DutchGrid

Authentication and Authorization

The Grid Security Infrastructure
and its implementation
in DutchGrid and DataGrid Test Bed 1

David Groep, NIKHEF

Overview

- Mechanisms for authentication
  - public key encryption; SSL and PGP
  - Certification Authorities
- Authentication in GSI and EDG Test Bed 1
  - your identity certificate
  - proxies and delegation
- Authorization in Test Bed 1
  - **As a user**: how do I get in?
  - **As an admin**: who can get in, how do I let people in?

Authentication

- The need to establish the identity of your partner (user *or* system)

- Options
  - just a name (username or DNS name)
  - fixed username/password
  - one-time passwords/tokens (cryptocard, DigiPass,…)
  - identity certificates in a `web-of-trust’

  - **identity certificates with trusted third parties**

secure communications using public key crypto

- conventional (symmatric) secure communication: *both parties need a pre-existing trusted channel*

- Asymmetric encryption (‘public key crypto’) allows secured communication

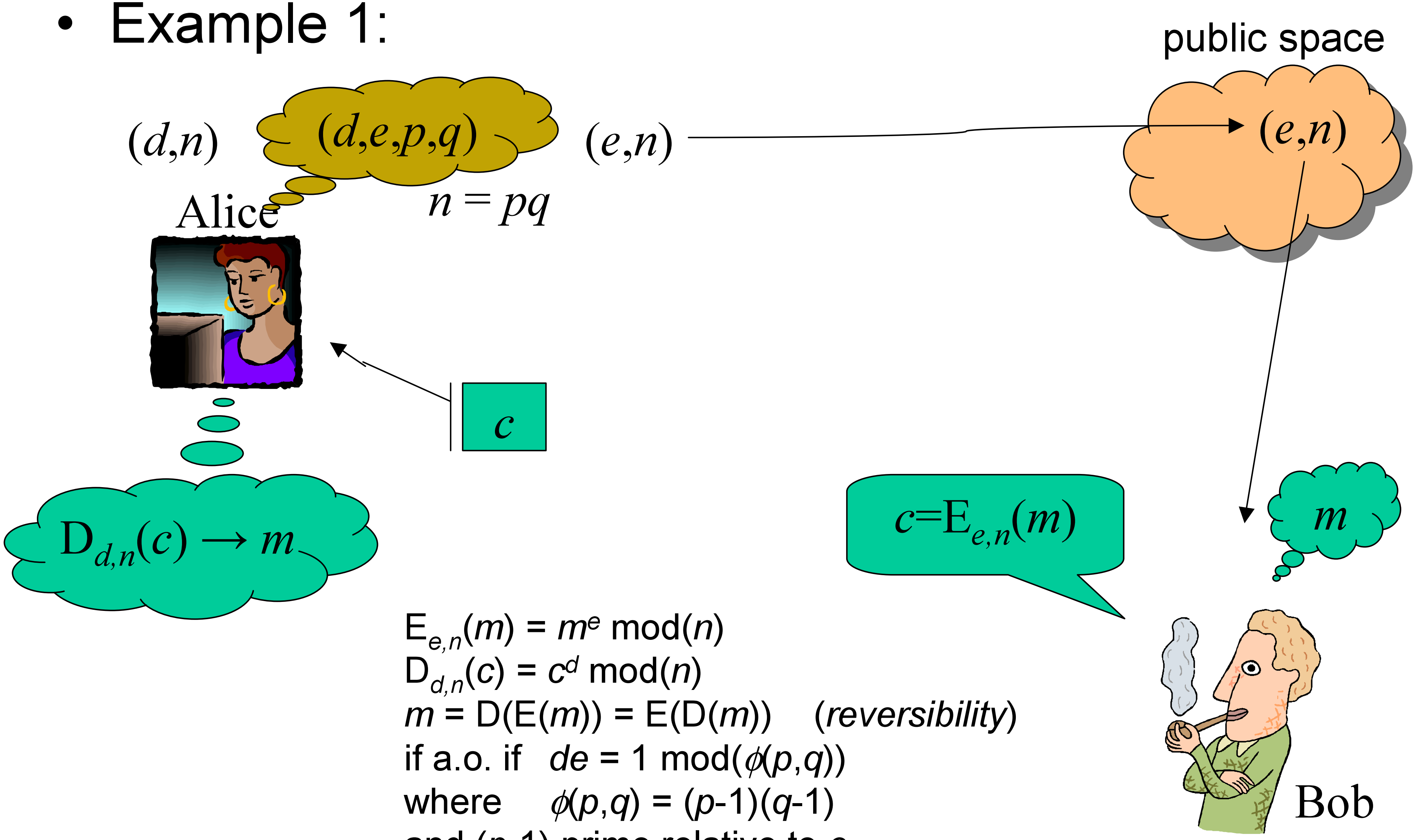
  without need for channel to share a secret

- You can reliably establish communications between two key pairs

- Relies on a (supposedly) difficulty problem, *e.g.*, factoring large numbers

How does it work?

