# Grid Security 101

*Dennis van Dok*

www.eu-egee.org

e-infrastructure

Information Society
and media

CAPACITIES

# Outline

Introduction

Trust

Obtain a certificate

Loading the certificate in a browser

Become a VO member

Get to work

One year later. . .

# What me worry?

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

# What me worry?

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

# What me worry II

Computer networks need security too!

# What me worry II

Computer networks need security too!

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

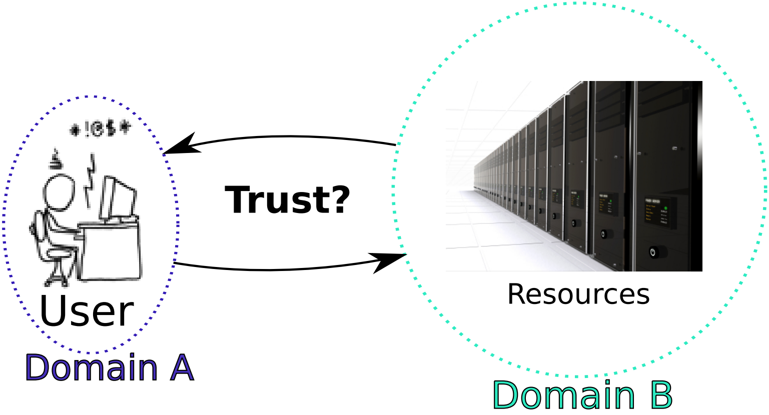
# The A'spects of computer security

**Brought to you by the letter A**:

- **Authentication**
- Authorization
- Accounting
- Auditing

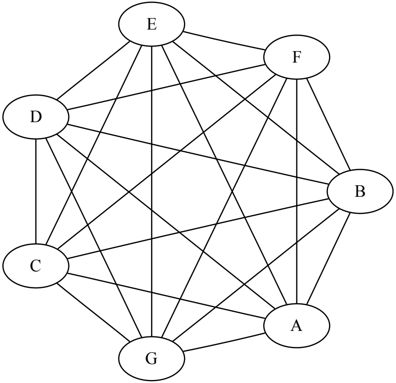
Your first and foremost worry is *authentication*

