VOMS architecture

Emidio Giorgio

Slides by Valerio Venturi, Vincenzo Ciaschini

INFN

Retreat between GILDA and ESR on gLite, Bratislava, 27-30.06.2005

Summary

- **Basic concepts**
  - GSI
- **VOMS**
  - Concepts
  - Architecture
  - Components

GSI

- Grid Security Infrastucture uses the Globus Toolkit for the purpose of authentication and authorization.

GSI – requirements (1)

- Single sign-on.
  - The user should not be required to repeat login procedures on the grid more than once.
- Delegation.
  - Once a user has successfully identified himself with the Grid, it should be possible for grid services to act on the behalf of the user as if they were the user himself.
- User-based trust relationship.
  - All trust mechanism should have the user's credential at their core.
    - If a user wants to access farms A and B, there should be no need for farms A and B to trust each other.
- The user's credential should be adequately protected.
  - Private data (keys, passwords, etc…) should not circulate on the net.

GSI – requirements (2)

- Integrated with local systems.
  - The grid security mechanism should not supplant the local authorization mechanism, but instead work on top of it.
- Simple to use.
  - The system should be simple enough on the user's side as not to require excessive preparations before real work could begin.
- The system used should employ well defined standards to permit multiple implementation

GSI – solution (1)

- X.509 certificates:
  - An ISO and IETF standard that ties public key credentials (public and private keys) to an identity.
  - Certificates are issued by a set of well-defined Certification Authorities (CAs).
  - Credentials are divided in two parts:
    - The public part in the certificate, supposed to be shared.
    - The private part, that must be kept secret by the user.
- PKI:
  - Public Key Infrastructure.
  - A set of IETF standards that define how the certificates and CAs must work together.

GSI – solutions (2)

- GSS-API:
  - An IETF standard that defines a unified interface to heterogeneous security mechanisms (Kerberos, X.509 certificates, etc…).
  - Generic Security Services Application Program Interface.
- GSI:
  - Globus Security Infrastructure.
  - Ties together the other three components.
  - Adds the capabilities of credentials delegation.
  - Defined in a set of documents on the Globus site (http://www.globus.org)

X.509 certificates

- A sample certificate

[venturi@pre-ui-01 venturi]$ openssl x509 –in /tmp/x509_up501 –text –noout

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1148 (0x47c)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=IT, O=INFN, CN=INFN Certification Authority

Validity

Not Before: Jan 31 13:29:07 2003 GMT

Not After : Jan 31 13:29:07 2004 GMT

Subject: C=IT, O=INFN, OU=Personal Certificate, L=CNAF, CN=Vincenzo Ciaschini/Email=Vincenzo.Ciaschini@cnaf.infn.it

……..

Signature Algorithm: md5WithRSAEncryption

Signature: …

- Once you know where it is located (normally in /tmp/x509_up<userid>) you can use openssl x509 command to read it as above.
The –noout option prevent openssl from showing the real data

-----BEGIN CERTIFICATE-----

MIIFXzCCBEegAwIBAgICBHwwDQYJKoZIhvcNAQEEBQAwQzELMAkGA1UEBhMCSVQx

DTALBgNVBAoTBElORk4xJTAjBgNVBAMTHElORk4gQ2VydGlmaWNhdGlvbiBBdXRo

b3JpdHkwHhcNMDMwMTMxMTMyOTA3WhcNMDQwMTMxMTMyOTA3WjCBlzELMAkGA1UE

BhMCSVQxDTALBgNVBAoTBElORk4xHTAbBgNVBAsTFFBlcnNvbmFsIENlcnRpZmlj

Proxy certificates

- Introduced by the Globus Toolkit
- Are used for delegating of credentials based on single sign-on
  - A new certificate (the proxy) is created, based on the user certificate
  - The user certificate never travels on the net, thus remaining secure
  - It's the proxy certificate that travels across the grid
    - The proxy certificate contains is private key, thus addressing the problem of single sign on and delegation (grid services can act on behalf of the user)
    - The proxy certificate is (should be) short lived (normally 12 hours), thus reducing the damage of stolen it

