Grid User Certificates

News

2020

GridKa denotes:

"Please be aware that from now on GridKa-CA certificates will be issued only on **Monday**, **Wednesday** and **Friday** afternoon."

Application is possible any time!

2019

The CA portal at GridKa now supports the Crypto-API of recent browser such as

- **Firefox** (from version 69)
- Microsoft Internet Explorer
- Chrome (from version 37)
- Safari (from version 10.1)
- Opera (from version 24)

- Konquerer and Microsoft Edge are **NOT** supported

See also GridKa News and GridKa FAQ.

Note

The Grid user certificate request procedure stores the private key (which **YOU AND ONLY YOU** possess) in the internal database of your browser. The private key **MUST NOT** get lost because it can not be recovered.

Please make sure that your *Firefox* browser is **NOT UPDATED** or reinstalled during the request/retrieval procedure!

Please **NEVER** ever spawn a **SECOND** request in the GridKa portal unless you are asked to do so!

Every new request generates work at GridKa because every single certificate request must be processed manually at a secure computer outside any network.

The DESY RA can be reached via grid-ra@desy.de.

Introduction

On order to access global Grid resources, users must hold a valid personal Grid user certificate (*authentication*) AND users must be member of a Virtual Organization (VO) (*authorization*).
A valid Grid user certificate is a prerequisite to request membership in a VO. Users usually have one Grid user certificate. Multiple VO membership is possible.

A Grid user certificate (format X509) consists of a *private* key with a private password and a certified *public* key. The private key and the password is exclusively possessed by the user and is NOT known to the *Registration Authority* (RA) or *Certification Authority* (CA) at any stage.

A certificate is valid for one (1) year and can be renewed. Users get notified by the CA via email three (3) weeks before the expiration date. It is strongly recommended to renew the certificate before its expiration.

The most frequent user issues for requests are:

1. The paper-based **DESY IDENTIFICATION FORM** has not been handed in yet (NOT needed for prolongations of certificates).
2. A non-working browser is used (*Konquerer* and *Microsoft Edge* are **NOT** supported).
3. Given and family **names** are not correctly filled.

A Grid user certificate can be seen as an analogy to a *passport*, whereas the VO membership compares to a *visa*.

If you observe **problems** to obtain a **proxy** via 'voms-proxy-init', inspect your certificate as described at the bottom of this pages.

Authorities

In Germany Grid user certificates are issued by the GermanGrid *Certification Authority* (**CA**) at GridKa in Karlsruhe. The GridKa CA is part of the The International Grid Trust Federation (IGTF) hence Grid user certificates are accepted by all Grid sites in WLCG. In order to facilitate the request procedure, many institutions in Germany operated R*egistration Authorities* (**RA**) which take over the necessary paper-work on behalf of the CA.

According to the GridKa policy, a user must be member (e.g. employee) of and located at the institute or university of which they request a Grid user certificate from (via the RA). This is necessary to contact users in case of security issues and to prove identity. This applies also for renewals. If the user changes group, institute or university, the new RA is in charge of approving certificates.

In the past the DESY RA approved Grid user certificate request also for guest scientist permanently located at DESY because their home institutions/countries did not have CAs. Since all institutions/countries do have CAs, please refer to The International Grid Trust Federation (ITGF) to find the relevant CA of your home institution.

Non-DESY users in Germany might find their responsible RA in the RA List of GridKa.

Users with non-German home institutions refer to ITGF.

Procedure

Step 0: Prerequisites (New request and renewal)

- You **must be** a member (registered employee and DESY email address) of DESY, the University of Hamburg (Campus Bahrenfeld), or the European XFEL. The support staff will check the DESY Identity and Access Management (IAM) system for your name.
- If this is not applicable, please request the certificate from your home institute; also students! The following procedure then will not apply to you.

Step 1: Paperwork at DESY (First request only)

For the FIRST certificate request at DESY ONLY!: We have to know you and your identity! Therefore you need to:

- Fill in the DESY IDENTIFICATION FORM and have it signed by your DESY group supervisor.
- (Only if you have changed our home institute or group - even within DESY or from DESY to U Hamburg or XFEL or vice-versa - we need a new ID-Form!)
- Send the form or hand it in personally (not by email) to UCO.
- You will NOT be notified of the arrival of the form, so immediately proceed to the next step.

Step 2: Electronic certificate request (First request and renewal)

This step is done electronically via browser, both for the first certificate request and for any subsequent renewals. For your name, please do not use capital letters only.

