Grid Security 101

Dennis van Dok

EGEE-III INFSO-RI-222667 Grid Tutorial 2008

Outline

Contents

1 Introduction **1**

2 Trust **3**

3 Obtain a certificate **8**

4 Loading the certificate in a browser **13**

5 Become a VO member **14**

6 Get to work **14**

7 One year later... **15**

1 Introduction

Security is not everybody's favourite topic. Yes, it's something you need, but most of the time it just gets in the way of what you are really trying to accomplish; yes, you know you've got to wear seatbelts but at best they're a mild nuisance.

What me worry?

Security is like wearing seatbelts. Most of the time they're a mild nuisance...

All in all, security is something we don't want to spent a whole lot of time thinking about.

When it comes to seatbelts, we're really happy to find they worked when they really had to. And when it comes to grids, there's plenty of people who take the security of their data—and yours—really serious.

What me worry II

Computer networks need security too!

- computer break-in
- privacy or confidentiality breach
- identity theft
- botnets
- credit card fraud
- child porn

There's plenty of problems to go around, even with all the usual safety measures in place.

When it comes to computer security, we have to deal with a number of words all starting with the letter A.

The A'spects of computer security

Brought to you by the letter A:

- **Authentication**
- Authorization
- Accounting

- Auditing

Your first and foremost worry is *authentication*

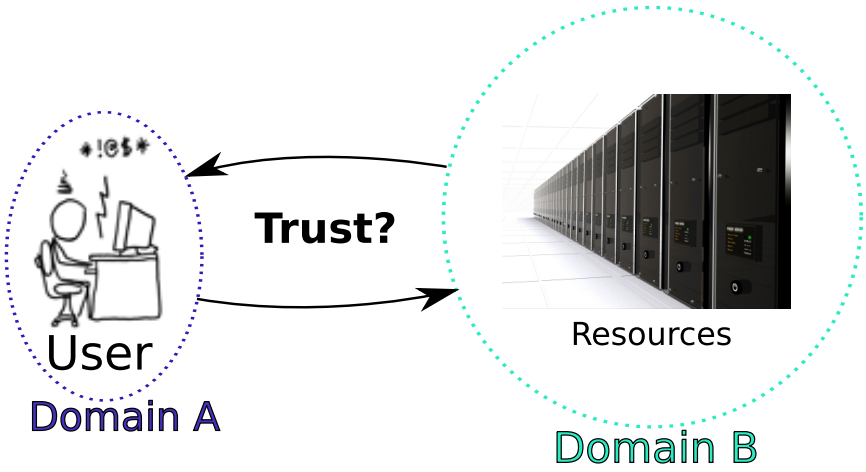
But today, we'll focus just on the first one: authentication. That means: proving that you are who you claim you are.

This may not sound so hard; a username and password is all that it takes after all to link your identity (you username) to a secret phrase that only you know.

2 Trust

But there's the rub. Grids are inherently going across multiple administrative domains. There is no central entity that administers all the users and machines. That would mean that you, or your home institute, will have to establish a trust relationship with every resource provider out there.

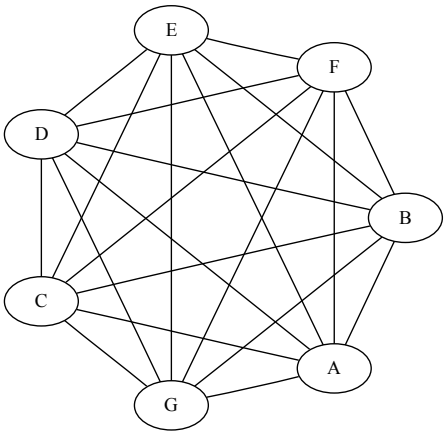
Knowing who to trust



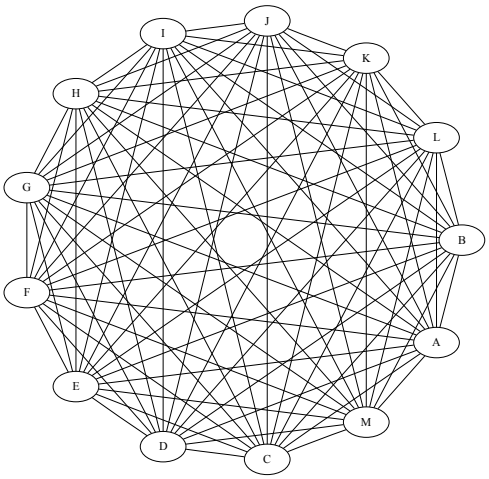
How many trust relationships will that yield, world wide?

