Instructions for requesting personal and host certificates

Introduction

The Grid utilizes public key or asymmetric cryptography for authentication of users and services. According to the basics of public-key cryptography, each resources on the Grid has a key pair, a public and a private key. The public key is made public while the private key must be kept secret. Encryption and authorization is performed using the public key while decryption and digital signature is performed with the private key. It is important to notice that generating a key pair does not automatically provide you access to the Grid resources. A trusted authority of the Grid, called the Certificate Authority (CA) needs to sign your key pair this way confirming your identity. This signing procedure of the CA is often referred as issuing a certificate.

In the Grid era the key file (userkey.pem) and the certificate file (usercert.pem) correspond to the key pair of the public-key cryptography. The userkey.pem file (or resourcekey.pem) contains the private key encrypted with your password (called pass phrase by some tools). The certificate file (usercert.pem) contains your public key together with additional important informations such as the subject name of the holder of the certificate, the name of the signing CA, and the digital signature of the CA. The important role of the CA is to establish a trustful connection between the identity of the user and the public key in the certificate file. The digital signature of the CA in the user's certificate file officially declares that the public key in the file belongs to the specific user (subject name). The certificate files are encoded with the x.509 format.

In order to obtain a valid "passport" to the Grid you need to create a key pair and submit your public key to the CA (this process is called as a certificate request) for a signature. The CA will follow its certificate policy and upon successful evaluation of your request your public key will be signed and posted back to you. As it was mentioned before all resources (i.e. gatekeepers, users, services) require a CA-signed key pair to be able to operate on the Grid. "Grid passport" (credentials) consists of two files, the private key file called by default userkey.pem and the public certificate file usercert.pem; you need to have both of them. The certificate file (usercert.pem) alone is not enough for the Grid. If you lose one of your credential files, you'd need to request a new certificate. File names can be changed, and most client tools can operate with arbitrary credential file names.

Grid host certificates and long lived grid user certificates both have a duration of a year. These certificates are issued by TSU Certification Authority (CA), which is accredited by EuGridPMA. Grid server certificates are needed by a tipical machine in a grid environment using middlewares such as gLite or EMI.

Long lived grid user certificates instead allow users to utilize grid resources, or access grid portals (e.g. the GOCDB in the WLCG collaboration) by uploading their grid certificate into the browser.

Below the commands for generating key pair and Certificate Request for the user using OpenSSL software are given. OpenSSL software is included in modern UNIX-like OS distributions.

This document describes the steps, which have to be done in order to request personal or host certificates from TSU CA. It is based on the TSU CA Certificate Policy and Certification Practice Statement (CP/CPS) document available at http://grid-ca.tsu.ge

Openssl

Secure Sockets Layer is an application-level protocol which was developed by the Netscape Corporation for the purpose of transmitting sensitive information, such as Credit Card details, via the Internet. SSL works by using a private key to encrypt data transferred over the SSL-enabled connection, thus thwarting eavesdropping of the information. The most popular use of SSL is in conjunction with web browsing (using the HTTP protocol), but many network applications can benefit from using SSL. By convention, URLs that require an SSL connection start with https: instead of http:.

X.509 is a specification for digital certificates published by the International Telecommunications Union - Telecommunication (ITU-T). It specifies information and attributes required for the identification of a person or a computer system, and is used for secure management and distribution of digitally signed certificates across secure Internet networks. OpenSSL most commonly uses X.509 certificates.

User certificate

A GRID user certificate is issued by a Certificate Authority (CA) which checks the identity of the user and guarantees that the holder of this certificate is existing and his certificate is valid. The user certificate is used for authentication instead of the user's account to avoid the replication of the user's account to all GRID sites. When authenticating to a site, the user's certificate is mapped to a local account under which all commands are executed. The certificate itself is not used during the actual GRID usage. All GRID jobs use a proxy of the certificate with a limited lifetime. This enhances security because the user has to re-establish the validity of his certificate after the lifetime of the proxy has ended. The proxy generation has to be repeated every time no valid proxy exists on the user's submission machine.

Generate user certificate request

1. Create a directory in the user's home directory:
   ```
   mkdir  ~/.globus
   cd ~/.globus
   ```
2. generate 2048-bit key pair and Certificate Request:
   ```
   openssl req -newkey rsa:2048 -sha256 -subj "/DC=GE/DC=TSU/O=People/O=Your Company/CN=Common Name" -out usercert_request.pem
   ```
3. Replace *“Your Company”* with full name of your company and *“Common Name”* with your name and surname.

You will be asked for passphrase to secure your private key.(For security reasons, an empty passphrase is not advisable)

4. Verify that the subject DN in the certificate request starts with "/DC=GE/DC=TSU/O=People/": check the output of
   ```
   openssl req -subject -noout -in usercert_request.pem
   ```
5. Copy the usercert_request.pem file to the USB flash or CD/DVD
6. Prepare following documents and data:
   - Your passport,
   - Official document from your organisation proving your relations with the organisation, signed and stamped by an official representative of the organisation.
   - Your work e-mail address and personal phone number
7. Register and login at http://grid-ca.tsu.ge web portal, upload usercert_request.pem using “Upload request file” under “User certificate menu”.

Installation of the user certificate

After the successful application, the certificate has to be installed in the user's home directory following these instructions:

1. After receiving usercert.pem file copy to ~/.globus directory.
   ```
   cp usercert.pem ~/.globus
   ```
2. Change directory to user's home directory:
   ```
   cd ~/.globus
   ```
3. Set the access mode on your userkey.pem and usercert.pem files:
   ```
   chmod 400 userkey.pem
   chmod 600 usercert.pem.
   ```
4. Further protection of the $HOME/.globus directory is necessary to prevent everyone except the user to enter this directory:
   ```
   chmod go-rx ~/.globus
   ```
5. Using your private key and certificate, you have to generate the user certificate in pkcs#12 format (Web browsers certificate format), which is used for signing the message:
   ```
   openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out usercert.p12
   ```
   You will be asked for two passphrase: the passphrase of the private key, which was set when generating the key pair and the passphrase for creating pkcs#12 file. For security reasons, an empty passphrase is not adviseable.
6. Import this certificate into web browser(IE, Firefox) or mail client(Thunderbird).

The user's GRID certificate (usercert.pem and userkey.pem) can be copied to every other machine to access the GRID by transporting the $HOME/.globus directory. The security measures described above have to be repeated.

Create a host Certificate Request

The host certificate can only be requested by the administrator who must already have a valid user certificate. The directory for the Grid host certificates is usually /etc/grid-security.

```
openssl req -newkey rsa:2048 -sha256 -nodes -subj "/DC=GE/DC=TSU/O=Hosts/O=Your Company/CN=Common Name" -out hostcert_request.pem
```

1. Replace "*Your Company"* with full name of your company and *"Common Name"* with DNS FQDN of the host.
2. Verify that the subject DN in the certificate request starts with "/DC=GE/DC=TSU/O=Hosts/": check the output of

   ```
   openssl req -subject -noout -in hostcert_request.pem
   ```

3. Login at http://grid-ca.tsu.ge web portal, upload hostcert_request.pem using "Upload request file" under "Host certificate menu".

Installation of the host certificate

After the successful application, the certificate has to be installed in the /etc/grid-security directory following these instructions:

1. After receiving hostcert.pem file copy to /etc/grid-security directory.

   ```
   cp hostcert.pem  /etc/grid-security
   ```

2. Set the access mode on your userkey.pem and usercert.pem files:

   ```
   chmod 400 /etc/grid-security/hostkey.pem
   chmod 600 /etc/grid-security/hostcert.pem
   ```