Certificate Authorization Problems in GIN (Grid Interoperability Now)

Oscar Koeroo

24th April 2006

This document summarizes the chain of events for this specific problem with the VOMS Server. It is most likely that other services can lack the same problem. It is written in my personal perspective as the VOMS Administrator for GIN.

Involved people:

- Cindy Zheng
- Vincenzo Ciaschini
- Oscar Koeroo

1 Intro

The VOMS server for the GIN effort is kuiken.nikhef.nl and it supports the 'gin.ggf.org' VO. The name is in the new style to avoid nameclashes in the world. Cindy Zheng is one of the first to register with the Virtual Organization Membership Service (VOMS) server through the VOMS Admin HTTPS web-interface. The first experience was not to be allowed to register herself through the web-interface. The glite-trustmanager refused the connection to the secured Tomcat web-interface because the certificate was signed by a non-trusted CA and thus authentication failed.

2 Trusting the certificate

The VOMS server is setup to trust all IGTF member CAs. The certificate she uses was signed by a CA outside of the International Grid Trust Federation (IGTF). The VOMS server needed to support Cindy's CA (/C=US/O=SDSC/OU=SDSC-CA/CN=Certificate Authority/UID=certman). The VOMS Administrator has added the CA to the trusted CAs on the VOMS server to help the GIN effort on this 'minor' problem. On the trusting party (the VOMS server) the SDSC CA is labeled as *volitile* because the policy they apply is unknown and their not an IGTF member (which conflicts with a local policy to follow only IGTF accredited CAs). Therefor only selected people may register to the VOMS server using a certificate signed by this CA. Others will not (easily) be granted access to the service using that particulaire CA. After the installation of the CA files (public cert, crl, signing_policy and creating the crl_url file, plus testing fetch-crl with it) the VOMS Admin 'check-for-new-CAs' daemon installed the SDSC CA into the CA. This proces was succesfull and is needed to register new users with this CA.

Cindy registered succesfully with her certificate to the 'gin.ggf.org' VO with the use of VOMS Admin with the following credentials:

Distinghuished Name (DN) /C=US/O=SDSC/OU=SDSC/CN=Cindy Zheng/USERID=zhengc

Certificate Authority (CA) /C=US/O=SDSC/OU=SDSC-CA/CN=Certificate Authority/USERID=certman

Her DN appeared in a grid-mapfile when executing the mkgridmap tool with the use of the 'gin.ggf.org' configuration details.

3 The problem

When Cindy tryed to execute "voms-proxy-init -voms gin.ggf.org" it failed. This command will contact the VOMS server though GSI interface of the vomsd or VOMS daemon. This daemon is responsible for creating a list of Attribute Certificates (ACs).

After putting the logs on paranoid, Vincenzo (VOMS daemon developer) and I could conclude the problem being in the database query on the parts of the UID or USERID in the DN. A DN is queried twice, once to match her delegated proxy with /UID and once with /USERID to select the correct group and role list within the VO. These RDNs are standardized (RFC 2253) on UID but a lot of code is still displaying this tag (DNs are represented as string by parsing the ASN.1 sequences of which it is constructed and concatinating them together).

The VOMS daemon didn't twin query the CA's DN, once with /UID and once with /USERID. This made the authorization fail on the database query not getting any results/

4 The hack

We (Vincenzo and I) hacked the database to change the substring from USERID to UID in the CA record to let the match succeed. This solved Cindy's disability to execute 'voms-proxy-init -voms gin.ggf.org'.

5 To conclude

The VOMS Admin uses the old style ASN.1 to string convergence for this RDN. The VOMS daemon generally produced the standard style representation. To solve the inconsitancy Vincenzo will apply a patch to the vomsd code in a next release which will execute the twin query for the CA certificates as it does for the user certificates, thus supporting either representations. It was a surprise to us that UID/USERID was used in the CA's DN. It will be wise to ban the use of such ambiguise RDNs in DNs at large and as a CA to follow the recommendations of the IGTF to overcome these impracticalities. Within the GIN effort it must stressed to only make use of the CAs within the IGTF.

The same wisdom should be applied for the Email/emailAddress, SN/serialNumber (for which SN can also be surname) and other ambiguise RDNs used for DNs. The biggest problem is the interpretation of the RDNs by different pieces of software. Software like OpenSSL constructs humanly readable strings out of the RDNs which are concatinated to form the whole DN. That end-result can be differently interpreted between software version due to changes and/or decissions over time and create such problems. I would strongly encourage test and checks of all interoperating software to be compliant with the standards of today. That will be the only good way to avoid inconsistent comparisons of such interpreted strings.