Number of trust relations

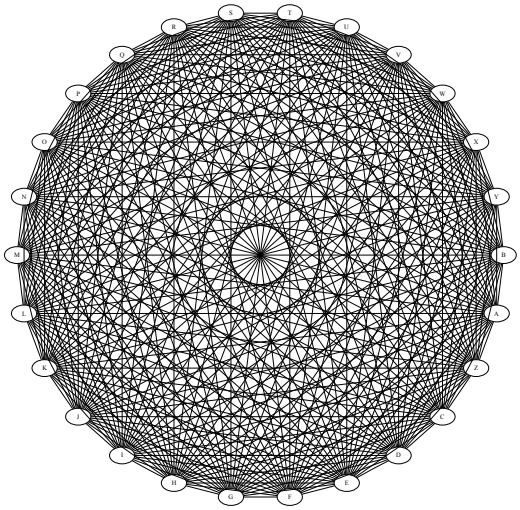
#domains = 7



#domains = 13



#domains = 26



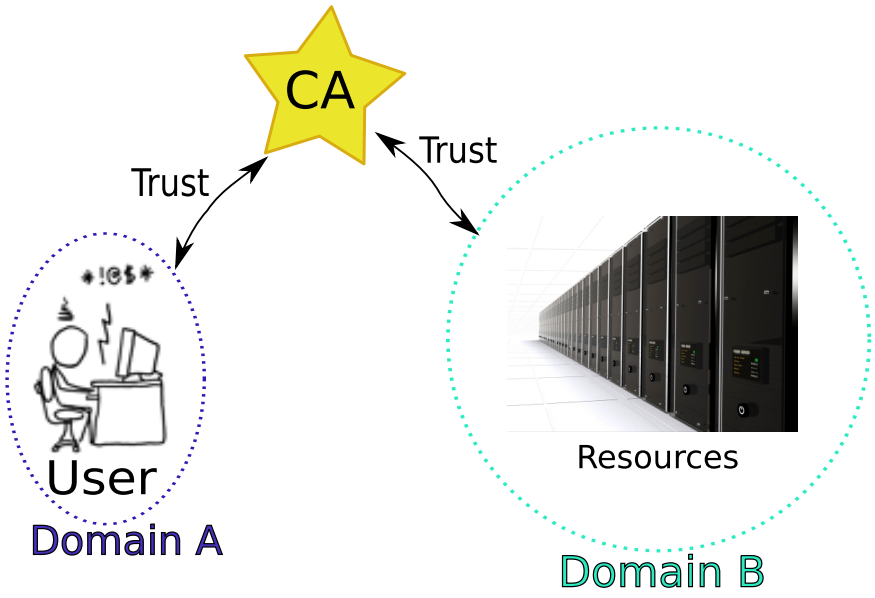
The way the clever grid folks have solved this is by employing the same technique that your on-line casino—oops, your on-line bank uses, or e-commerce sites like Amazon or Ebay: digital certificates.

A digital certificate is like a passport. The holder of the certificate can prove his identity because of the trust we place in the government that issued that official document. Likewise, a certificate is signed by an authority that we all implicitly trust to be careful when handing out certificates.

Digital Certificates

Mind you, the trust only goes as far as the veracity of the identity, it doesn't mean that a certificate holder is particularly trustworthy. You know, like banks. Likewise even the owner of a passport may be a thief.