- Example 1:



$E_{e,n}(m) = m^e \bmod(n)$
$D_{d,n}(c) = c^d \bmod(n)$
$m = D(E(m)) = E(D(m))$ (*reversibility*)
if a.o. if $de = 1 \bmod(\phi(p,q))$
where $\phi(p,q) = (p-1)(q-1)$
and $(p-1)$ prime relative to e

6-bit RSA key generation

- Take a (small) value e = **3**
- Generate a set of primes (p,q), each with a length of $k/2$ bits, with (p-1) prime relative to e.
  (p,q) = **(11,5)**
- $\phi(p,q) = (11-1)(5-1) =$ **40**; $n=pq=$**55**
- find d, in this case **27** [3*27 = 81 = 1 mod(40)]

- Public Key: **(3,55)**
- Private Key: **(27,55)**

$E_{e,n}(m) = m^e \bmod(n)$
$D_{d,n}(c) = c^d \bmod(n)$
$m = D(E(m)) = E(D(m))$ (*reversibility*)
if a.o. if $de = 1 \bmod(\phi(p,q))$
where $\phi(p,q) = (p-1)(q-1)$

Message Exchange

(3,55)

Encryption:

- Bob thinks of a plaintext $m(<n)$ = **18**
- Encrypt with Alice's public key **(3,55)**
- $c=E_{\mathbf{3;55}}(18)=18^3 \text{ mod}(55) = 5832 \text{ mod}(55) = \mathbf{2}$
- send message **"2"**

$E_{e,n}(m) = m^e \text{ mod}(n)$
$D_{d,n}(c) = c^d \text{ mod}(n)$
$m = D(E(m)) = E(D(m))$
if a.o. if $de = 1 \text{ mod}(\phi(p,q))$
where $\phi(p,q) = (p-1)(q-1)$

Decryption:

- Alice gets **"2"**
- she knows private key **(27,55)**
- $E_{\mathbf{27;55}}(2) = 2^{27} \text{ mod}(55) = \mathbf{18}$!

- If you just have (3,55), it's hard to get the 27…

What can be done?

- Confidentiality
  no-one but the recipient can read what you say

- Message integrity
  encrypt a digest of your message
  with a private key

- Non-repudiation
  similar to integrity

- This encryption works both ways with 2 key pairs

From crypto to trust?

- You establish communication between key pairs but not between entities!

- Binding needed between key pair and an identity (*this is implicit in symmetric solutions, but not here!*)
- in a trusted way …

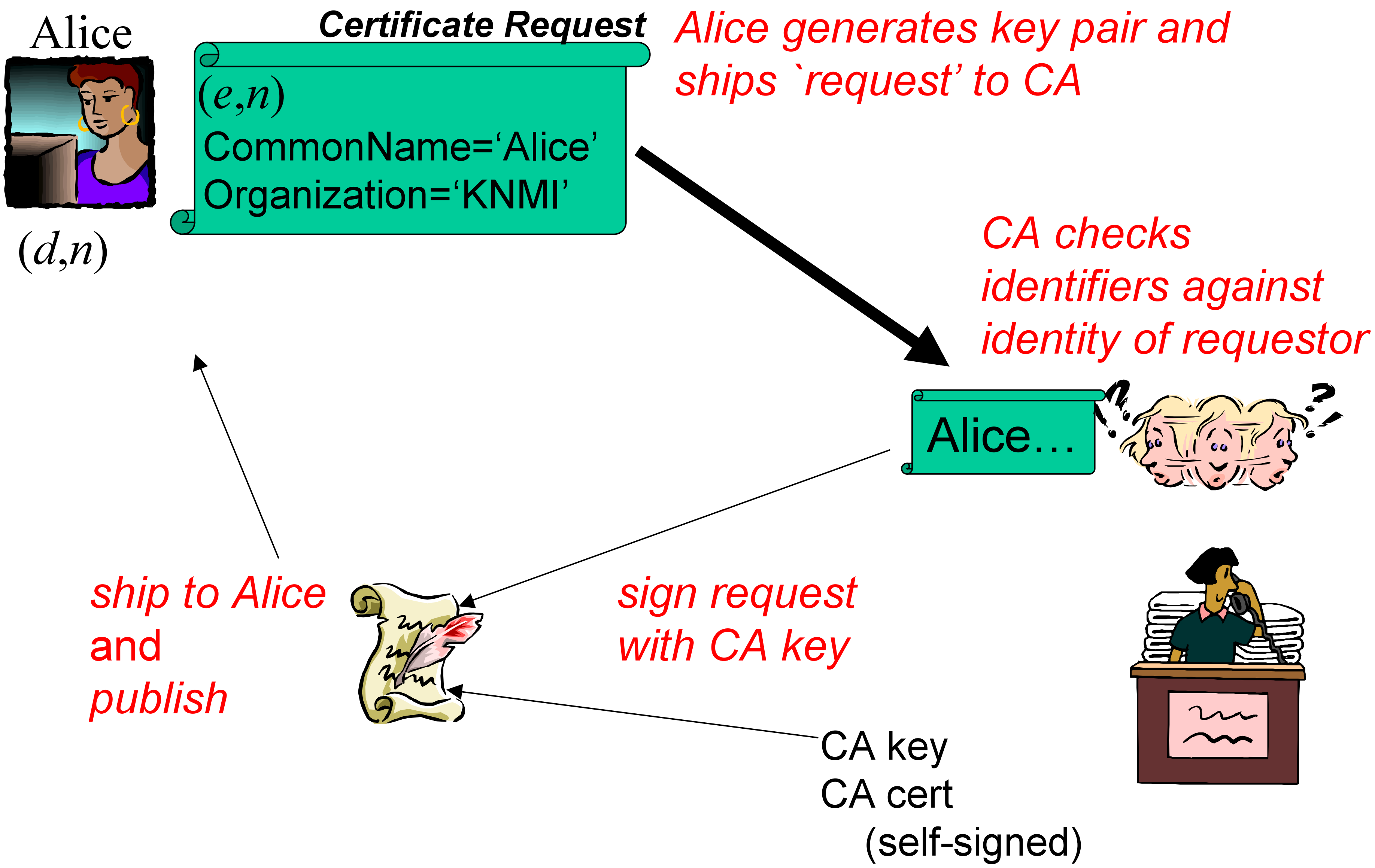
- Distributed trust models (PGP)
- **Hierarchical (authoritarian) model (PKI)**

PKI and the CA

- The PKI Certificate `X.509'
  - structured message with:
  - public key
  - identifier(s)
  - digitally signed by a trusted third party

