example value
Main executable (binary or script)	<b>executable</b>	MyAnalysis.py
Arguments of the executable	<b>arguments</b>	-i input.dat -o output.dat
Input files	<b>inputfiles</b>	https://store.lu.se/physlab/2012/file1.dat
Output files	<b>outputfiles</b>	https://store.lu.se/physlab/2014/file1.dat
Standard input file	<b>stdin</b>	stdin.txt
Standard output file	<b>stdout</b>	stdout.txt
Standard error file	<b>stderr</b>	stderr.txt
Time (used by CPU)	<b>cputime</b>	1 hour
Memory (maximum needed, Mbytes)	<b>memory</b>	1000
Disk space (maximum needed, Mbytes)	<b>disk</b>	1000
Job name	<b>jobname</b>	My data analysis
Number of slots (cores) for the job	<b>count</b>	36

and many others: ARC job description language XRSL has 37 attributes, see <http://www.nordugrid.org/documents/xrsl.pdf>

# Create and submit your `hello_grid.xrsl`

- Prepare job description for the “Hello Grid” task:
  - Use Geany (or Vim, or Emacs) to create a file `hello_grid.xrsl`
  - Use at least the following XRSL attributes: `executable`, `arguments`, `jobname`
    - Hint: copy the example from the previous slide
- Submit your first Grid job to our Iridium cluster:
  - First, make sure you have a valid proxy:  
`arcproxy -I`
  - Use the `arcsub` command with explicit cluster selection:  
`arcsub -c arc-iridium.lunarc.lu.se hello_grid.xrsl`
  - Find the returned **job ID** (a long string that looks like a URL)
  - Check the job’s status:  
`arcstat <jobid>`
  - Check what the job “session directory” looks like on the cluster:  
`arcls <jobid>`
  - Check what does the job print out:  
`arccat <jobid>`

# Manipulate the jobs: kill, retrieve

- Submit a couple more jobs
  - You may want to change the job names in `hello_grid.xrsl`
  - Or you may even want to change what do the jobs produce
- Check the status of all your jobs:  
`arcstat -a`
- Terminate some of them and check the status afterwards:  
`arckill -k <jobid>`  
`arcstat <jobid>`
  - `-k` here means “keep the job files”, otherwise they will be wiped out
- Retrieve job results (download job output):  
`arcget -k <jobid>`
  - `-k` here has the same meaning as for `arckill`
- Find where the downloaded files are, and look what is there
  - Inspect the content of the `gmlog` sub-directory: it has files useful for error diagnostics and debugging

# If you have some time left

- Find the hidden directory `~/.arc` and file `client.conf` therein
- Open `client.conf` in Geany (or any other editor)
- Find blocks `[registry/index1]` , `[registry/index2]` etc and uncomment them and their content
  - Save `client.conf` and quit the editor
- Try to submit `hello_grid.xrsl` to the entire Grid

```
arcsub hello_grid.xrsl
```