Knowing who to trust



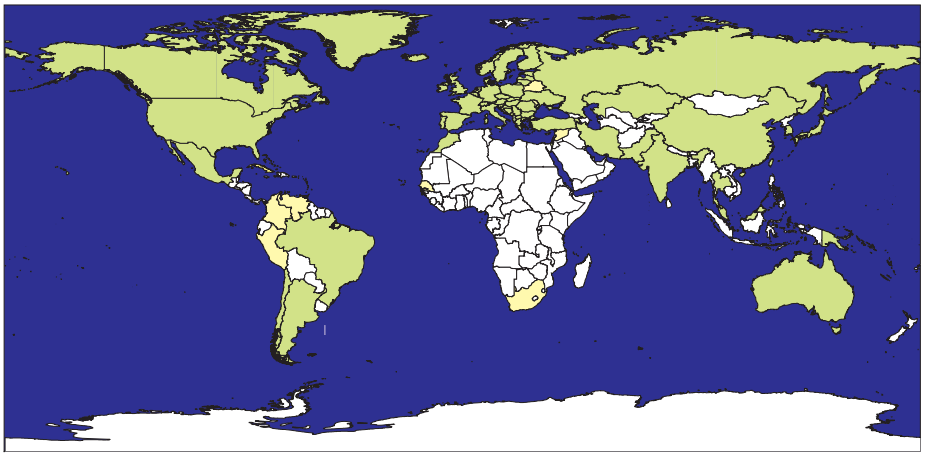
The certificate authority is a trusted third party, and certificate holders, users and resources alike, establish their trust through that. They only need to check eachothers certificates.

If you open your web browser's preferences, and look for certificates, you'll find a list of CAs that we all apparently trust. You can obtain a certificate from them, usually for money.

For the grid, there is a collective of CAs that work together called the IGTF. They have regular meetings and talk about policies, which is terrifyingly exciting. And they issue *grid certificates*, which I will explain in a moment.

Trusted third parties

- All research grid infrastructures share the same base set of trusted third parties ('CAs')
- There is typically one in each country
- The credentials they issue are comparable in quality

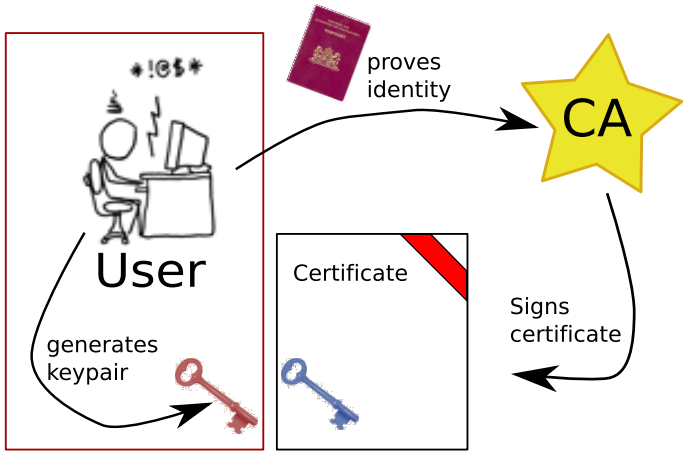


But thanks to the grid-wide trust in them, you can obtain a certificate to use anywhere on the grid, which I will now show you.

3 Obtain a certificate

A digital certificate comes in two parts: the *public* part that explains who the certificate holder is, how long it is valid, and who signed it. This part is what everybody can read. The *private* part is only known by the certificate holder, and the two parts are linked because they contain the cryptographic counterparts: a public/private keypair. Only the holder of the private key can answer challenges that are based on the public key.