# Knowing who to trust



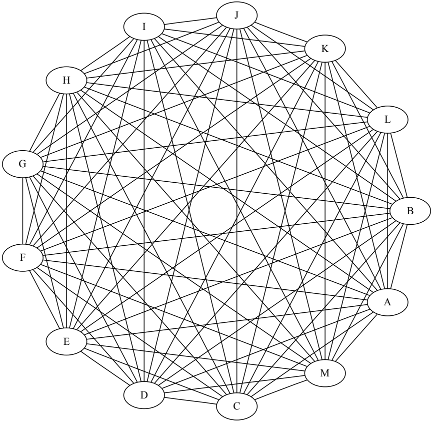
# Number of trust relations

#domains = 7



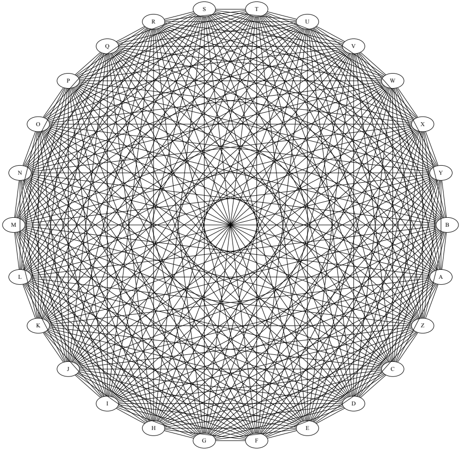
# Number of trust relations

#domains = 13

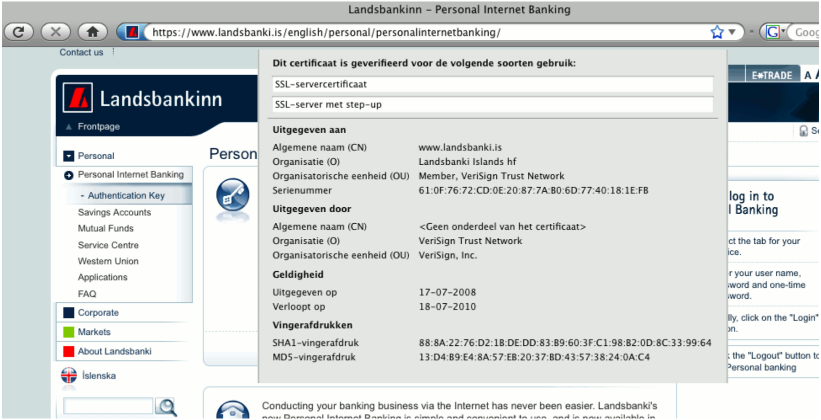


# Number of trust relations

#domains = 26



# Digital Certificates



**Dit certificaat is geverifieerd voor de volgende soorten gebruik:**

SSL-servercertificaat

SSL-server met step-up

**Uitgegeven aan**

| | |
|---|---|
| Algemene naam (CN) | www.landsbanki.is |
| Organisatie (O) | Landsbanki Islands hf |
| Organisatorische eenheid (OU) | Member, VeriSign Trust Network |
| Serienummer | 61:0F:76:72:CD:0E:20:87:7A:B0:6D:77:40:18:1E:FB |

**Uitgegeven door**

| | |
|---|---|
| Algemene naam (CN) | <Geen onderdeel van het certificaat> |
| Organisatie (O) | VeriSign Trust Network |
| Organisatorische eenheid (OU) | VeriSign, Inc. |

**Geldigheid**

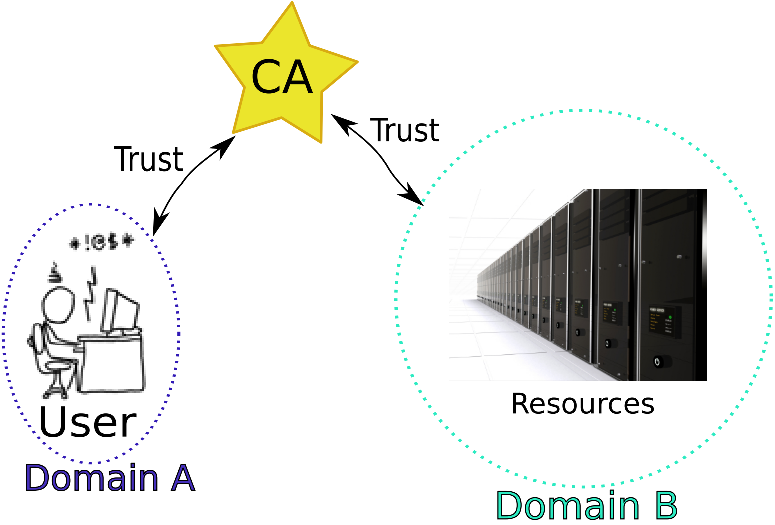
| | |
|---|---|
| Uitgegeven op | 17-07-2008 |
| Verloopt op | 18-07-2010 |

**Vingerafdrukken**

| | |
|---|---|
| SHA1-vingerafdruk | 88:8A:22:76:D2:1B:DE:DD:83:B9:60:3F:C1:98:B2:0D:8C:33:99:64 |
| MD5-vingerafdruk | 13:D4:B9:E4:8A:57:EB:20:37:BD:43:57:38:24:0A:C4 |

Conducting your banking business via the Internet has never been easier. Landsbanki's new Personal Internet Banking is simple and convenient to use, and is now available in