Proxy certificates

- A proxy certificate is an X.509 certificate, so you can read it the same as X.509 with openssl x509 command but
  - The Issuer is the user instead of a CA
  - The subject contains “Proxy” in the CN
    - actually, this is true for old proxy (GT < 2.2), while RFC 3820 compliant proxy differs from the user in
      - The DN contains a unique identificative for the user
      - The certificate contains a critical extension (Proxy Certifcate Info extension)

Local authorization

- Based on matching of the DN on a list of accepted users (grid-mapfile).
- Very coarse grained authorization
  - Remote users are mapped directly to UNIX users.
  - Classification of users into categories must be done on a local farm basis without input from the VO (may result in the same user having very different privileges in different farms).
  - No support for groups or roles
  - Grid-mapfile authorization is not flexible.

VOMS

- Virtual Organization Membership Service (VOMS) is a service that keeps track of the members of a VO and grants users authorization to access the resource at VO level, providing support for group membership, roles (e.g. administrator, sofware manager, student) and capabilities.
- Support for it is integrated in most of the grid services.

VOMS - requirements

- Provide a secure system for VO to organize the user in groups and/or roles and to disseminate this information
- User should be able to decide which information wants to publish
- Compatibility with Globus Toolkit

VOMS - solution

- Each VO has its own server(s) containing groups membership, roles and capabilities informations for each member
- User contact the server requesting his authorization info
- The server send the authorization info to the client
- The client include it in a proxy certificate

FQAN

- short for Fully Qualified Attribute Name, is what VOMS uses to express membership and other authorization info
- Groups membership, roles and capabilities may be expressed in a format that bounds them together <group>/Role=[<role>][/Capability=<capability>]

```
[venturi@pre-ui-01 venturi]$ voms-proxy-info -fqan
/testVO/Role=NULL/Capability=NULL

[venturi@pre-ui-01 venturi]$ voms-proxy-info -fqan
/testVO/Role=VO-Admin/Capability=NULL

[venturi@pre-ui-01 venturi]$ voms-proxy-info -fqan
/testVO/Role=SoftwareManager/Capability=NULL
```

- FQAN are included in an Attribute Certificate

AC - Attribute Certificate

- Defined in RFC 3281
- Attribute Certificates are used to bind a set of attributes (like membership, roles, authorization info etc) with an identity
- AC are digitally signed

VOMS and AC

- VOMS uses AC to include the attributes of a user in a proxy certificate
- The server creates and sign an AC containing the FQAN of the user (or better the FQAN requested by the user, when applicable)
- The client include this AC in the proxy certificate
  - **The AC is included in a well-defined non critical extension**
    assuring compatibility with GT-based mechanism
  - At the resource level, the authorization info is extracted from the proxy and processed by the local site

VOMS - operations

1. Mutual authentication beetween client and server via GSI.
2. The client send a request to the server.
3. The server check the correctness of the request.
4. The server send back the required info (in FQAN format) included in an Attribute Certificate.
5. The client check the consistency and validity of the information returned.
6. Step 1-5 may be repeated for any number of servers.
7. The client create a proxy that includes the info returned by the server in a non critical extension.
8. The client may add user-supplied information.

