D4Science Infrastructure - Task #1273

Check CA hierachy of GARR certificates issued by TERENA to create a truststore to add to production nodes

Oct 29, 2015 04:57 PM - Luca Frosini

Status:	Closed	**Start date:**	Oct 29, 2015
Priority:	Urgent	**Due date:**	Oct 30, 2015
Assignee:	Luca Frosini	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	CouchDB Deployment		
Infrastructure:	Pre-Production, Production		

Description

The hierarchy can be found here:
http://pki.cesnet.cz/en/ch-tcs-ssl-ca-2-crt-crl.html

TERENA certificate can be found here:
http://crt.tcs.terena.org/TERENASSLCA.crt

History

#1 - Oct 29, 2015 04:59 PM - Luca Frosini

- Priority changed from Normal to Urgent

#2 - Oct 29, 2015 04:59 PM - Luca Frosini

- Status changed from New to In Progress

#3 - Oct 29, 2015 05:17 PM - Andrea Dell'Amico

I just discovered that we already had an incident about the Terena CA certificate. But at that time I didn't know that the GARR got the certificates from them: see #414. When we'll have the needed hierarchy sorted out we shall need a new keyring for all the java services involved.

#4 - Oct 29, 2015 05:21 PM - Luca Frosini

Using the right username and password I successfully created a db using https like this:

```
$ HOST=https://XXXX:XXXX@accounting-d4s.d4science.org
curl --cacert ./chain_TERENA_SSL_CA_2.pem -X PUT $HOST/aux
```

I got the pem certificate from here
https://pki.cesnet.cz/certs/chain_TERENA_SSL_CA_2.pem

Further details can be found here
http://pki.cesnet.cz/en/ch-tcs-ssl-ca-2-crt-crl.html

#5 - Oct 29, 2015 05:27 PM - Luca Frosini

- File chain_TERENA_SSL_CA_2.pem added

- Status changed from In Progress to Feedback

- % Done changed from 0 to 90

I also tried successfully to remove the **AddTrust External CA Root** from pem.
So the only certificates needed to trust are this one:
https://pki.cesnet.cz/certs/USERTrust_RSA_Certification_Authority.pem
https://pki.cesnet.cz/certs/TERENA_SSL_CA_2.pem

The global pem I edited is available as attachment

#6 - Oct 29, 2015 05:27 PM - Luca Frosini

- Due date set to Oct 30, 2015

#7 - Oct 29, 2015 05:51 PM - Andrea Dell'Amico

I just changed the certificates configuration on haproxy server to add the certificates needed to complete the trust chain.
Now curl connects successfully.

#8 - Oct 30, 2015 10:42 AM - Luca Frosini

I confirm that curl works perfectly.
I'm going to test java code.

#9 - Oct 30, 2015 12:32 PM - Luca Frosini

- Status changed from Feedback to Closed

Java code works too.
I'm going to close the ticket

#10 - Nov 19, 2015 12:34 PM - Luca Frosini

- % Done changed from 90 to 100

Files

chain_TERENA_SSL_CA_2.pem	4.17 KB	Oct 29, 2015	Luca Frosini