Simplifying grid certificates
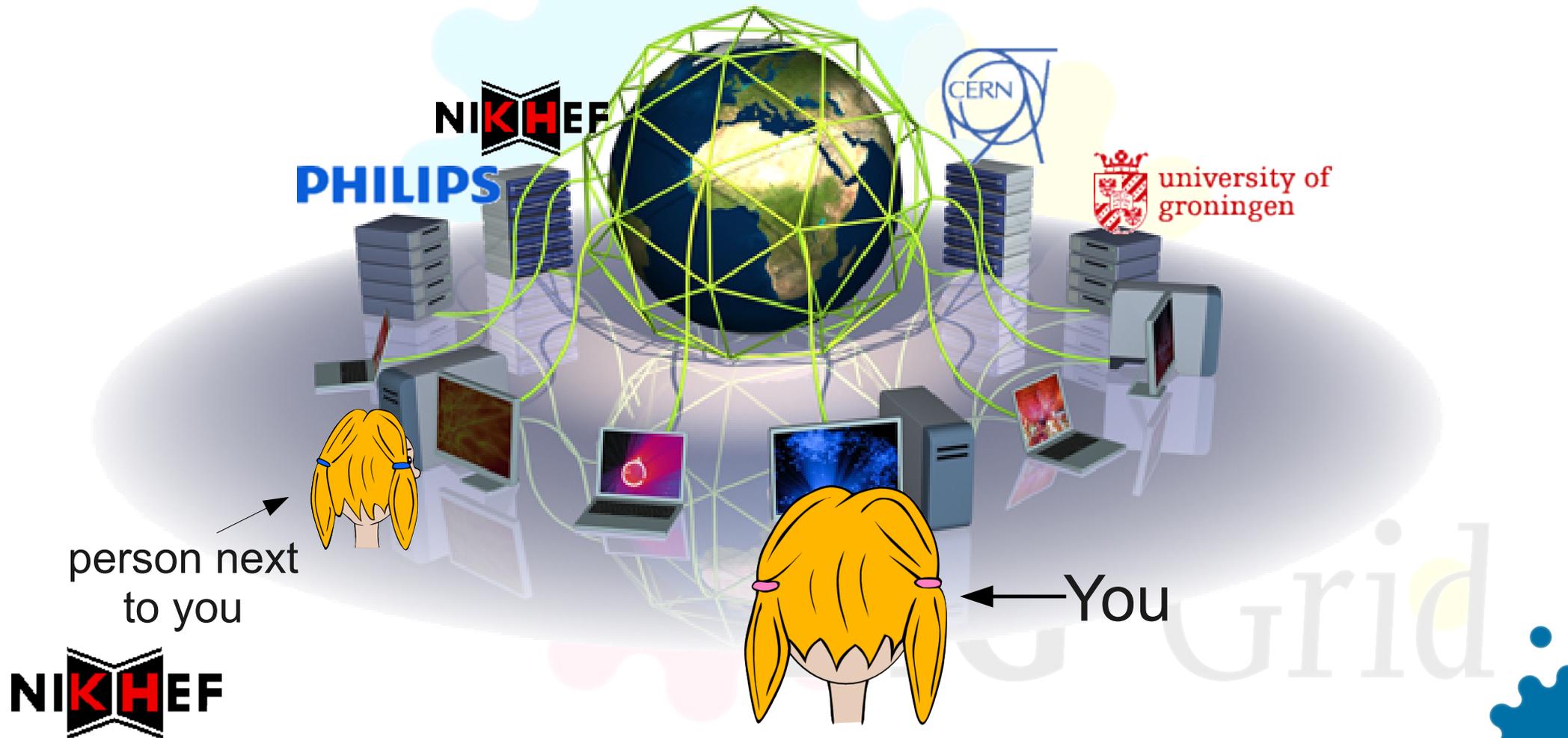
jGridstart
and
beyond

Willem van Engen, Nikhef, Jamboree 16th of December, 2009

NIKHEF

BiG Grid

Grid certificates

* The grid needs to know who you are

Grid certificates

* **The grid needs to know who you are**

  * Public *certificate*   and   private *key*

Keyholder is indeed
Jan Klaassen

Dutch Grid

(your secret!)

-----BEGIN CERTIFICATE-----
MZIEdyCCA12gAwIBAgICCmcVDQYJKoZxXxcNAQEFBQAwUjELMAkGA1USBxMCTkwx
DzANBgN6BFoABk5JS0hFRjSDMDAGA1UEAxM6TklLS8VGIG1lZGl1bS1zZWNQWml0
eSBjZXJJGa1Zbv2F0aW9uIGF1dGGgwWhcNMDkwbvIxMDAwMDAwWhcNMTAwOTIxMTQy
NjM4WjBQMRmwzAYDVQQdDzgkdXRjaGdyaWQxDjAMBgNVBAoMBXVzZXZXJzMQ$zDQYD
VQQKDAZuaWtoZWYxGTAXBgNVBAMMEFdpbGxlSB2YW4grRW5nZW4wgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMI/JAoGBAKFfKdXC2ybdKoSwWZeqWE+5dHFGUfqwe#8sI5XR
iXgByN96nA82/xx6DYW/QTl4qUcHAYCx+7jFK7sOSD80axbOZYoDeMmgj6cPyHaC
1L74tiouHD/AaltUKF/HQIijSnDki0dm3mWkO2GQlWHffa7S5c+lwcwB8rjtT2ry
...

