VOMS C++ API tutorial

Emidio Giorgio

INFN Catania – EGEE NA3

CERN, 25-26.09.2006

Summary

- VOMS
  - Concepts
  - Architecture
  - API usage

Proxy certificates

- Introduced by the Globus Toolkit
- Are used for delegation 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 its own private key, thus addressing the problem of single sign on and delegation (grid services can act on behalf of the user)
    - The proxy certifcate is (should be) short lived (normally 12 hours), thus reducing the damage if stolen

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 & solutions

- 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

- 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 & AC

- 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>]
- FQAN are included in an Attribute Certificate
- 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

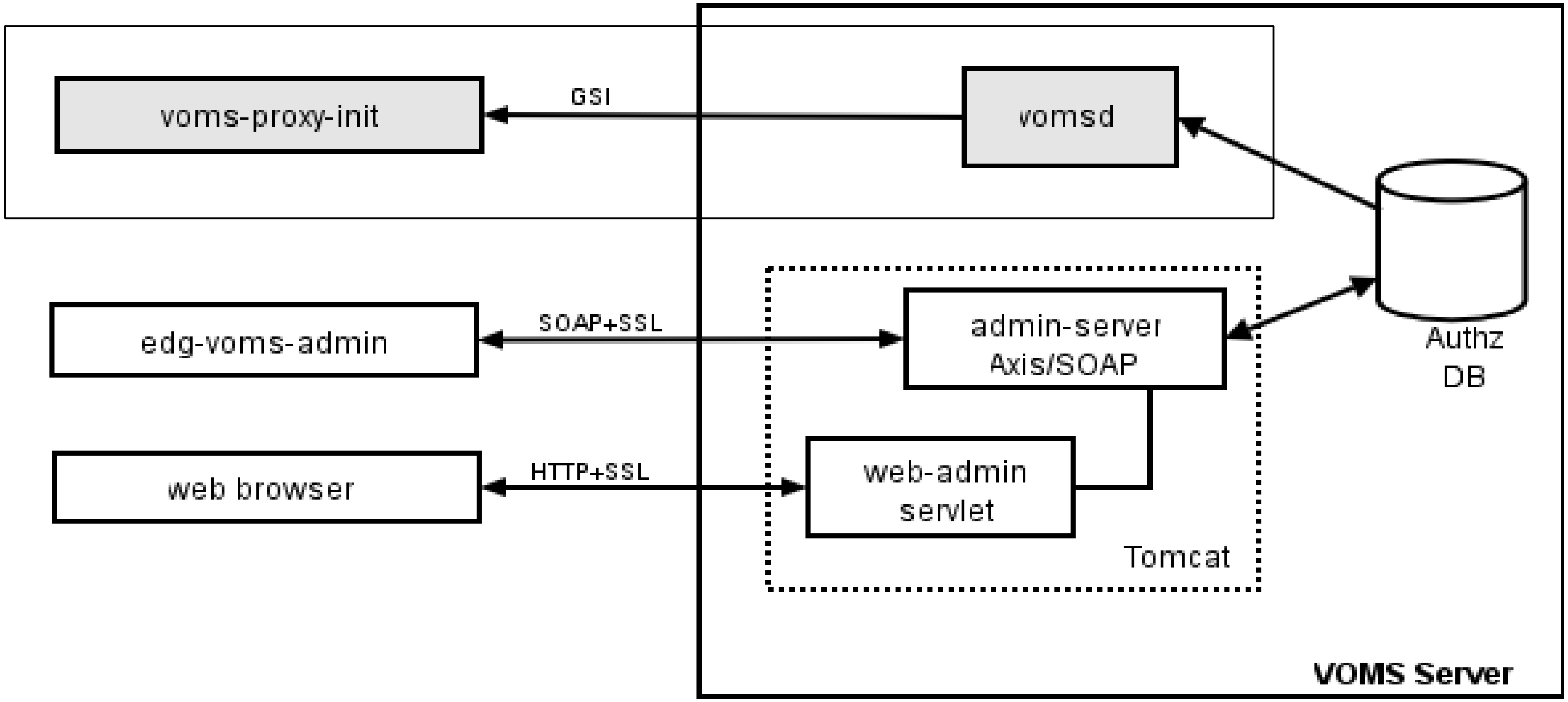
VOMS - operations

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

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.
    - API : same functionalities of clients, allows custom clients creation
- 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).

API overview

- Currently VOMS API are available in C/C++ and Java
- Not all clients functionalities are provided…..
- …but the essential has been made available
- Full functionalities APIs will be soon released

Practicals overview

- **What are you going to do ?**
  - Compile a c++ source code which shows infos contained in your VOMS proxy
  - Compile a c++ source code which, contacting a voms server, creates a new proxy inserting the obtained AC

Enjoy !