Table of Contents

Procedures

Shortly speaking all the services that are going to communicate inside the GRID need a certificate to authenticate themselves. In order for this certificate to be recognized as a valid one for a proper communication it should pass 3 steps:

1. Initially issued from a CA (Certificate Authority) recognized as a valid one in the GRID
2. Registered in the proper VO that is going to use it.
3. Mapped to a User recognized inside the VO (mapped to its primary account)

Notes

Here follows some notes related to the CRAB3 certificates and the above three steps:

Common Notes:

1. **Services that need authenticated communication (more precisely with CMSWEB):**

- In the Schedds:
  - WMArchiveUploader
  - Overflow
- In the TaskWorker:
  - Taskworker
- In the CrabServer
  - CrabServer
  - CRabCache
  - Frontend

2. **Standard place for hosting these certificates:**

```
/data/certs/
```

While being there the certificates (and also the directory containing them) must be owned by the proper user that is going to run the service using the certificate:

- for the TaskWorker crab3:root
- for the CrabServer crab3:root
- for the Schedds condor:root

Once you create this directory during the deployment process of the relevant machine please do the following:

```
chown <user>:root -R /data/certs
chmod 700 /data/certs
chmod 400 /data/certs/*key*.pem
chmod 440 /data/certs/*cert*.pem
```

- Exceptions:

1. Crabserver:

Copy the certificates/keys also to:

```
cp /data/certs/servicecert.pem /data/srv/current/auth/crabserver/dmwm-service-cert.pem
cp /data/certs/servicekey.pem /data/srv/current/auth/crabserver/dmwm-service-key.pem
chown _sw:_config /data/srv/current/auth/crabserver/dmwm-service*.pem
chmod  400 /data/srv/current/auth/crabserver/*key*.pem
chmod  440 /data/srv/current/auth/crabserver/*cert*.pem
```

Notes about the Procedures:

1. **Initial issuing:**

While following the steps described in [1] please work directly on the machine that is going to use the certificate (in such a way the private key generated for the request will never leave the machine).

And also please:

- Keep your work at one place, preferably at:

```
/root/ssl-valid.d/
```

Keep there only the currently valid certificates (this place can also be used as a backup storage of the currently valid certificate) - all the rest (old) certs/keys please move to:

```
/root/ssl-old.d/
```

After finishing the procedure please protect the backups in a way that they could be accessed only by root:

```
chown root:root -R /root/ssl-valid.d/
chmod 000 -R /root/ssl-valid.d/
```

- Add the proper service name in front of the hostname:

```
<service>/<hostname>
```

For example:

```
schedd/vocms059.cern.ch
tw/vocms052.cern.ch
crabserver/vocms035.cern.ch
```

- Add the proper SAN (Subject Alternative Name) using the naming schema described here [5]. Because the SAN will enter inside the certificate as a proper DNS record it should not contain symbols like '/' but the standard is not very clear about that [6] so just to be on the safe side add them both (with and without the service in front of the alias) as a comma separeted list. For example:

```
crab-dev-tw01.cern.ch, tw/crab-dev-tw01.cern.ch
```

After finishing the procedure the end certificate should contain the additional fields (extensions) related to the DNS aliases you have created earlier:

```
X509v3 extensions:
       X509v3 Key Usage: critical
           Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
            DNS:crab-dev-tw01.cern.ch, DNS:tw/crab-dev-tw01.cern.ch, DNS:vocms058.cern.ch
```

2. **Registration with the VO**

- Please contact Stefano Belforte as described in [3].
- You can check if the DN from the certificate is registered in the VO at: [2].

3. **Mapping to a user primary account:** This process is happening in SiteDB in order for the certificate to be mapped correctly.

- Please contact Stephan Lamel and send him the DN of the certificate and a decent description about what is this certificate and what is it going to be used for.
- You can check if the DN from the certificate is mapped to any account in [4].

Notes about Puppet management:

- Currently we still use the manual procedure for the initial issuing of the service certificates because of lac of a solution to this one: [7].
- For the renew process is used the 'certmgr' puppet module provided by CERNIT. Once the certificate is in the proper place it is expected that the next year it should be renewed automatically. But since [7] is not finally resolved it is strongly recommended to keep track about errors in in the `puppet reports` in [8] at around the moment when the certificates are going to expire. There should be one and only one error message that tells that the certificate could not be renewed because of a server error and after that it will not try again and silently fail. If we miss this error event though we will have at east one month left from the certificate lifetime we will still fail to update it on time. the error message in the puppet report will look something like this:

```
Notice: /Stage[main]/Hg_vocmsglidein::Profiles::Crabtaskworker/Certmgr::Certificate[tw/vocms0118.
Error: /Stage[main]/Hg_vocmsglidein::Profiles::Crabtaskworker/Certmgr::Certificate[tw/vocms0118.c
Error: /Stage[main]/Hg_vocmsglidein::Profiles::Crabtaskworker/Certmgr::Certificate[tw/vocms0118.c
```

[1] https://ca.cern.ch/ca/host/Request.aspx?template=ee2host

[2] https://voms2.cern.ch:8443/voms/cms/user/search.action

[3] https://twiki.cern.ch/twiki/bin/view/CMSPublic/CompOpsGlideinWMSCerts

[4] https://cmsweb.cern.ch/sitedb/prod/people

[5] https://twiki.cern.ch/twiki/bin/view/CMSPublic/Crab3BackendDeployment#Crab3Aliases

[6] https://www.ietf.org/rfc/rfc5280.txt

[7] https://cern.service-now.com/service-portal/view-incident.do?n=INC1420946

[8] https://judy.cern.ch/hosts?utf8=%E2%9C%93&search=vocmsglidein%2Fcrab

Useful links:

[9] https://twiki.cern.ch/twiki/bin/viewauth/CMS/SiteDBForCRAB

[10] https://twiki.cern.ch/twiki/bin/view/CMSPublic/SWGuideVomsFAQ

-- TodorTrendafilovIvanov - 2017-08-30

This topic: CMSPublic > NotesAboutServiceCertificateManagement
Topic revision: r2 - 2018-12-06 - TodorTrendafilovIvanov