VO-based Dynamic Security Associations in Collaborative Grid Environment

COLSEC'06 Workshop, 15 May 2006, Las Vegas

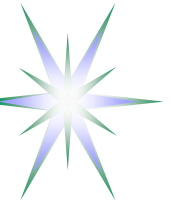Yuri Demchenko <demch@science.uva.nl>
on behalf of
Leon Gommans, Cees de Laat, Martijn Steenbakkers
SNE Group, University of Amsterdam
Vincenzo Ciaschini, Valerio Venturi
INFN, Italy

Outline

- Computer Grids and VO controversy
- VO use in EGEE and LCG Projects
  - VO Membership Service (VOMS)
- Dynamic associations and VO operational models
- Conceptual VO management model
- Additional information
 - GridShib profile

VO definition by Grid Evangelists

Resources and services virtualisation together with provisioning are two key concepts in Grid and OGSA

Anatomy of Grid (by Ian Foster et al)

p.1 - Grid which we define as flexible, secure, coordinated resource sharing among dynamic collections of individuals, institutions, and resources - what we refer to as virtual organizations.

p.2 - The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations.

p.4 - Sharing relationships can vary dynamically over time, in terms of the resources involved, the nature of the access permitted, and the participants to whom access is permitted.

Physiology of Grid (by Ian Foster et al)

Ubiquity. The Grid goal of enabling the dynamic formation of VOs from distributed resources means that, in principle, it must be possible for any arbitrary pair of services to interact.
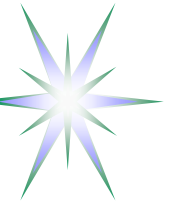
VO Controversy

Problems with the VO use outside of Grid

- Virtualisation
- Dynamics
- Trust management
- Setup and configuration
- Discovery (and population)
- Tools

VO in Collaborative applications and Complex resource provisioning

- **Two basic use cases**
  - Grid based Collaborative applications/environment (GCE) built using Grid middleware and integrated into existing Grid infrastructure
  - Complex resource provisioning like Optical Lightpath provisioning (OLPP), or bandwidth-on-demand (BoD)
- **VO based functionality (and requirements) to support dynamic security associations**
  - Dynamic Trust management
    - Establishing dynamic trust management relations between VO members
  - Attribute and metadata resolution and mapping
    - VO-based access control service requires common VO-wide attributes that however can be mapped to the original ones
  - Policy combination and aggregation
    - To allow conflict resolution and policy harmonisation between VO members
  - Flexible/distributed VO management infrastructure
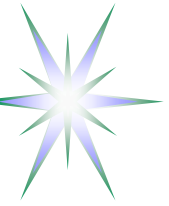
VO bridging inter-organisational barriers
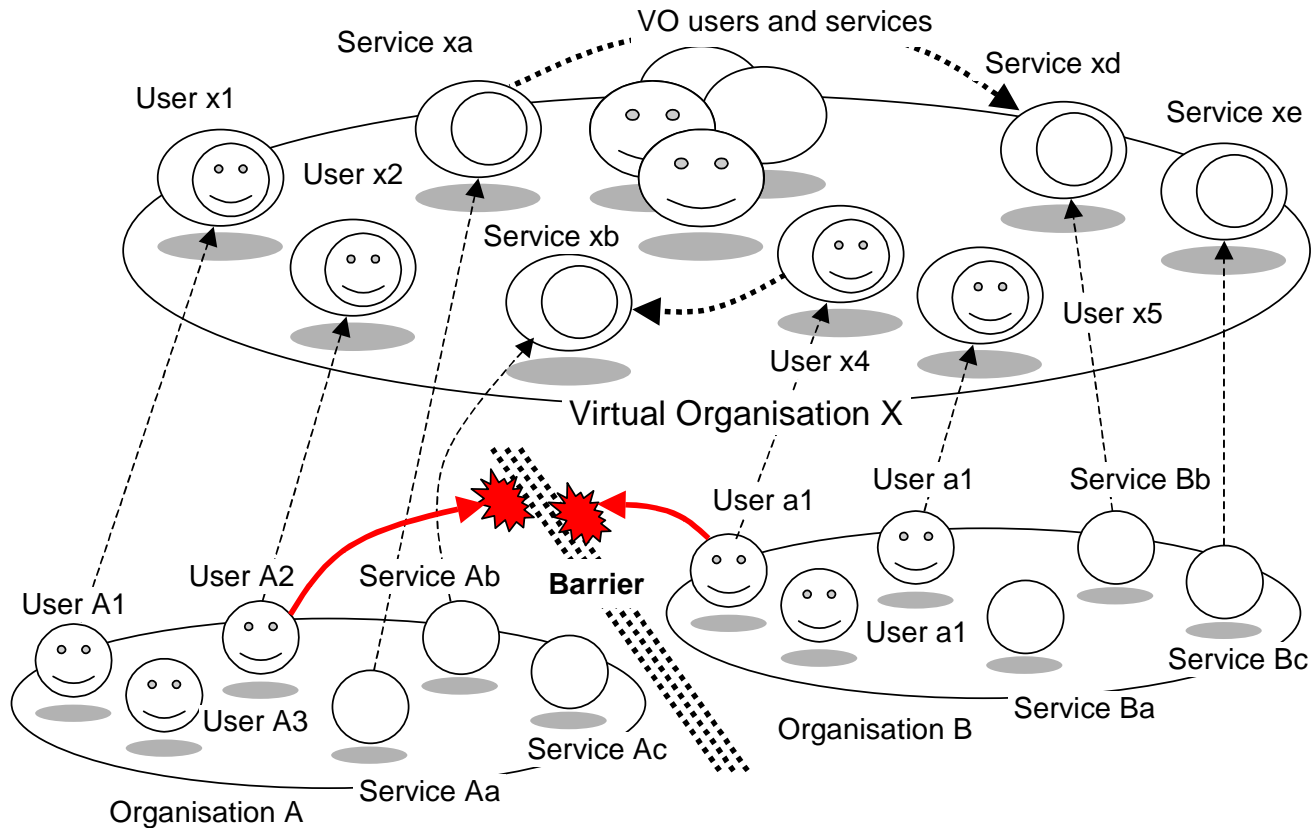
VO allows bridging inter-organisational barriers without changing local policies