# Knowing who to trust



CA

Trust

Trust

User

Domain A

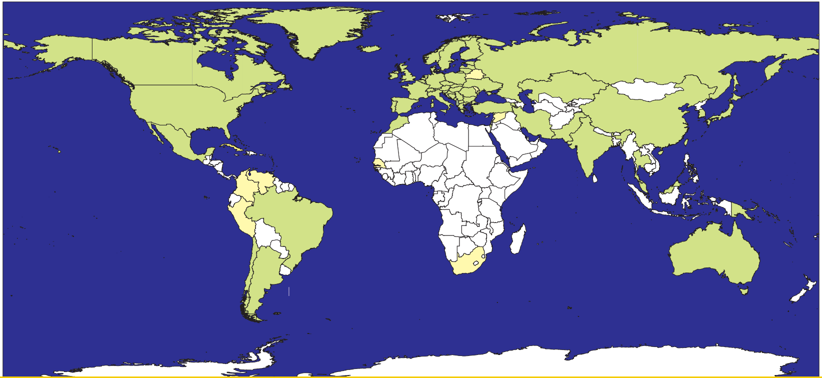
Resources

Domain B

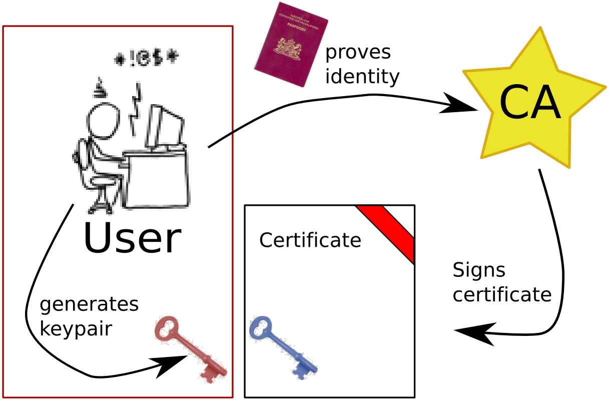
# Trusted third parties

- 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

IGTF
International Grid Trust Federation
AP|EU|TAG

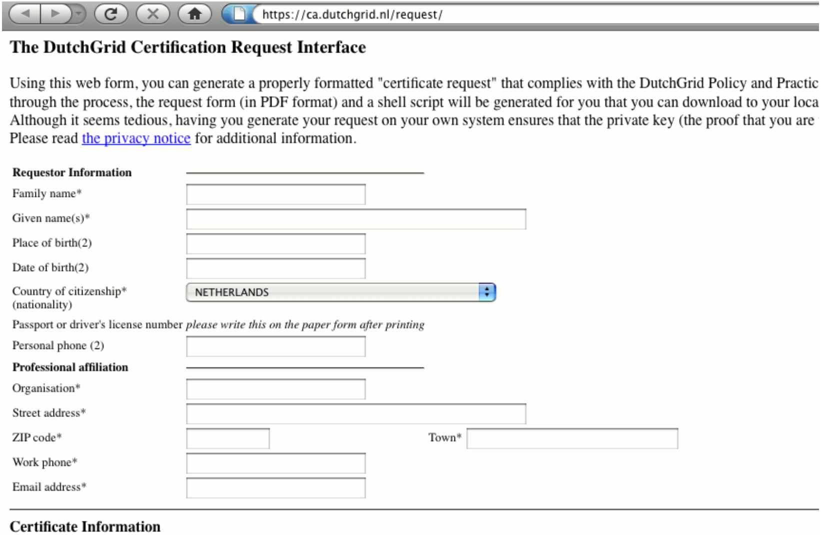


# How to obtain a certificate



# Request a certificate

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



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

## The DutchGrid Certification Request Interface

Using this web form, you can generate a properly formatted "certificate request" that complies with the DutchGrid Policy and Practic
through the process, the request form (in PDF format) and a shell script will be generated for you that you can download to your loca
Although it seems tedious, having you generate your request on your own system ensures that the private key (the proof that you are
Please read the privacy notice for additional information.