- Certification Authority (CA)
  - binds user-supplied identifiers to a public key
  - in accordance with a defined Certification Policy
  - following the guidelines of a Certification Practice Statement

Identity Certification



Alice

(d,n)

Certificate Request

(e,n)

CommonName='Alice'

Organization='KNMI'

Alice generates key pair and ships `request' to CA

CA checks identifiers against identity of requestor

Alice…

sign request with CA key

CA key

CA cert (self-signed)

ship to Alice and publish

An example certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=NL, O=NIKHEF, CN=NIKHEF medium-security certification auth
        Validity
            Not Before: Feb 20 13:29:27 2001 GMT
            Not After : Feb 20 13:29:27 2002 GMT
        Subject: O=dutchgrid, O=users, O=nikhef, CN=David Groep
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ce:d7:1f:04:b4:50:eb:1b:da:ab:c7:db:ec:d9:
                    . . . .
                    f0:47:79:1e:3b:94:62:76:55
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                This CERT was issued under the NIKHEF medium...
            X509v3 CRL Distribution Points:
                URI:http://certificate.nikhef.nl/medium/cacrl.pem
            Netscape CA Policy Url:
                   http://certificate.nikhef.nl/medium/policy/
     Signature Algorithm: md5WithRSAEncryption
        14:6f:c3:8f:36:6d:41:48:f9:01:b2:48:f3:62:7a:a0:e3:52:
        . . . .
        0e:d2:85:65
```

Common Policy Items

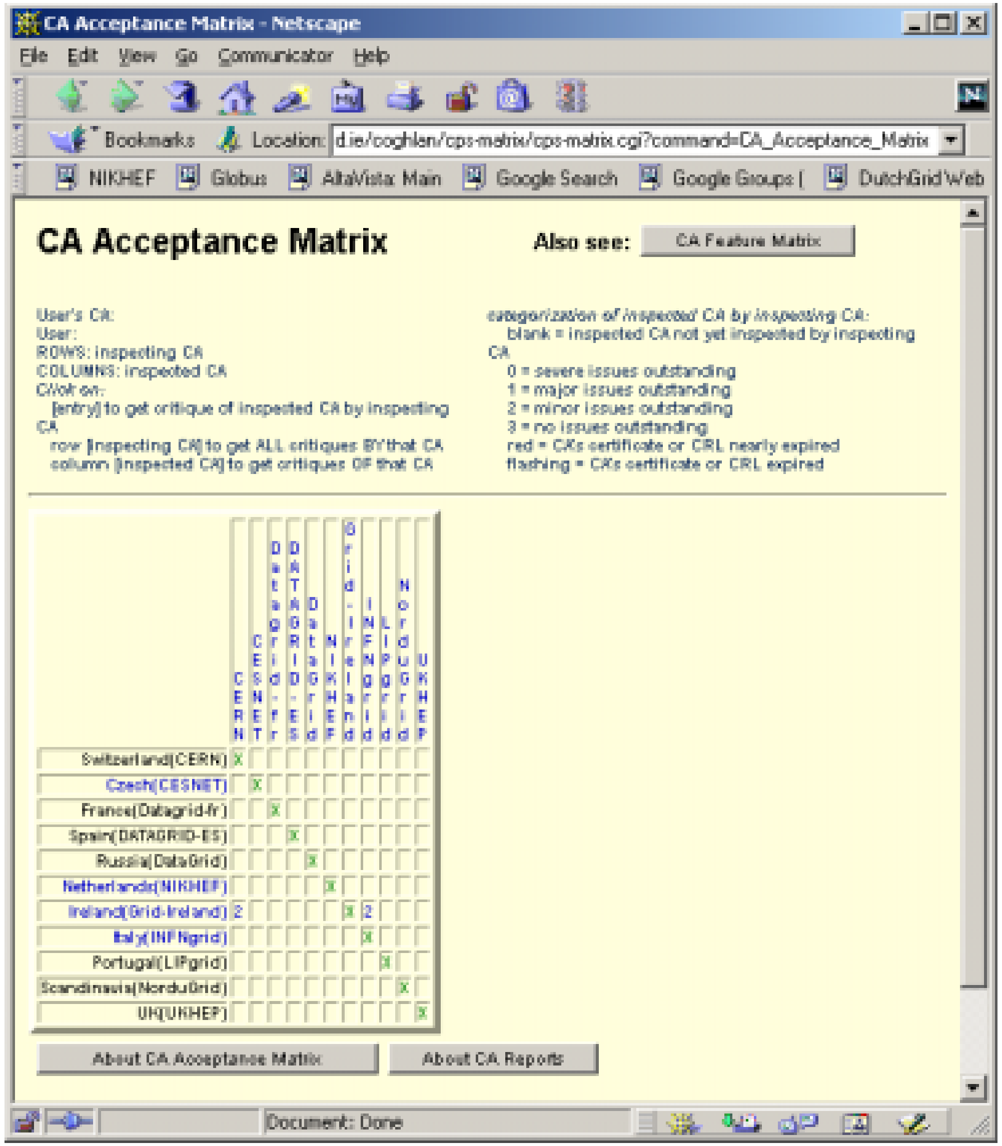
- EU DataGrid CA’s adhere to minimum standards:

- Check identity of requestor by
  - personal appearance before Registration Authority
  - voice recognition for people the RA knows

- Identifiers corresponds to `official’ name (nat. ID)
- Affiliation is required and known to be correct