- Requires VO Agreement and VO Security policy
- VO dynamics depends on implementation but all current implementations are rather static

Virtualisation and Dynamics

- There is a gap between current VO concept and existing practice due to the lack of appropriate theoretical foundation
    - OGSA's vision of the VO and virtualisation is not supported by more detailed description of the VO functionality and operation
    - Current VO implementation in LCG/EGEE needs more conceptual/higher-level definition to be aligned with (yet to be developed) OGSA VO concept
        - The VO is directly associated with two projects where VO is managed under the project administration
        - There is still no clear/formal definition of the VO Agreement and VO policy in LCG/EGEE
- This causes different understanding of the VO concept and functionality by different groups of potential adopters and users
    - first issue is a relation between virtualisation and VO
        - presumably can be resolved with the definition of the VO management functionality including VO foundation/agreement and life cycle
    - second issue to be clarified is a relation between VO and dynamic associations
        - which part of the VO concept is static (like CA/PMA and AttrAuth) and which can support dynamic associations (and dynamic trust management)

VOMS – standard-de-facto for VO management

VO Membership Service (VOMS) is a standard-de-facto for VO management and VO-based authorisation in Grid

- VO is represented as a complex, hierarchical structure with groups and subgroups
  - Subgroup management may be delegated to different administrators
- Every user in a VO is characterised by the set of attributes
  - Group/subgroup membership, roles and capabilities – so-called 3-tuples
  - Combination of all 3-tuples for the user is expressed as a Fully Qualified Attribute Name (FQAN)
  - FQAN is included into VOMS X.509 Attribute Certificate (AC)
- VOMS infrastructure
  - May contain multiple VOMS serves and synchronised VODB's
  - Supports user calls for VOMS AC's and VOMS admin tasks
- VOM Registration is developed by Open Science Grid (OSG) project to support users self-registration

Dynamic Security Associations

- **Session** – establishes security context in the form of session key that can be a security token or simple UID bound to secure credential/context
  - Session may associate/federate users, resources and actions/processes
- **Job/workflow** – more long-lived association and may include few sessions
  - May need to associate more distributed collection of users and resources for longer time required to deliver a final product or service
  - Job and workflow may contain decision points that switch alternative flows/processes
  - Security context may change during workflow execution or Job lifetime
  - Job description may contain both user and resource lists and also provide security policy and trust anchor(s) (TA)
- **Project or mission oriented cooperation** – established for longer time cooperation (involving people and resources) to conduct some activity
  - This is actually the area of currently existing VO associations
- **Inter-organisational association or federation** – established for long-term cooperation, may have a wide scope of cooperative areas
  - This is the area of inter-university associations
    - Shibboleth Attribute Authority Services (SAAS) is designed for this kind of federations

VO Operational Models

- **User-centric VO (VO-U) -** manages user federation and provide attribute assertions on user (client) request
- **Resource/Provider centric VO (VO-R)** - supports provider federation and allows SSO/access control decision sharing between resource providers
- **Agent centric VO (VO-A) -** provides a context for inter-domain agents operation, that process a request on behalf of the user and provide required trust context to interaction with the resource or service
- **Project centric VO (VO-G) -** combines User centric and Provider centric features what actually corresponds to current VO use in Grid projects
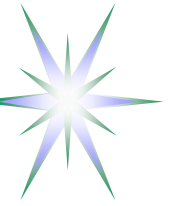
Conceptual VO Management Framework