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,26c639f0a01b0186

1DEdWeCQldFVZCsSAsBqC2+Tbo2DzQB0/4nFGDvka8GTysL7qU66rFpwyq94qZJb
ODp7iG5ZxVAV/43Z2dUGYvkciO37/6dArm3b0e/CruvgD9upeC4A4OsUraoK4hMB
n/fs+yTN72N9NPkGqGa571u6ToM+XEI8pp5L2zGhjUZxBFZ2iDh2t3GvcFYSDugA
bM9OueRhhOnN57N7pnKsiEXoiU1Zw30/mSmIzaxHvWBIvEb5bXiJC/9asXJzGU8F
xcMQDJGT35ELidAvwSWF7qrcHNvEFPe8gEqAN0o3uhoaieNkuCNAP80aiWnB3DjY
...

NIKHEF

Yesterday: web, scripts & openssl

User Registration - Mozilla Firefox

File Edit View History Delicious Tools Help

dutchgrid.nl https://ca.dutchgrid.nl/request/

User Registration

The DutchGrid Certific...

Using this web form, you can... (CP/CPS). When you have succe... you can download to your loc... Although it seems tedious, ha... claim to be) is kept confident...

Requestor Information

Family name*

Given name(s)*

Place of birth(2)

Date of birth(2)

Country of citizenship* (nationality)

Passport or driver's license number

Personal phone (2)

Professional affiliation

Organisation*

Street address*

ZIP code*

Work phone*

Email address*

Certificate Information

Certificate Type:

Organization:

Organizational Unit:

Fully qualified domain name applicable

Robot function description (...

Your requested certificatio...
- ⦿ Medium security, for use i...
- ○ Demo certification, for stu...

[Request certification]

(*) This is a required field

```
$ sh makerequest.sh
Generating user request and private key in /user/jk/.globus
Do NOT delete the private key in this directory
NOTICE: you are about to create the cryptographic k
        in your certificate. The private key is hig
        information! Do not share it with anyone an
        by mail to the Certification Authority
        Your private key is stored in a file named

Generating a 1024 bit RSA private key
........++++++
.................++++++
writing new private key to '/user/jk/.globus/userke
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Mailing [CA:medium] certificate request to the Dutc

WARNING: the certificate request and your private k
         were NOT created in your /user/wvengen/.gl
         IF you want to use them with the Globus to
         EDG middleware, you MUST place these files
         yourself (including the signed certificate
         be sent to you by the CA

Please preserve your private key, named /user/jk/.g
This file is needed alongside with the public key y
the certification author
In the authentication pr
provide a proof-of-posse
may involve you providing
below:

DB0794988C190639DA58D2EF
7C99B262BF34D88064D2ABE7
11874E26200CD629ACBC13F8

*** Fill in the registra
```

```
$ cd ~/.globus
$ openssl pkcs12 -export -in usercert.pem -inkey userkey.pem \
    -out your-new-packed-cert.p12
Enter pass phrase for userkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
$ chmod 0600 your-new-packed-cert.p12
```

Mozilla Firefox

File Edit View History Delicious Tools Help — Search Bookmarks

Firefox Preferences

Main | Tabs | Content | Applications | Privacy | Security | Advanced

General | Network | Update | Encryption

Protocols
- ☑ Use SSL 3.0
- ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:
- ○ Select one au...

[View Certificate]

🛈 Help

DutchGrid Cer...

Reserved for CA op...

/O=dutc...   ...nik...

□

wait up to 3 days

PASPOORT

G...
Ja...

Place...   Date of birth

Certificate Manager

Your Certificates | People | Servers | Authorities | Others

You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
▷ NIKHEF			

[View...] [Backup...] [Backup All...] [**Import...**] [Delete...]

Today: jGridstart

Today: jGridstart

DutchGrid Certification Authori[ty]

Reserved for CA operations use

/O=dutchgrid/O=users/O=nikhef/CN=Jan Klaassen

☐ ID document valid   ☐ PoP challenge **bededd03a849**

Surname
Klaassen

Given names
Jan

Place of Birth   Date of birth

Identity paper type, number, country

SOFI number *(optional)*

(for PoP challenge, see CA area at top of form)

Contact Information

Name
Jan Klaassen

Organisation

wait up to 3 days

Elly

Dennis   **David**

NIK

Today: jGridstart

BiG Grid

NIKHEF

Today: jGridstart

* ✳ Single intuitive user-interface
  * ✳ No need to use the command-line anymore
* ✳ Renewal is just as easy

Available now at a Certificate Authority near you

Next year: online certificate service

* What makes it so involved?
    * We need to see your id
    * Secret key must remain private

Next year: online certificate service

* What makes it so involved?
  * ~~We need to see your id~~
  * Secret key must remain private
    for local use

* But ... can't this be solved?
  * Yes!   *Terena Online Certificate Service*
  * Generate your certificate with institution login

Conclusion

Managing your (user) certificate

has never been easier

and it'll only get better :)

supported by

BiG Grid

NIKHEF

BiG Grid