



ID: INFNGRID20030714-0930

Version: v1.0.0

Date: April 19, 2005

# INFN-GRID personal certificates

## howto

Andrea Caltroni

INFN-Padova (andrea.caltroni@pd.infn.it)

Andrea Ferraro

INFN-CNAF (andrea.ferraro@cnafe.infn.it)

Enrico Ferro

INFN-Padova (enrico.ferro@pd.infn.it)

**Abstract:** *Some information about user certificate request, management and use.*

# Contents

1	Introduction	3
2	Install INFN CA certificate on your browser	3
3	Certificate request: go to your Registration Authority	3
4	Create your private key with your web browser	3
5	Download your certificate	3
6	Export your certificate	4
7	Install your certificate on the UI	4

# 1 Introduction

This document describes the steps required to access to INFN-GRID; they are required to:

- Be authenticated: request a certificate to a Certification Authority (CA)
- Be authorized: register it into a Virtual Organization (VO) server
- Use the certificate: install the certificate in the host that gives you access to the grid

## 2 Install INFN CA certificate on your browser

Currently the Certification Authority issuing certificates for INFN-GRID infrastructure is only INFN CA. A CNR CA is foreseen. Go to the INFN CA URL:

- <http://security.fi.infn.it/CA>

and select *Certificato INFN CA*; follow the instructions to install in your browser the INFN CA certificate. From this moment your browser will recognize as valid certificates issued by INFN CA (like your).

## 3 Certificate request: go to your Registration Authority

Current INFN CA policy requests that in your institute a Registration Authority (RA) is defined. A Registration Authority is a person responsible to identify you for INFN. So the first step is to go to your local Registration Authority with and ask for a digital certificate. The Registration Authority will start a simple procedure and will give you an ID.

At the following URL you can find the RA list (and the person to contact at your institute). If there is no RA, follow the procedure described to setup a RA for your institute:

- <https://security.fi.infn.it/CA/RA/>

## 4 Create your private key with your web browser

Once the RA gave you the ID request, go to:

- <http://security.fi.infn.it/CA>

and select *Richiesta certificati*. Compile your personal data and the ID, verify them and confirm. At this point your browser will ask you for a password (or to define it, if you never used certificates before): this password is used to the encrypt your private key before saving it locally.

Then the browser will generate the couple of private-public and it will send your public key to the CA to be signed.

## 5 Download your certificate

In a few days you will receive an email from INFN CA with an URL. Use *the same browser and the same machine* you used to *generate the couple private-public key* to connect to that URL. The browser will install your certificate (i.e. your public key signed by INFN CA) and you will be prompted for the password to access to the private key.

## 6 Export your certificate

At this point the certificate + your private key are saved encrypted on the configuration files of your web browser and you are listed in the VO server as an authorized grid user. The next step is to export them from the browser and install them on the machine where you will be allowed to submit job to the grid (a UserInterface). For Mozilla the steps are:

**Edit / Preferences / Privacy and Security / Certificates / Manage Certificates / Backup**

You will be prompted for a filename; your browser will ask for the password to decrypt the certificate + private key. Then it will ask for a new password: this password will be used to encrypt *the new file*.

## 7 Install your certificate on the UI

Log in into the UserInterface, copy there the file you exported, and create a directory where your certificate + private key will be stored:

```
mkdir ~/.globus
```

It is likely that you have got from the browser a PKCS12 file (\*.p12). Unfortunately this format is not accepted by Globus security infrastructure, but you can easily convert it into the supported standard (PEM). This operation will split your \*.p12 file in two files: the certificate (usercert.pm) and the private key (userkey.pm). The conversion can be performed with *openssl* tool:

```
openssl pkcs12 -nocerts -in mycert.p12 -out ~/.globus/userkey.pem
openssl pkcs12 -clcerts -nokeys -in mycert.p12 -out ~/.globus/usercert.pem
chmod 0400 ~/.globus/userkey.pem
chmod 0600 ~/.globus/usercert.pem
```

Of course replace mycert.p12 with the right filename. At end you should have something like:

```
[rossi@userinterface .globus]$ pwd
/home/rossi/.globus
[rossi@userinterface .globus]$ ll
total 8
-rw-----  1 rossi   rossi   2008 Nov 13 16:50 usercert.pem
-r-----  1 rossi   rossi   963 Nov 13 16:50 userkey.pem
```

Permission are *vital* not only for security: grid-proxy-init command will fail if your private key is not protected as listed.