- VO establishes own virtual administrative and security domains
  - It may be completely separate or simply bridge VO-member domains
- VO management service should provide the following functionalities
  - Registration and association of users and groups with the VO
  - Management of user attributes (groups, roles, capabilities)
  - Association of services with the VO
  - Association of policies with the VO and its component services
- VO Registry service for wider VO implementation may be required
 - VO naming should provide uniqueness for the VO names

VO Security Services

- VO as a component of the Security infrastructure should provide the following security services
  - ◆ Policy Authorities
  - ◆ Trust management service
  - ◆ Identity Management Service
  - ◆ Attribute Authorities
  - ◆ Authorization service
  - ◆ Authentication service
  - ◆ Accounting
 - ◆ Operational services (Intrusion detection, Incident response, etc.)

Example VO Security services operation
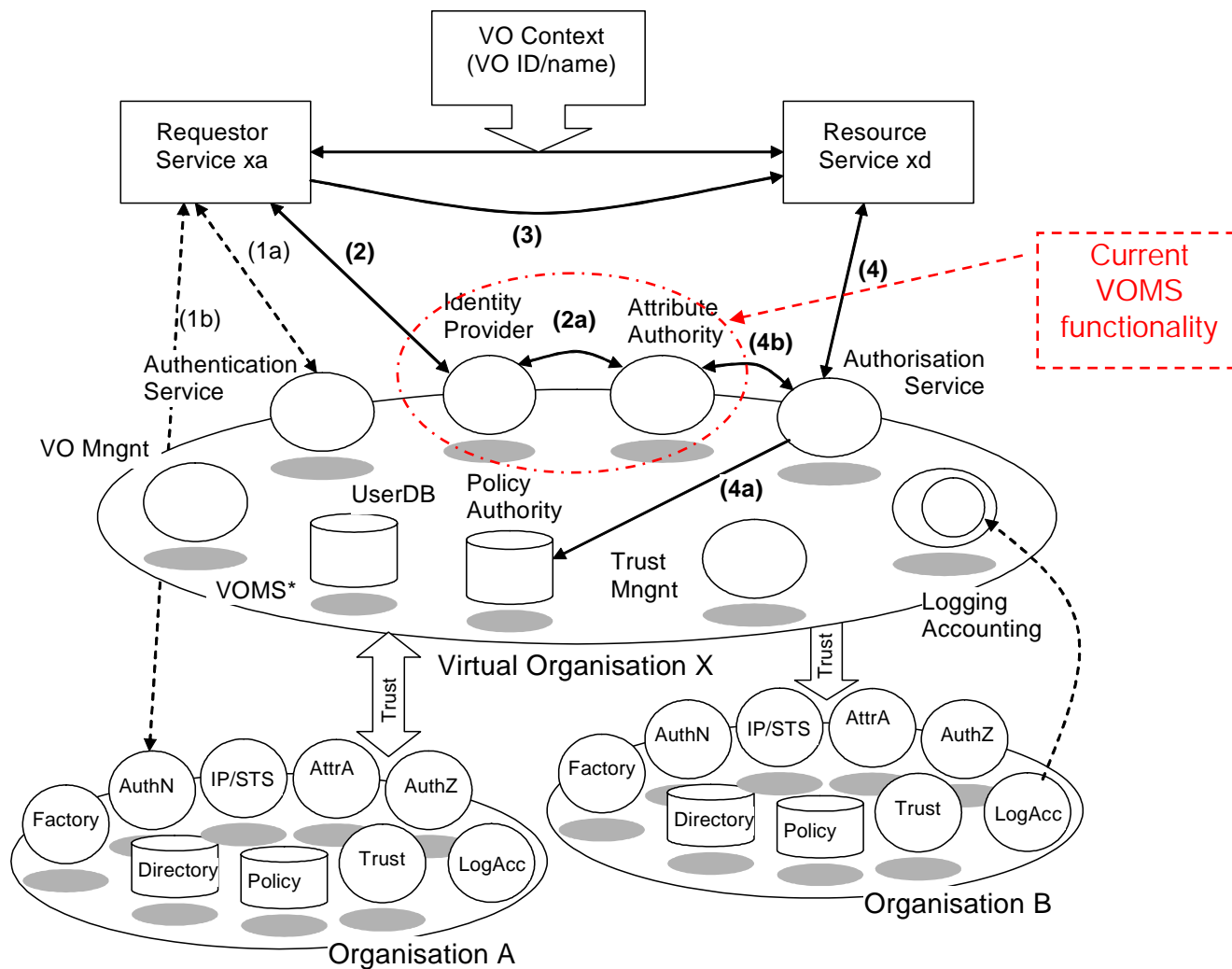
VO and DNSSEC – Feasibility Analysis