**Requestor Information**

Family name*

Given name(s)*

Place of birth(2)

Date of birth(2)

Country of citizenship* (nationality) NETHERLANDS

Passport or driver's license number *please write this on the paper form after printing*

Personal phone (2)

**Professional affiliation**

Organisation*

Street address*

ZIP code* Town*

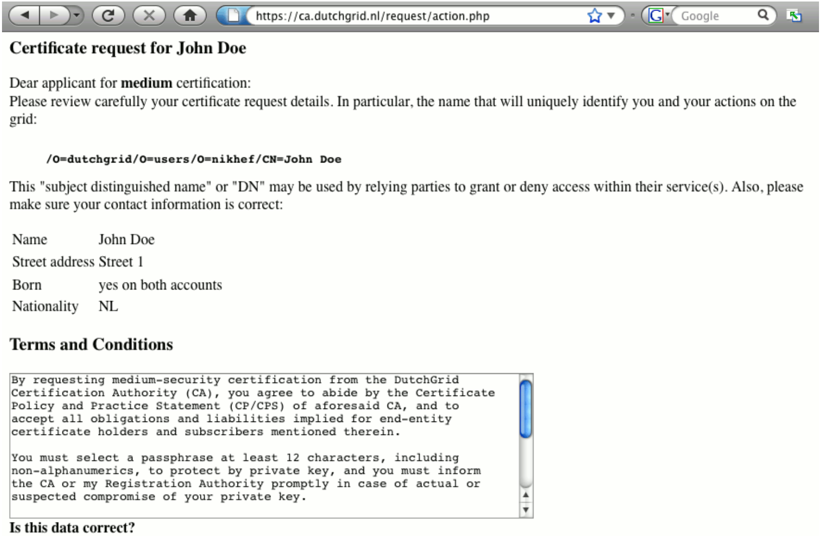
Work phone*

Email address*

**Certificate Information**

# Request a certificate

## Verify your data and continue



### Certificate request for John Doe

Dear applicant for **medium** certification:
Please review carefully your certificate request details. In particular, the name that will uniquely identify you and your actions on the grid:

```
/O=dutchgrid/O=users/O=nikhef/CN=John Doe
```

This "subject distinguished name" or "DN" may be used by relying parties to grant or deny access within their service(s). Also, please make sure your contact information is correct:

| | |
|---|---|
| Name | John Doe |
| Street address | Street 1 |
| Born | yes on both accounts |
| Nationality | NL |

### Terms and Conditions

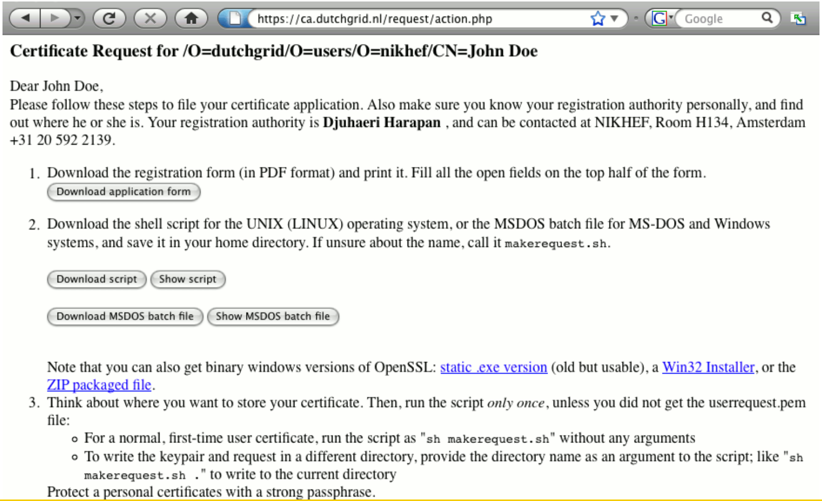
```
By requesting medium-security certification from the DutchGrid
Certification Authority (CA), you agree to abide by the Certificate
Policy and Practice Statement (CP/CPS) of aforesaid CA, and to
accept all obligations and liabilities implied for end-entity
certificate holders and subscribers mentioned therein.

You must select a passphrase at least 12 characters, including
non-alphanumerics, to protect by private key, and you must inform
the CA or my Registration Authority promptly in case of actual or
suspected compromise of your private key.
```

**Is this data correct?**

# Request a certificate

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



**Certificate Request for /O=dutchgrid/O=users/O=nikhef/CN=John Doe**

Dear John Doe,
Please follow these steps to file your certificate application. Also make sure you know your registration authority personally, and find out where he or she is. Your registration authority is **Djuhaeri Harapan** , and can be contacted at NIKHEF, Room H134, Amsterdam +31 20 592 2139.