- Note: The procedure below has proven to work for **many recent browsers.** *Konquerer* and *Microsoft Edge* are **NOT** supported.
- Go to the GridKa CERT REQUEST PAGE.
- Make sure to fill in your DESY email address (see example below).
- Make sure to fill in the right institute (Organization: DESY, U Hamburg or XFEL).

Final steps (First request and renewal)

- Once we have confirmed your identity (first request only), and you have requested a certificate to GridKa, the DESY Registration Authority will either accept or reject this request. You will be notified by email about the approval or disapproval of your request. **No action from your side is requested at that point**.
- Once the DESY Registration Authority has accepted the request, the Certification Authority (CA) at GridKa will proceed and sign your certificate request. You will then be contacted once your certificate is **ready for retrieval**.
- Follow the instructions contained in your notification email. Note: **Use the browser used for the certificate request**.
- You can now use the certificate to authenticate against web servers. For job submission or data management, you must convert your certificate and store it under the $HOME/.globus/ directory. Consult the GridKa help page [in German

Please use a **DESY email address** (first.last@desy.de)!

Please use a recent browser. *Konquerer* and *Microsoft Edge* are **NOT** supported. See GridKa FAQ.

Please **do NOT send copies of your passport and/or ID card around.**
Identification of users is carried out by the group admins who are supposed to authorize requests of their group members by checking ID cards and denoting the last digits of the ID number on the registration form (see below).

Please **do not issue a second certificate request** in the GridKa portal unless you are asked to do so, e.g. because your request is erroneous.

In case you **extend** your certificate please make sure you **chose the same DN**, as the current one is probably already registered with a VO. A changed DN requires to re-register with the VO(s).

Links

- GridKa
- The International Grid Trust Federation (ITGF)

- GridKa FAQ
- GermanGrid policy
- RA List of GrmanGrid
- DESY group supervisor
- namespace supervisor
- UCO

- DESY IDENTIFICATION FORM
- GridKa CERT REQUEST PAGE

/ in English], especially *Exporting certificates from your browser* and *Converting certificates and keys*.

Robot Certificates

For some special cases such as regularly running services, which need authentication/authorization though proxies, a so-called robot certificate can be used. This is clearly a non-standard case for experts only!

Robot certificates can be requested via the GridKa portal as 'Host/ Service/ Robot Zertifikate' by a user. Make sure they contain the word 'Robot' in the CN, e.g.:

```
/C=DE/O=GermanGrid/OU=DESY/CN=Robot: blablabla
```

Technicalities

Technically a new private/public key pair is created with every renewal.

Finding certificates in Firefox browser

```
Preferences -> Privacy & Security -> Certificates -> View Certificates -> Your Certificates (-> Backup)
```

Inspecting Grid user certificates

Please make sure your public (usercert.pem) and private (userkey.pem) keys are:

- in the correct directory,
- have the correct permissions,
- show your DN,
- are valid,
- match each other (have the same md5sum),
- your remember the password.

```
 > cd ~/.globus

 > ls -l ~/.globus
-r--r--r-- 1 xxx yyy  1728  8. Apr 09:36
usercert.pem
-r-------- 1 xxx yyy  2012  8. Apr 09:36 userkey.
pem

 > openssl x509 -subject -issuer -dates -noout -
in usercert.pem
subject= /C=DE/O=GermanGrid/OU=DESY/CN=NNNN
issuer= /C=DE/O=GermanGrid/CN=GridKa-CA
notBefore=Mar 29 16:32:00 2019 GMT
notAfter=Apr 27 16:32:00 2020 GMT

 > openssl x509 -noout -modulus -in usercert.pem
| openssl md5
 > openssl rsa -noout -modulus -in userkey.pem |
openssl md5
```

- X509
- GridKa help
- Exporting certificates from your browser

The **private** key is created by the browser when the request is issued on the GridKa portal page and is therefore stored in that particular browser. Hence the certified public key must be retrieved from GridKa with the same browser which was used for the request.

A lost private/public keys or the password can not be recovered by any means by the CA or RA.

Known issues

- Make sure to export the certificate from the browser you requested and retrieved it with in as 'usercert.p12'.
- Make sure you remember the pass-phrase for the key and for the export.
- Make sure your have 'usercert.pem' and 'userkey.pem' in the direcory ~/.globus/
- Make sure the access permissions to 'usercert.pem' and 'userkey.pem' are correct.

- We found that a cert did now work with 'voms-proxy-init' although everything had been checked. Only a new extraction from the exported cert 'usercert.p12' helped.