How to obtain a certificate



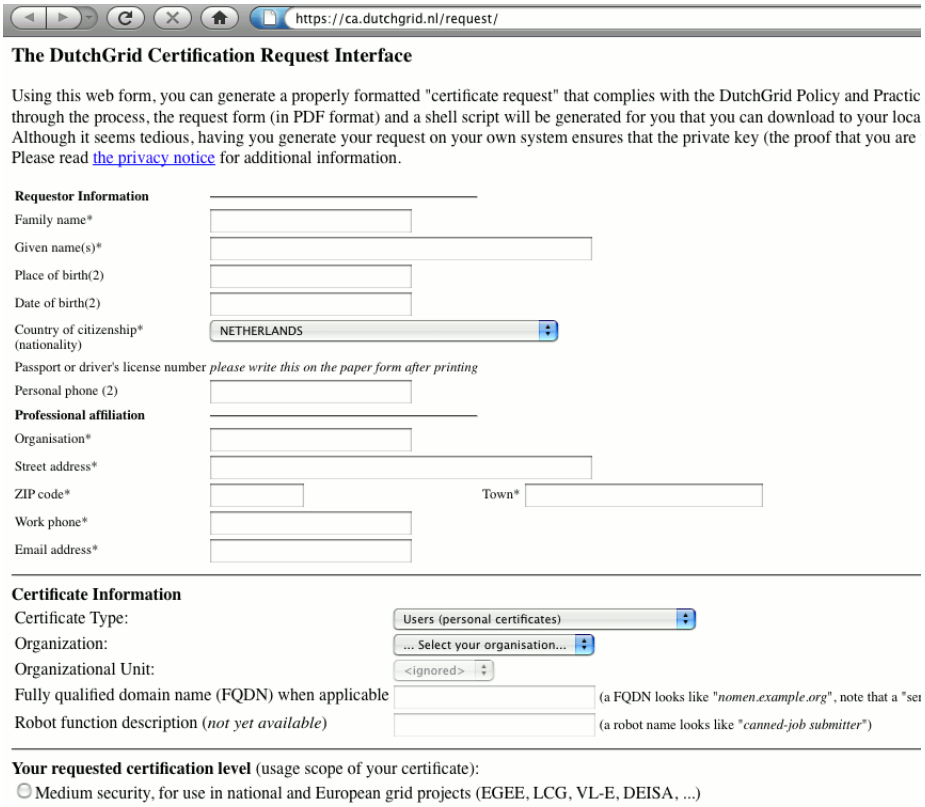
This picture shows some of the essential details. The user generated a public and private keypair, and carefully keeps the private key to himself. The public key will end up embedded in the certificate, and the signature of the CA will make it official.

The user will of course have to prove to the CA what his true identity is.

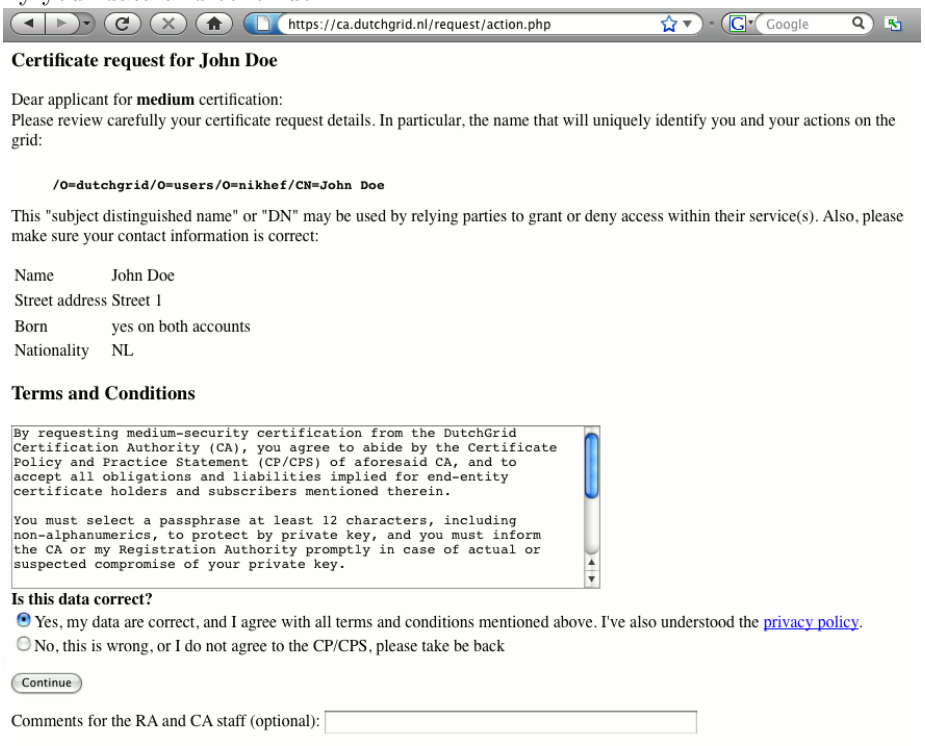
But what do you *really* have to do? Here's a step-by-step breakdown.

