Table of Contents

Request new Host Certificates

This procedure allows you to request host certificates for Cern nodes **without** need to change the *owner* or the *main user* of the machine in the LAN db. In order to do this, the webservice of the CA is invoked via a **service account** trusted by the CA, under the responsibility of the GD group.

People holding the password of this account are allowed to request host certificates for **every** node at CERN (even those which they don't manage).

So it is extremely important not to disclose that password to people not accounted by the GD group to perform this particular action.

The script *host-certificate-manager*, produced by FIO, is used to interface with the CE webservice through the trusted account **gdadmin**.

The script is available in cvs in

http://isscvs.cern.ch/cgi-bin/cvsweb.cgi/fabric/CERN-CC-host-certificate-manager/?cvsroot=fio

A working copy of the script (version 1.12) has been made available in the yaim-server directory

E.g. , a simple way to apply for a certificate is to log in lxplus and run

- `cd /afs/cern.ch/project/gd/yaim-server/`
- `./host-certificate-manager --from=EMAIL_ADDRESS --username=gdadmin --nosindes --dir ~ HOSTNAME.cern.ch`

OR

- = /usr/bin/host-certificate-manager --from=EMAIL_ADDRESS --username=gdadmin --nosindes --dir ~ HOSTNAME= (**without .cern.ch** !!!)

- Notifications about expiration of the certificate will be sent to the provided e-mail address. So it would be preferable to use an appropriate mailing list. E.g.

Context	EMAIL_ADDRESS
Production	it-dep-gd-gmod@cernNOSPAMPLEASE.ch
PPS	grid-cern-pps-admins@cernNOSPAMPLEASE.ch
Certification	project-lcg-deployment-bitface@cernNOSPAMPLEASE.ch

- The Nice password of the *gdadmin* account is required.

- The certificates and keys will be stored in a temporary directory :-(.

- A destination directory for the certificates can be specified using the option `--dir=PATH`

- The `--nosindes` option is used not upload the certificate in SINDES (eventually to be changed)

- Bulk requests for several machine can be done using a particualr syntax fro the HOSTNAME string : e.g. the string `lxdev03,lxplus0[01,09-12]` will be expanded in an array containing the nodes `(lxdev03 lxplus001 lxplus009 lxplus010 lxplus011 lxplus012)`

- Remember to set the correct permissions for the certificates, specifically

- `> chmod 400 hostkey.pem`

- Some documentation can be found as text comments in the script.

How to check the certificate in "clear" text

```
openssl x509 -text -in hostcert.pem
```

-- Main.aretico - 01 Dec 2006

This topic: LCG > GDReqHostCert
Topic revision: r10 - 2007-07-17 - AntonioRetico