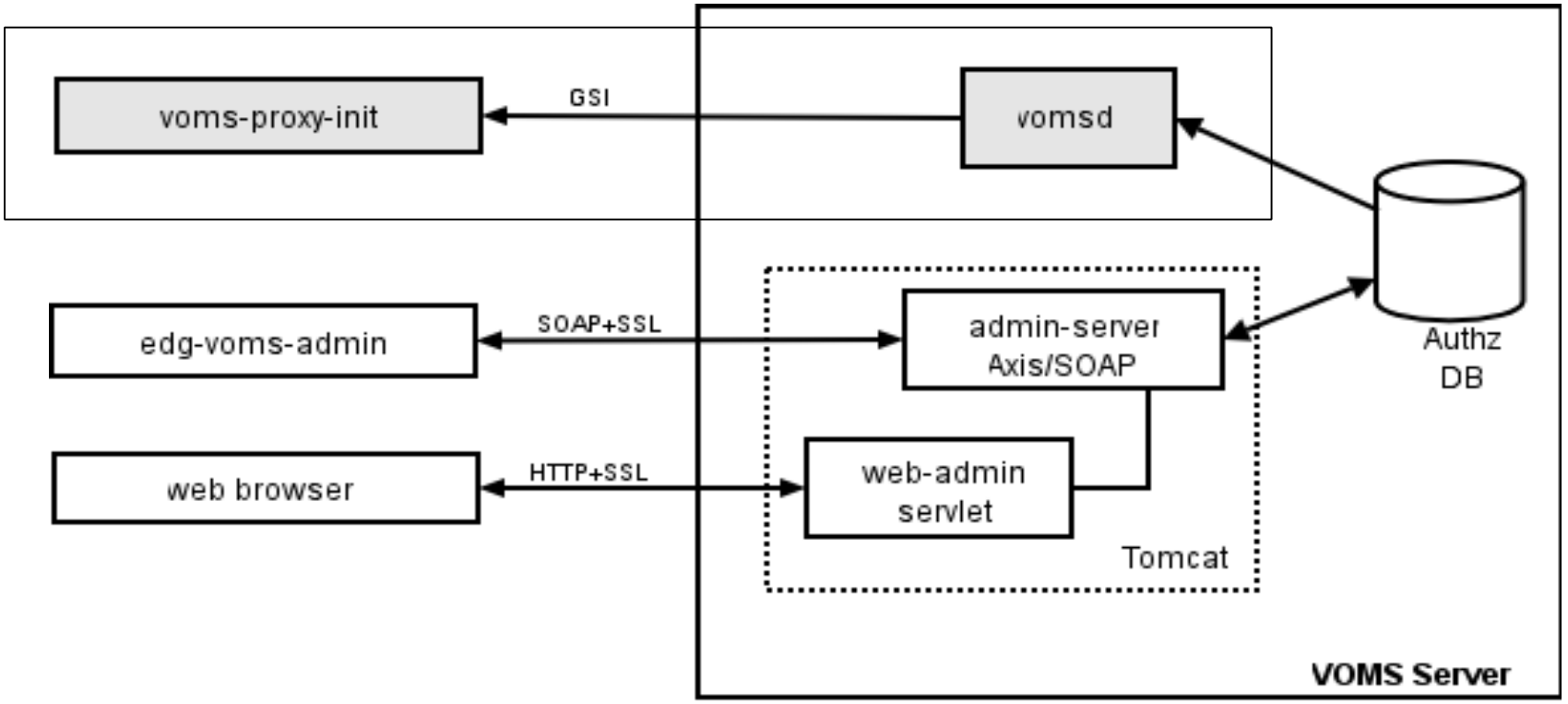
VOMS - administration

- What VO Managers uses to manage the authorization info for the users of a VO.
- Web interface and command line client are available.
- A user connect with a browser (having a certificate) to a page and submit a requests. VO Manager accept or refuse that request.
- VO Manager have the command line utilities to modify the info for a user.

VOMS - components

- VOMS Core Services
  - Server - return authorization info to the client.
  - Client applications
    - voms-proxy-init
      queries the server for authorization info and create a proxy certificate including it.
    - voms-proxy-info
      shows the info included in a proxy.
    - voms-proxy-destroy.
- VOMS Admin
  Used by VO administrator for management of membership, roles and capabilities in a VO.

VOMS - components



- Authz DB is a RDBMS (currently MySQL and Oracle are supported).