1. Download the registration form (in PDF format) and print it. Fill all the open fields on the top half of the form.
   Download application form
2. Download the shell script for the UNIX (LINUX) operating system, or the MSDOS batch file for MS-DOS and Windows systems, and save it in your home directory. If unsure about the name, call it `makerequest.sh`.

   Download script  Show script

   Download MSDOS batch file  Show MSDOS batch file

   Note that you can also get binary windows versions of OpenSSL: static .exe version (old but usable), a Win32 Installer, or the ZIP packaged file.
3. Think about where you want to store your certificate. Then, run the script *only once*, unless you did not get the userrequest.pem file:
   - For a normal, first-time user certificate, run the script as "`sh makerequest.sh`" without any arguments
   - To write the keypair and request in a different directory, provide the directory name as an argument to the script; like "`sh makerequest.sh .`" to write to the current directory

   Protect a personal certificates with a strong passphrase.

# 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
the certification authority.
```

# Running the script

```
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:

B811761282B5AC7FCC59DE7B4381B879DD02FB6280A20DB2B42F3EC4AEDF36A2
2074484DF7B407B77A1C30FF825C15C3A7DFD659F72815DD90AC59067A85D23F
E1BB4FAD134B8FDB1A1F064AE29DB38169A03ACF1E0C99E6DE0F88CE1DCE87D5
EDE5EBCB260FD40D

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

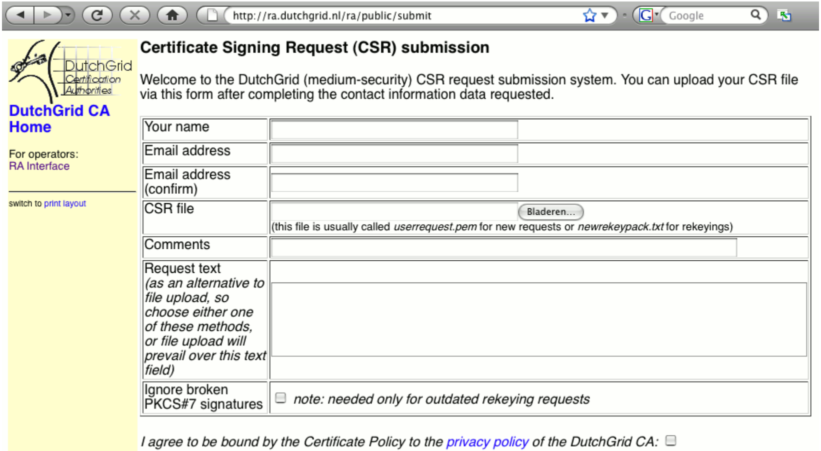
# Running the script

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 |

# Upload the request

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



**DutchGrid CA Home**

For operators:
RA Interface

switch to print layout

## Certificate Signing Request (CSR) submission

Welcome to the DutchGrid (medium-security) CSR request submission system. You can upload your CSR file via this form after completing the contact information data requested.

| | |
|---|---|
| Your name | |
| Email address | |
| Email address (confirm) | |
| CSR file | Bladeren...<br>(this file is usually called *userrequest.pem* for new requests or *newrekeypack.txt* for rekeyings) |
| Comments | |
| Request text *(as an alternative to file upload, so choose either one of these methods, or file upload will prevail over this text field)* | |
| Ignore broken PKCS#7 signatures | □ *note: needed only for outdated rekeying requests* |

*I agree to be bound by the Certificate Policy to the privacy policy of the DutchGrid CA:* □

# 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

# 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`

# 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`

# 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!

# Thanks for your attention. . .

. . . You've been a wonderfull audience.