- Issues certificates for `local region’ only

CA Acceptance Matrix


CA Acceptance Matrix - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: d.ie/coghlan/cps-matrix/cps-matrix.cgi?command=CA_Acceptance_Matrix
NIKHEF
Globus
AltaVista: Main
Google Search
Google Groups |
DutchGrid Web
Document: Done

CA Acceptance Matrix

Also see: CA Feature Matrix

User's CA:
User:
ROWS: inspecting CA
COLUMNS: inspected CA
Click on:
[entry] to get critique of inspected CA by inspecting CA
row [inspecting CA] to get ALL critiques BY that CA
column [inspected CA] to get critiques OF that CA

categorization of inspected CA by inspecting CA:
blank = inspected CA not yet inspected by inspecting CA
0 = severe issues outstanding
1 = major issues outstanding
2 = minor issues outstanding
3 = no issues outstanding
red = CA's certificate or CRL nearly expired
flashing = CA's certificate or CRL expired

	CERN	CESNET	Datagrid-fr	DATAGRID-ES	DataGrid	NIKHEF	Grid-Ireland	INFNgrid	LIPgrid	NorduGrid	UKHEP
Switzerland(CERN)	X										
Czech(CESNET)		X									
France(Datagrid-fr)			X								
Spain(DATAGRID-ES)				X							
Russia(DataGrid)					X						
Netherlands(NIKHEF)						X					
Ireland(Grid-Ireland)	2						X	2			
Italy(INFNgrid)								X			
Portugal(LIPgrid)									X		
Scandinavia(NorduGrid)										X	
UK(UKHEP)											X

About CA Acceptance Matrix

About CA Reports

Overview of all EDG CA's

Aid for site admins to establish trust in the various CA's

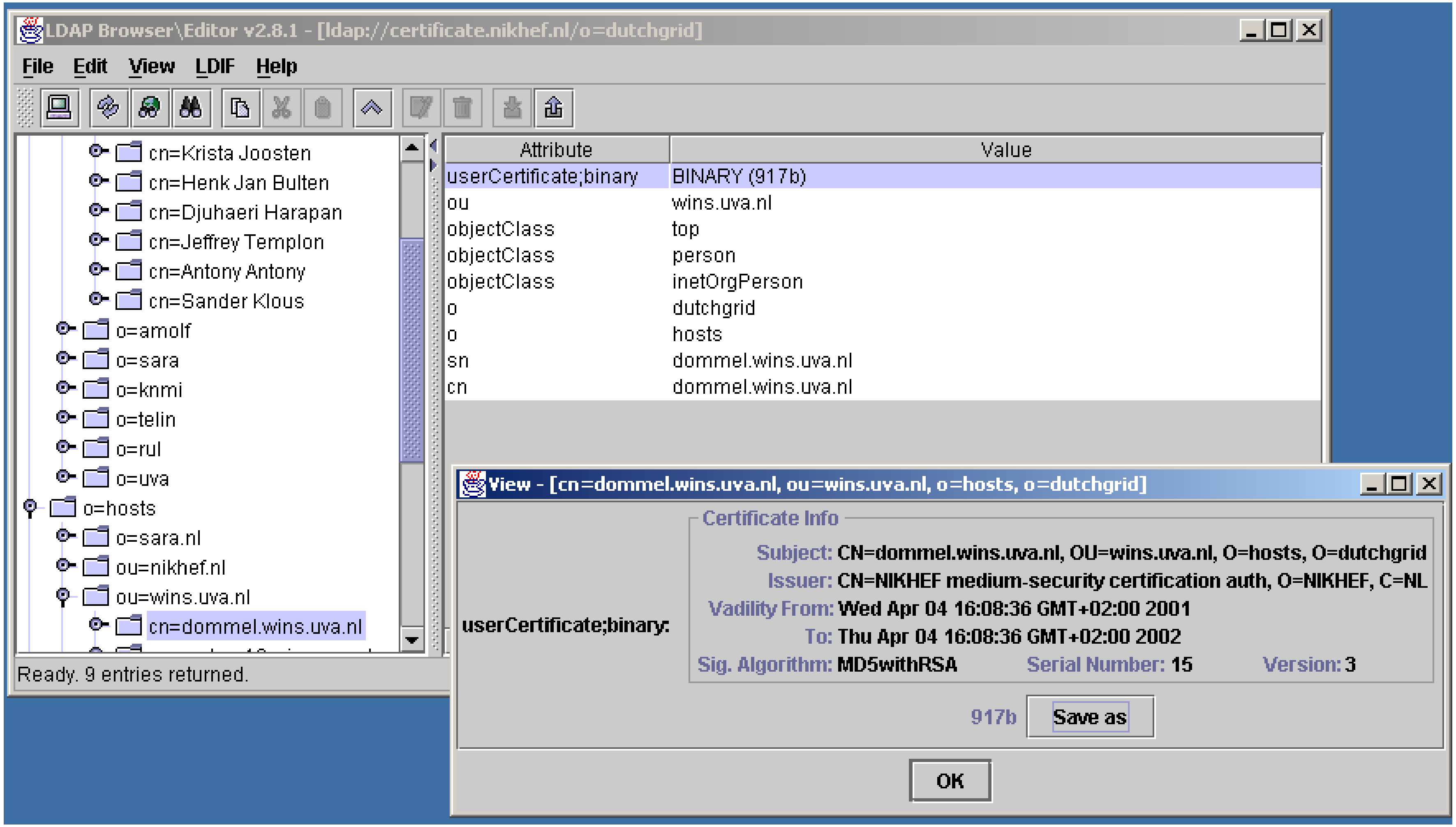
From WP6/CA web site
http://marianne.in2p3.fr/

Also list of features

by Brian Coughlan (TCD)

Certificate Repositories

LDAP directory with all certificates → send mail or build VO's


LDAP Browser\Editor v2.8.1 - [ldap://certificate.nikhef.nl/o=dutchgrid]
File
Edit
View
LDIF
Help