VOMS Core Services– software status

- Two CVS repository
  - The main is at: http://infnforge.cnaf.infn.it/cgi-bin/cvsweb.cgi/voms/?cvsroot=voms
  - The gLite one is at http://jra1mw.cvs.cern.ch:8180/cgi-bin/jra1mw.cgi/org.glite.security.voms
- Releases
  - 1.3.7 in LCG 2.4.0
  - 1.2.32 in gLite 1.1 (1.5.4 is release candidate for 1.2)
  - 1.4.2 in VDT 1.3.6
- Version mismatches are due to projects release rules, no compatibility issues are present between this release (due to Oracle support, different configuration for the VOMS server are needed starting from 1.5.1).

VOMS Admin – software status

- CVS repository at http://jra1mw.cvs.cern.ch:8180/cgi-bin/jra1mw.cgi/
- Releases
  - 0.7.6 in LCG 2.4.0
  - 1.0.5 in gLite 1.1

voms-proxy-init - configuration

- voms-proxy-init get information on the server to contact by files located in $GLITE_LOCATION/etc/vomses (system-wide) or $HOME/.glite/vomses (user-specific). This location could be overwritten specifying –userconf and –confile options. In case they are directories, all the files within are scanned.
- A vomses file look like this:

```
[venturi@pre-ui-01 venturi]$ cat /opt/glite/etc/vomses
"infngrid" "cert-voms-01.cnaf.infn.it" "15002" "/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-01.cnaf.infn.it" "infngrid"
"dteam" "voms.cern.ch" "15004" "/C=CH/O=CERN/OU=GRID/CN=host/voms.cern.ch" "dteam"
"cms" "cert-voms-01.cnaf.infn.it" "15004" "/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-01.cnaf.infn.it" "cms"
"gildav" "cert-voms-01.cnaf.infn.it" "15008" "/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-01.cnaf.infn.it" "gildav"
"cdf" "cert-voms-01.cnaf.infn.it" "15009" "/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-01.cnaf.infn.it" "cdf"
```

  While the last entry is the name of the VO, the first is the nickname to pass to the --voms option (usually coincide). Others are location of the server, port and DN of the hostcert.

  An optional entry could be present to specify the globus version of the server:

```
[venturi@pre-ui-01 venturi]$ cat ~/.glite/vomses
"dteam-lcg" "voms.cnaf.infn.it" "15020" "/C=IT/O=INFN/OU=Host/L=CNAF/CN=voms.cnaf.infn.it" "dteam" "22"
```

- In X_509_VOMSDIR (default /etc/grid-security/vomsdir) there should be public key of each VOMS server supported by the client
- These files are normally distributed by VO managers.

voms-proxy-init – example usage

- [venturi@pre-ui-01 venturi]$ voms-proxy-init --voms dteam-lcg
  Your identity: /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it
  Enter GRID pass phrase for this identity:
  Creating temporary proxy ..... Done
  /C=IT/O=INFN/OU=Host/L=CNAF/CN=voms.cnaf.infn.it
  /C=IT/O=INFN/CN=INFN Certification Authority
  Creating proxy ..... Done
  Your proxy is valid until Thu Jun 9 21:45:59 2005

  Specify the VO server to contact to retrieve the attributes.
  Also used to specify the set of attributes to be included in the AC.
  --voms <server[:command]>
  where command could be either a FQAN or 'all' meaning to retrieve all the attributes for the user. If command is absent is taken to be 'all'.
  - **Note that membership in groups is mandatory. Membership in all groups wll always be retrieved.**

voms-proxy-init – useful options

- All the options accepted by grid-proxy-init are also accepted by voms-proxy-init.
- Some useful extra options are:
  - --vomslife duration of the attribute certificate (limited by server configuration).
  - --order <group[:role]> specify the order in which the attributes should be included in the AC.
  - --include <file> includes a user specified file in the user's proxy that may contain additional authentication info, e.g. Kerberos ticket.
  - --noregen avoids generating the proxy for the connection to the server.
- For the complete list of options see the man page.

voms-proxy-init – common problems

- [venturi@pre-ui-01 venturi]$ voms-proxy-init --voms pippo
  VOMS Server for pippo not known!