Request a certificate

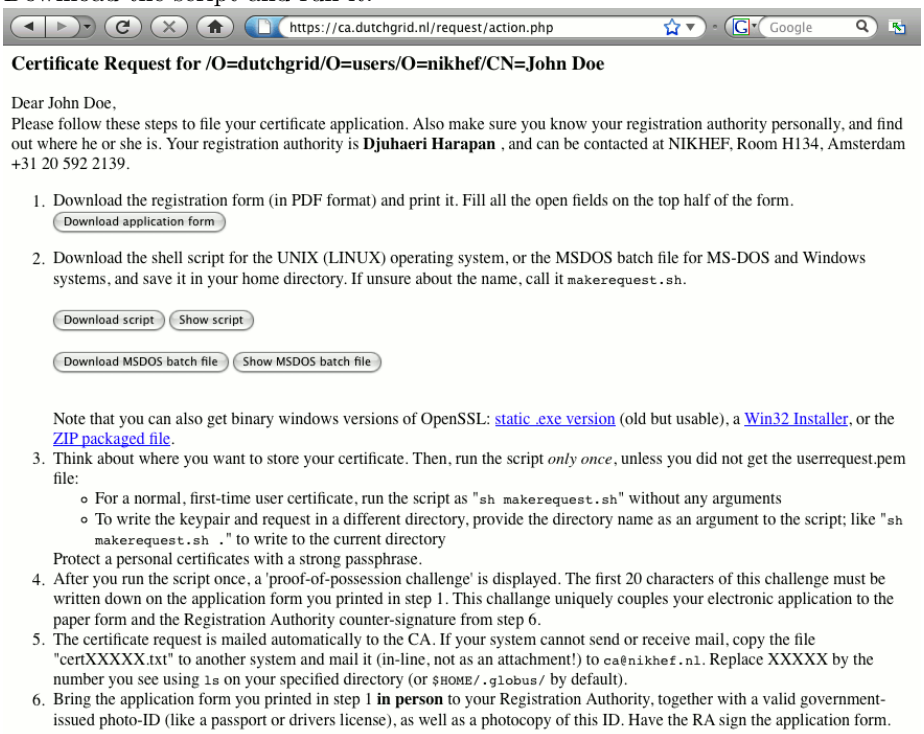
Go to `https://ca.dutchgrid.nl/` and fill out the entire form.



Verify your data and continue



Download the application form (PDF) and print it.
Download the script and run it!



You must choose your home institute here, as you can see this ends up being a part of your certificate. The application form has some fields filled in already, the rest you have to do by hand.

Running the script should generate

- a new keypair, which will require a 'secret passphrase'.
- a new certificate request
- a printout of the key's modulus, which you'll need to transcribe to the paper form.

Running the script

```
sh makerequest.sh
Generating a 1024 bit RSA private key
...++++++
...........++++++
writing new private key to './userkey.pem'
Enter PEM pass phrase: *****
Verifying - Enter PEM pass phrase: *****
-----
Mailing [CA:medium] certificate request to the DutchGrid CA
Please preserve your private key, named ./userkey.pem
This file is needed alongside with the public key you submitted to
the certification authority.
```

```
In the authentication process by the CA, you may be asked to
provide a proof-of-possession of the keypair you submitted. This
may involve you providing part of your public keydata displayed
below:

B811761282B5AC7FCC59DE7B4381B879DD02FB6280A20DB2B42F3EC4AEDF36A24E0A1D7388D58EDB
2074484DF7B407B77A1C30FF825C15C3A7DFD659F72815DD90AC59067A85D23F52005C05C3DD24F7
E1BB4FAD134B8FDB1A1F064AE29DB38169A03ACF1E0C99E6DE0F88CE1DCE87D5836F157194FFA193
EDE5EBCB260FD40D

*** Fill in the registration form now, and go to your RA.
```