```
      cn=Krista Joosten
      cn=Henk Jan Bulten
      cn=Djuhaeri Harapan
      cn=Jeffrey Templon
      cn=Antony Antony
      cn=Sander Klous
    o=amolf
    o=sara
    o=knmi
    o=telin
    o=rul
    o=uva
  o=hosts
    o=sara.nl
    ou=nikhef.nl
    ou=wins.uva.nl
      cn=dommel.wins.uva.nl
```

Attribute	Value
userCertificate;binary	BINARY (917b)
ou	wins.uva.nl
objectClass	top
objectClass	person
objectClass	inetOrgPerson
o	dutchgrid
o	hosts
sn	dommel.wins.uva.nl
cn	dommel.wins.uva.nl

Ready. 9 entries returned.

View - [cn=dommel.wins.uva.nl, ou=wins.uva.nl, o=hosts, o=dutchgrid]

userCertificate;binary:

Certificate Info

Subject: CN=dommel.wins.uva.nl, OU=wins.uva.nl, O=hosts, O=dutchgrid
Issuer: CN=NIKHEF medium-security certification auth, O=NIKHEF, C=NL
Vadility From: Wed Apr 04 16:08:36 GMT+02:00 2001
To: Thu Apr 04 16:08:36 GMT+02:00 2002
Sig. Algorithm: MD5withRSA Serial Number: 15 Version: 3

917b

Getting your own certificate

- On a DataGrid testbed system:
  - initialialize your environment
  - type `grid-cert-request’
  - mail it to **ca@nikhef.nl**
  - the CA will get back to you

- For all other certs (from any system):
  - Go to http://certificate.nikhef.nl/
  - Use the Build-a-Cert interface

  - Have a command prompt handy with OpenSSL (for all of Unix, Linux and Win32!)

Storing your cert

- **Your private key is valuable, keep it safe**
  - protected with a pass phrase (conventional symmetric crypto)
  - store it securely (e.g. on removable medium)
  - keep it private
  - never share with others

- Find all your credential data in **`$HOME/.globus/`**
  - Private key in “userkey.pem”
  - Public key certificate in “usercert.pem”
  - CA’s that ***you*** trust in “~/.globus/certificates/” (if needed)

Your proxy

- you use a `proxy certificate’ to authenticate

- derived from your `long-lasting’ certificate
- limited validity (default 12 hours, can be longer)

- limits exposure of key pair
- limits the damage done when compromised

- get it with **grid-proxy-init**

Authorization

- Authorization deals with actual access to resources
- Various possible models (push, pull, agent)
  see http://www.aaaarch.org/
- The GSI is *now* based on per-resource access lists
  - grid-mapfiles: map grid identifiers to local user ID's
- In the future
  - "token-based" authorization
  - based on agreements per user community
  - "Community Authorization Service" (CAS)

the grid-mapfile

- Local administrator remains `in control’
- this list, owned by root, determines who gets in

```
$ ssh polyeder cat /etc/grid-security/grid-mapfile
"/O=dutchgrid/O=users/O=nikhef/CN=David Groep" davidg
"/O=dutchgrid/O=users/O=nikhef/CN=Michiel Botje" h24
#"/O=dutchgrid/O=users/O=sara/CN=Ron Trompert" griduser
"/O=dutchgrid/O=users/O=nikhef/CN=Jeffrey Templon" aliprod
#
# alice testbed users
"/C=IT/O=INFN/L=Catania/CN=Roberto Barbera/Email=roberto.barb……
"/O=Grid/O=CERN/OU=cern.ch/CN=Predrag Buncic" aliprod
"/O=Grid/O=CERN/OU=cern.ch/CN=Federico Carminati" aliprod
"/C=FR/O=CNRS/OU=SUBATECH/CN=Yves Schutz/Email=schutz@in2p3.fr” …
"/C=IT/O=INFN/L=Torino/CN=PiergiorgioCerello/Email=Piergiorgio……
```

The User: getting in the map

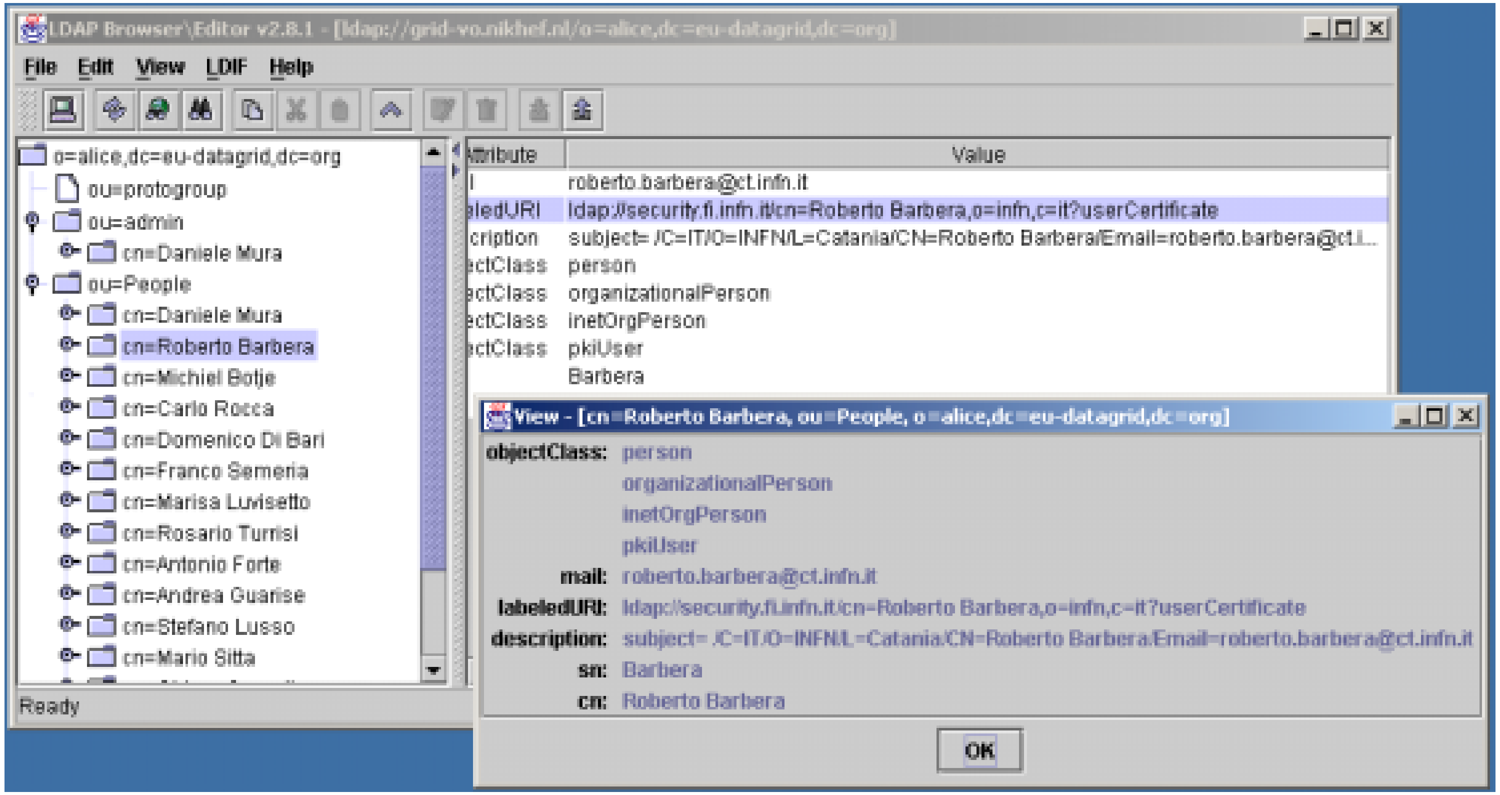
- Within the EU DataGrid context: **join a VO**
  - contact your WP manager or
  - your Experiment Coordinator(s): http://datagrid-wp8.web.cern.ch/datagrid-wp8/

- Or contact the desired site administrator
  - state your Subject name
  - your local user name (if you have one)
  - and send lots of apple pie ☺ or equivalent

- Acceptable Use Policy/Contract (AUP) forthcoming (only relevant for EDG, still under serious discussion)

The VO: making a directory

- The VO directory contains
  - People
  - Groups and Group Admins (group administrators)
  - A `Super User' (VO Manager)


LDAP Browser\Editor v2.8.1 - [ldap://grid-vo.nikhef.nl/o=alice,dc=eu-datagrid,dc=org]
File
Edit
View
LDIF
Help
Ready