  The specified vo nickname is not present in any of the configuration files.

- [venturi@pre-ui-01 venturi]$ voms-proxy-init --voms dteam
  Your identity: /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it
  Enter GRID pass phrase for this identity:
  Creating temporary proxy ..... Done
  /C=CH/O=CERN/OU=GRID/CN=host/voms.cern.ch
  /C=CH/O=CERN/OU=GRID/CN=CERN CA
  Can't interpret AC!
  dteam: Unable to satisfy G/dteam Request!

  The user is not a member of the VO. Contact the VO manager to request membership.

voms-proxy-init – common problems

- [venturi@pre-ui-01 venturi]$ voms-proxy-init --voms dteam-lcg
  Your identity: /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it
  Enter GRID pass phrase for this identity:
  Creating temporary proxy ..... Done

  Trying for old (1.1.x) server

  The client cannot contact the server. The message was improved starting from version 1.3.x. The support for 1.1.x servers will be dropped in future versions so that message will disappear.

voms-proxy-info – example usage

- [venturi@pre-ui-01 venturi]$ voms-proxy-info -all

```
subject   : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio
Venturi/Email=valerio.venturi@cnaf.infn.it/CN=proxy
issuer    : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio
Venturi/Email=valerio.venturi@cnaf.infn.it
identity  : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio
Venturi/Email=valerio.venturi@cnaf.infn.it
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u501
timeleft  : 11:20:05
VO        : dteam
subject   : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it
issuer    : /C=IT/O=INFN/OU=Host/L=CNAF/CN=voms.cnaf.infn.it
attribute : /dteam/Role=NULL/Capability=NULL
timeleft  : 11:20:05
```

Shows all the info that also grid-proxy-info shows, then the information in the attribute certificate. The second timeleft is the duration of the attribute certificate.

voms-proxy-info – common problems

- [venturi@pre-ui-01 venturi]$ voms-proxy-info
  error = 5025
  WARNING: Unable to verify signature!
  subject : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it/CN=proxy
  issuer : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it
  identity : /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Valerio Venturi/Email=valerio.venturi@cnaf.infn.it
  type : proxy
  strength : 512 bits
  path : /tmp/x509up_u501
  timeleft : 11:07:16

  A problem occurred verifiyng the AC signature. The host certificate of the VOMS server is not present in the $X509_VOMS_DIR (default /etc/grid-security/vomsdir) directory.

voms-proxy-destroy – usage example

- [venturi@pre-ui-01 venturi]$ voms-proxy-destroy
  - Will destroy the currently existing proxy.
  - Also works with plain old grid-proxy-init proxies.

- [venturi@pre-ui-01 venturi]$ voms-proxy-destroy

  Proxy file doesn't exist or has bad permissions.
  - This means that no proxy was found.

References

- VOMS
  - Available at http://infnforge.cnaf.infn.it/voms/
  - Alfieri, Cecchini, Ciaschini, Spataro, dell'Agnello, Fronher, Lorentey, From gridmap-file to VOMS: managing Authorization in a Grid environment
  - Vincenzo Ciaschini, A VOMS Attribute Certificate Profile for Authorization
- GSI
  - Available at www.globus.org
  - A Security Architecture for Computational Grids. I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. *Proc. 5th ACM Conference on Computer and Communications Security Conference*, pp. 83-92, 1998.
  - A National-Scale Authentication Infrastructure. R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. *IEEE Computer*, 33(12):60-66, 2000.
- RFC
  - S.Farrell, R.Housley, An internet Attribute Certificate Profile for Authorization, RFC 3281