The script leaves a number of files:

`-rw-r--r-- userrequest.pem`	generated request
`-rw-r--r-- certreq10915.txt`	the same, plus extra info
`-r-------- userkey.pem`	*this is your secret key!*
`-rw-r--r-- certreq10915.cnf`	harmless/useless

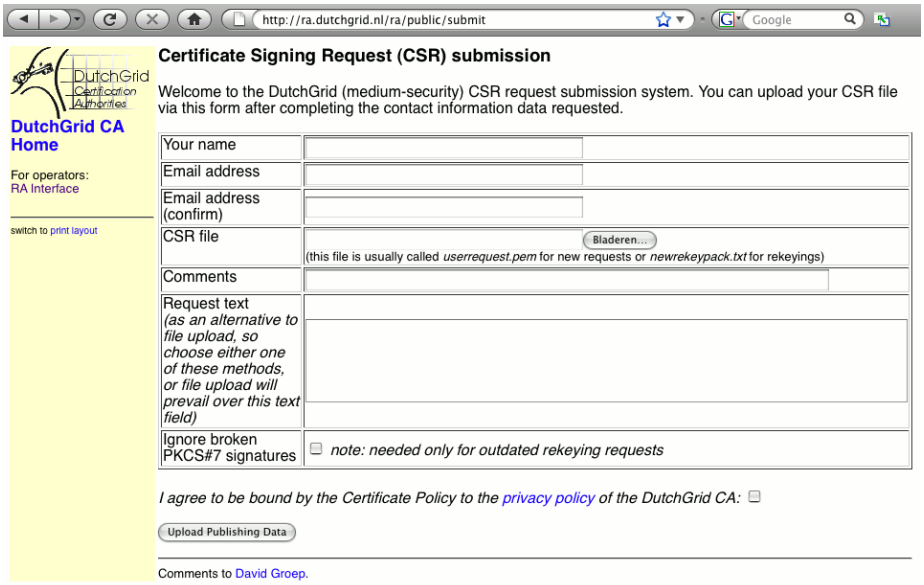
The script will ask you for a passphrase. This is very important, so choose carefully! It must be something that is hard to guess, but easy for you to remember. This will protect the private key, just in case it gets stolen.

At the end of the run the script will print out a lot of garbage; this is the key's modulus. By transcribing the first twenty characters or so of this stuff to the paper form, you prove that you are the owner of the private key.

Sign the paper form and take it to an RA for verification. Now I should explain what an RA is. The Registration Authorities are just the henchman of the CA in this evil pyramid scheme. The RA will check your identity and sign your form as well. You must then send it to the CA. A photocopy of your ID card is normally required for cross-checking, but not today.

Upload the request

- If the mail fails, upload the request to `http://ra.dutchgrid.nl/ra/public/submit`.
- Paste the text from certreqXXXXX.txt



If all is well, you should receive your certificate in a couple of work days. Save this file along with your private key. If you do this today, you receive your certificate tomorrow!

Those of you who are going to generate a request today are advised to put all the files on the memory stick and leave nothing lying around on the computers; of course. if you brought your own laptop you can put it there.

4 Loading the certificate in a browser

One of the essential steps is to load your certificate, private key and all, into your browser. But don't do that with a browser you dan't fully trust. What I mean by that is: a browser that other users have access to, such as a shared computer account, a borrowed laptop, an internet café, etc. Make sure this browser is yours, and yours alone!

Load certificate in browser

Convert your certificate to PKCS#12 format:

```
openssl pkcs12 -export \
-in ~/.globus/usercert.pem \
-inkey ~/.globus/userkey.pem \
-out user.p12 \
-name 'Joe Smith'
```

Use the "certificate store" of your browser

- Windows: double-click on the .p12 file
- Explorer: Internet Options-tab: Content
- Firefox: Preferences → advanced → encryption → certificates → import

To load into your browser, you have to convert the certificate and private key in yet another format called PKCS#12, by using the right openssl mantra. After that, it depends on your browser how to import this file.