```
o=alice,dc=eu-datagrid,dc=org
    ou=protogroup
    ou=admin
        cn=Daniele Mura
    ou=People
        cn=Daniele Mura
        cn=Roberto Barbera
        cn=Michiel Botje
        cn=Carlo Rocca
        cn=Domenico Di Bari
        cn=Franco Semeria
        cn=Marisa Luvisetto
        cn=Rosario Turrisi
        cn=Antonio Forte
        cn=Andrea Guarise
        cn=Stefano Lusso
        cn=Mario Sitta
```

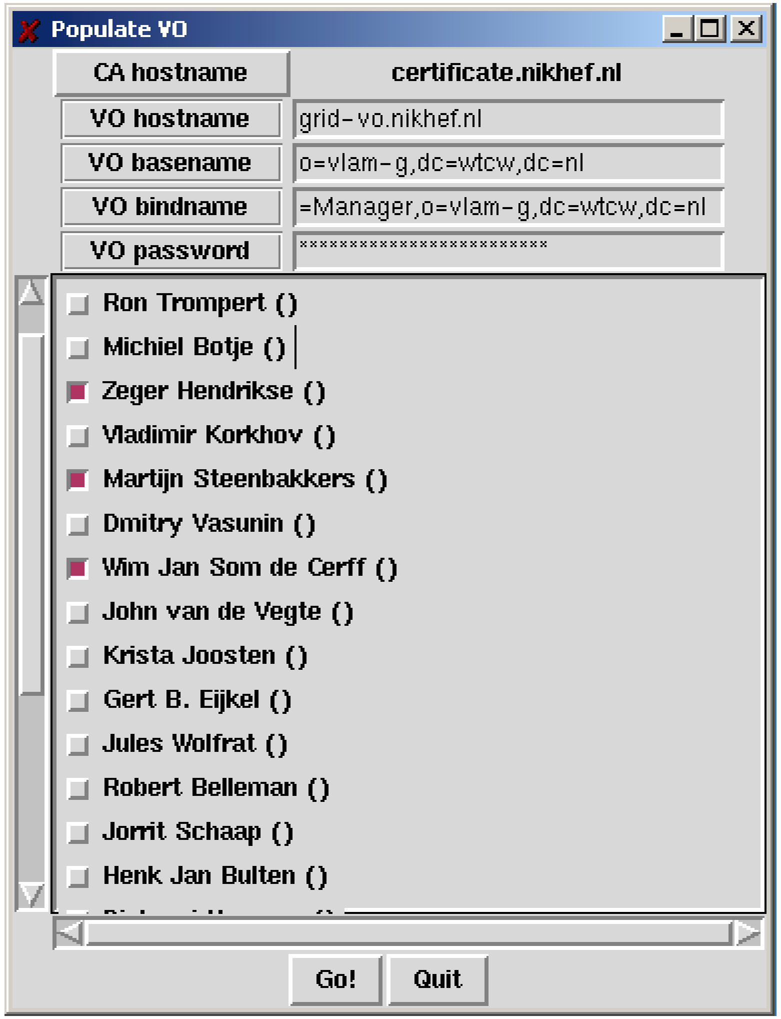
ttribute	Value
l	roberto.barbera@ct.infn.it
eledURI	ldap://security.fi.infn.it/cn=Roberto Barbera,o=infn,c=it?userCertificate
cription	subject= /C=IT/O=INFN/L=Catania/CN=Roberto Barbera/Email=roberto.barbera@ct.i...
ectClass	person
ectClass	organizationalPerson
ectClass	inetOrgPerson
ectClass	pkiUser
	Barbera

View - [cn=Roberto Barbera, ou=People, o=alice,dc=eu-datagrid,dc=org]
OK

objectClass: person
organizationalPerson
inetOrgPerson
pkiUser
mail: roberto.barbera@ct.infn.it
labeledURI: ldap://security.fi.infn.it/cn=Roberto Barbera,o=infn,c=it?userCertificate
description: subject= /C=IT/O=INFN/L=Catania/CN=Roberto Barbera/Email=roberto.barbera@ct.infn.it
sn: Barbera
cn: Roberto Barbera

VO Tools: VOP

- Add People to a VO
- based on
  CA Directory
- Can be run by
  VO Managers
- *cert2ldif*



CA hostname: certificate.nikhef.nl

VO hostname: grid-vo.nikhef.nl

VO basename: o=vlam-g,dc=wtcw,dc=nl

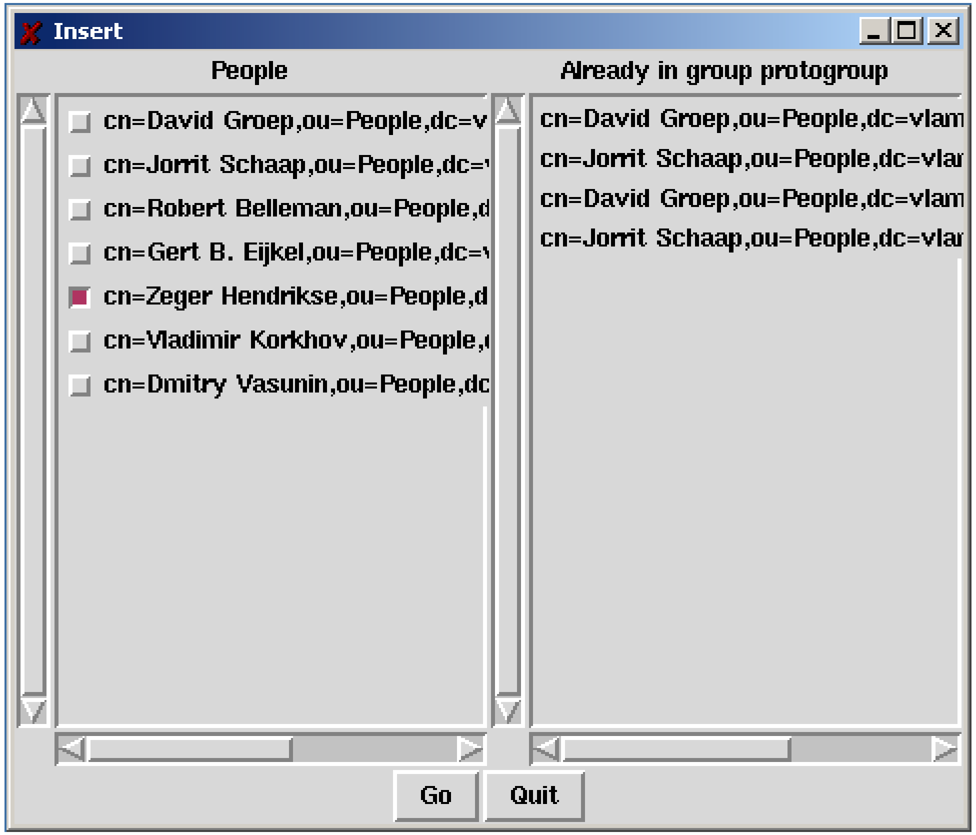
VO bindname: =Manager,o=vlam-g,dc=wtcw,dc=nl

VO password: *************************