5 Become a VO member

With your certificate neatly embedded in Firefox or whatever you can now apply for the good stuff: membership of a virtual organisation. What you should realize is that although we base our trust in you on your affiliation with your home institute, the grid resources like computing and storage are allotted to organisations based on their scientific application area. Since these projects often involve people from multiple institutes, we call them virtual organisations or VOs.

Many of the VOs for the Dutch projects are managed through the VOMS instance at Sara, so point your browser at http://voms.grid.sara.nl:8443/vomses and apply for membership of one of the VOs there.

Apply for VO membership

Go to `https://voms.grid.sara.nl:8443/vomses` and pick your favourite VO!

(Is it in this list?)

`astron astrop dans emutd esr lofar lsgrid magic ncf omegac phicos pvier tutor vldbi vledut vlefi vlemed vlibu scia`

6 Get to work

Now you want to get to work, but hang on a second there. You can now make yourself known on the grid, and prove your identity to anyone out there, but are you willing to sit out the entire 8-hour work plan you are about to submit? Because every time your job needs to access files, or talk to other grid apparati, you need to prove your identity again. Can you see the frustration already on the face of the hapless grid user? What? I just told you who I was, how could you have forgotten so quickly?

There is no way to 'log on' to the grid. As your job is hopping from system to system, it may cross several domain boundaries along the way.

So you think, I'll just pass along my entire certificate, private key and all. But that is a completely bad idea. Anybody getting a hold of your private key is going to be you.

Create a proxy

A VOMS proxy...

- is a 'delegate' of your *real* certificate
- is created by `voms-proxy-init -voms` ⟨*vo-name*⟩
- has no passphrase
- proves your vo membership

- is automatically used by the grid tools
- has a lifetime of 12 hours. Hurry up!

Other useful commands:

- `voms-proxy-info -all`
- `voms-proxy-destroy`

To limit the problem somewhat we've come up with an ugly hack called the grid proxy. This is yet another certificate file, only this time signed by yourself (this is called delegation, by the way), and only valid for 12 hours. It is regarded safe to pass the proxy along, as any problem is going to expire in 12 hours anyway.

What you also need are some signed attributes from the VOMS server, as these are not part of you original certificate. Compare your certificate with a passport, and the attributes with visa.

So you should call voms-proxy-init with the proper -voms line to get on the way. This would be the time to use that magic 'ol passphrase again!

You can always request the state of your proxy by typing voms-proxy-info. Once your done with your work you may call voms-proxy-destroy. But you cannot revoke remote proxies; they should have a limited lifetime anyway.

7 One year later...

By the time you really are picking up steam on the grid, you get a nasty mail in your inbox explaining that the grid certificate you once so strenuously struggled to obtain is about to expire. Oh dear, not that again. Fortunately, you don't have to do it all over again: since you already have a working certificate, it is now possible to base the new request on the existing certificate. This will forego a number of steps, especially the paperwork, although we will contact the RA to check whether you're still with the organisation that's part of your identity.

Renew your certificate

- Your certificate has a validity of 12 months, then you will have to renew
  - you get an email warning 4 weeks in advance
  - download the script from the web site (`http://ca.dutchgrid.nl/rekey`)
  - run it on a Unix system with OpenSSL installed.
- The script generates a *signed email message*
  - send the signed message to `ca@dutchgrid.nl`
  - do not modify the message in any way, preferably use `sendmail -t < newrequest.txt` as the script tells you at the end
  - your Registration Authority will be contacted for confirmation
  - after response from the RA, a new certificate is mailed to you

- When you get the new certificate, remember to also put the newkey.pem file in the proper place!

So download and run the renewal script, it will generate a new key. You have to go through some of the later steps anyway: loading the new certificate in your browser. But you don't need to register again with your VO.

The only tricky part here is to replace the old key and certificate with the new ones, without getting them mixed up. The best thing is to rename the old key first, then the old certificate, then to move the new key in place and finally to download or save the new certificate.

Thanks for your attention...

...You've been a wonderfull audience.