- □ Ron Trompert ()
- □ Michiel Botje ()
- ☒ Zeger Hendrikse ()
- □ Vladimir Korkhov ()
- ☒ Martijn Steenbakkers ()
- □ Dmitry Vasunin ()
- ☒ Wim Jan Som de Cerff ()
- □ John van de Vegte ()
- □ Krista Joosten ()
- □ Gert B. Eijkel ()
- □ Jules Wolfrat ()
- □ Robert Belleman ()
- □ Jorrit Schaap ()
- □ Henk Jan Bulten ()

VO tools: Group

- Add VO members to a group
- Can be run by group admins



People

□ cn=David Groep,ou=People,dc=v
□ cn=Jorrit Schaap,ou=People,dc=
□ cn=Robert Belleman,ou=People,d
□ cn=Gert B. Eijkel,ou=People,dc=
☑ cn=Zeger Hendrikse,ou=People,d
□ cn=Vladimir Korkhov,ou=People,
□ cn=Dmitry Vasunin,ou=People,dc

Already in group protogroup

cn=David Groep,ou=People,dc=vlam
cn=Jorrit Schaap,ou=People,dc=vla
cn=David Groep,ou=People,dc=vlam
cn=Jorrit Schaap,ou=People,dc=vla

The Admin: making the map

1. You can add users by hand: tedious&trusted
2. You can get lists of users from the VO’s: tedious & somewhat less trusted (group accounts)

- If you have chosen for (2), you better use: **mkgridmap** from the EDG Authorization group

- Based on VO-maintained user lists
- retain lots of local control over configuration http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/mkgridmap/

mkgridmap.conf

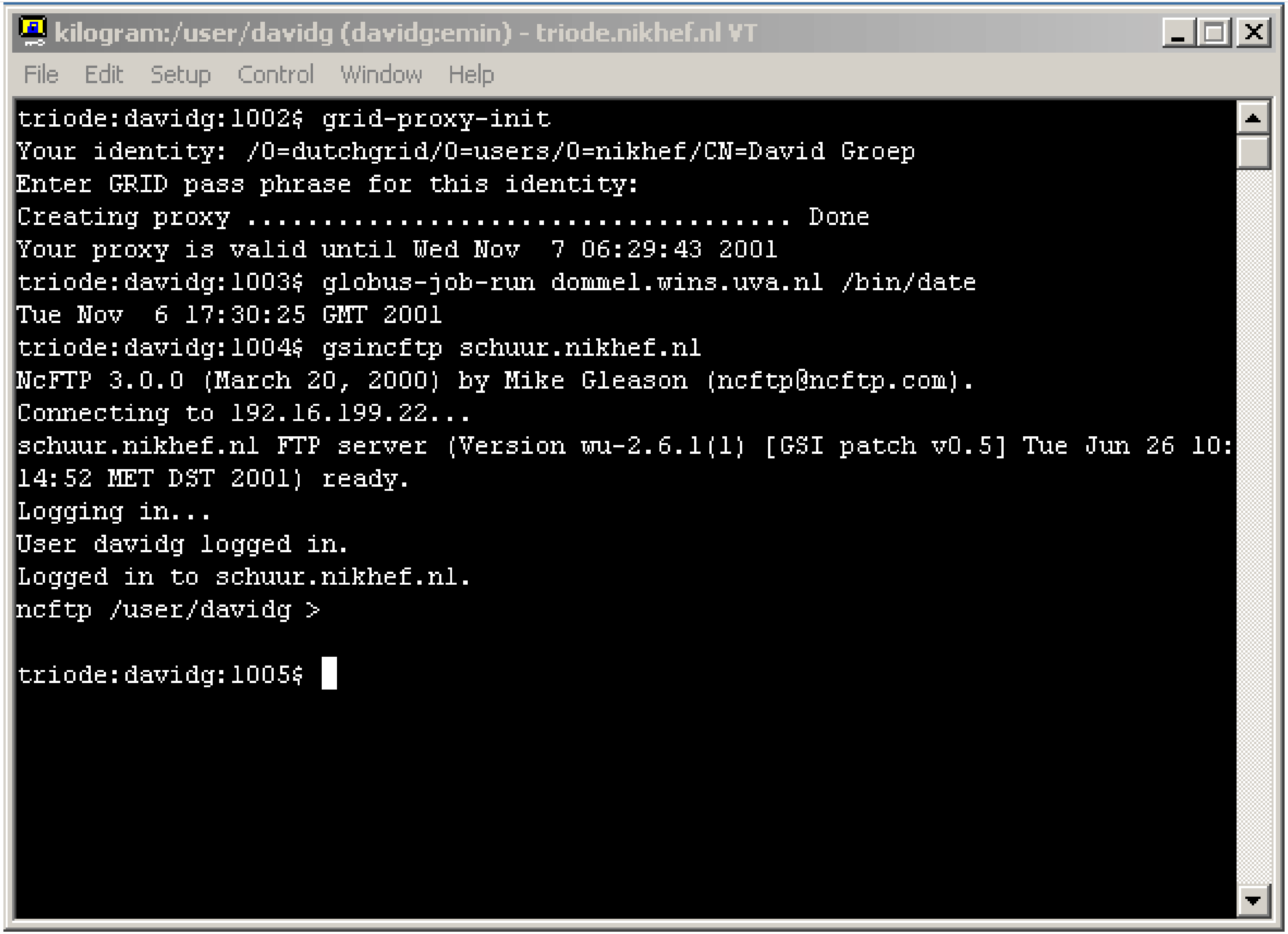
```
#### GROUP: group URL [lcluser]
group ldap://grid-vo.nikhef.nl/ou=omi,o=earthob,dc=eu-datagrid,dc=org  tb2
group ldap://grid-vo.nikhef.nl/ou=mcprod,o=alice,dc=eu-datagrid,dc=org aliprod

#### ACL: deny|allow pattern_to_match
deny  *L=Parma*
allow *O=INFN*
allow *CESNET*
deny  *John*
allow *dutchgrid*

#### DEFAULT LOCAL USER
default_lcluser testbed1

##### GRID-MAPFILE-LOCAL
gmf_local /etc/grid-security/grid-mapfile-local
```

What can you do now?


kilogram:/user/davidg (davidg:emin) - triode.nikhef.nl VT
File Edit Setup Control Window Help

```
triode:davidg:1002$ grid-proxy-init
Your identity: /O=dutchgrid/O=users/O=nikhef/CN=David Groep
Enter GRID pass phrase for this identity:
Creating proxy .................................... Done
Your proxy is valid until Wed Nov  7 06:29:43 2001
triode:davidg:1003$ globus-job-run dommel.wins.uva.nl /bin/date
Tue Nov  6 17:30:25 GMT 2001
triode:davidg:1004$ gsincftp schuur.nikhef.nl
NcFTP 3.0.0 (March 20, 2000) by Mike Gleason (ncftp@ncftp.com).
Connecting to 192.16.199.22...
schuur.nikhef.nl FTP server (Version wu-2.6.1(1) [GSI patch v0.5] Tue Jun 26 10:
14:52 MET DST 2001) ready.
Logging in...
User davidg logged in.
Logged in to schuur.nikhef.nl.
ncftp /user/davidg >

triode:davidg:1005$
```

More Info?

http://www.dutchgrid.nl/