- Existing LCG/EGEE VO registration procedure allows actually using DNSSEC for populating VO together with its (secondary) public key that can be used for initial trusted introduction of the VO and secure session request by the requestor
  - VO registry problem can be solved
- DNSSEC limitations
  - Limited space for putting the key information because of DNS/DNSSEC response message allows only one non-fragmented package of size 1220 bytes for standard DNS message and 4000 bytes for special DNSSEC extension [RFC4034]
  - DNSSEC domain record (in our case VO domain name) and key must be signed by upper layer domain's key, and therefore DNSSEC trust tree must be compatible with the application oriented trust domain
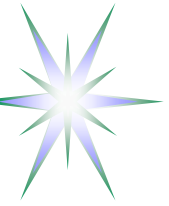
Additional information

- EGEE/LCG Practice
- GridShib Profile

Using VO/VOMS for Dynamic GCE and Resource Provisioning

Issues to be taken into account when considering VO in dynamic GCE and for dynamic resource provisioning:

- Current VO management and VOMS infrastructure are rather designed for long-term collaborative projects
  - VO setup is a complex long-time procedure and cannot be used as a solution for the global ad-hoc dynamic trust establishment
  - VOMS server Attribute Certificate is based on X.509 AC for Authorisation, its use for Gird authorisation (within Globus Toolkit) suggests using Proxy Certificate
  - VOMS client-server protocol is not clearly defined
  - Current VO/VOMS implementation has no flexible attribute namespace management (and corresponding procedure and policy)
- Dynamic VO infrastructure must provide a solution for dynamic distributed trust management and attribute authority
  - VOMS provides all necessary functionality for creating ad-hoc dynamic VO associations
  - GridShib (GT4/WS-enabled) profile can be used for VO with distributed membership management

EGEE/LCG Practice: VO Registration Procedure

1. Naming the VO

2. Request VO integration into existing EGEE infrastructure from one of designated bodies EGEE Generic Applications Advisory Panel (EGAAP) or NA4/SA1 Joint Group

3. Setting-up a VO. The VO management selects a site where to run the VO database (VODB) server and the Registration service/database (where the acceptance of the Grid Usage Rules by the user is registered).

4. Populating a VO. Candidate entries in the VODB are passed through successful Registration process and Registration database additions.

5. Integrating VO into existing infrastructure

6. Organising support structure for the VO

EGEE/LCG Practice: VO Security Policy (operational)

VO enrolment process MUST capture and maintain at least the following information:

1. VO Name

2. VO Acceptable Use Policy

3. Contact details and certificates for the VO Manager and at least one Alternate

4. Email address of a generic VO contact point for the VO managers

5. A single email address of the security contact point

6. URL of one or more VO Membership Servers

Note. Actual use of the VO membership for AuthZ in Grid is defined by the Resource/Service access control policy

Using VO for Dynamic Resource Provisioning (2)

VOMS and SAAS interoperation and integration

- GridShib profile targets for SAAS integration into Grid/GT environment
  - Expected to provide a framework for combing well developed Shibboleth attribute management solutions and VOMS functionality
- Differences in VOMS and SAAS operation on the user/client and service/resource sides
  - In VOMS the user first needs to obtain VOMS AC by requesting particular VOMS server, and next include it into newly generated Proxy Cert and send request to the service
  - In SAAS the user sends request to the Shib-aware service and may include a particular IdP reference, otherwise service will poll trusted AA/IdP's based on preconfigured list of trusted providers.
  - VOMS requires user ID and therefore doesn't provide (user) controlled privacy protection (in contrary to Shibboleth).

GridShib Attribute Handling Models

- Basic Globus-Shibboleth integration without anonymity using attributes request/pull by the resource from the trusted SAAS

- Basic Globus-Shibboleth integration without anonymity using attributes provided by the requestor which are previously obtained from the trusted SAAS

- Globus-Shibboleth integration with anonymity and attributes requested by the resource from the trusted SAAS that is can release attributes based on user pseudonym or authentication confirmation credentials.

- Globus-Shibboleth integration with anonymity using attributes provided by the requestor which are previously obtained from the trusted SAAS for the user pseudonym or anonymous authentication confirmation credentials (Authentication/identity token)

Establishing Security context for GridShib

1. The Grid User and the Grid Service each possess an X.509 credential that uniquely identifies them.

2. The Grid User is enrolled with a Shibboleth Identity Provider (IdP), and correspondently with IdP's AA.

3. The IdP is able to map the Grid User's X.509 Subject DN to one and only one user in its security domain.

4. The IdP and the Grid Service each have been assigned a unique identifier called a providerId.

5. The Grid Client application has access to the Grid User's X.509 certificate and the IdP providerId. This information is used to create Proxy Cert that will contain IdP providerId and signed by the User private key.

6. The Grid Service has a set of certificates identifying IdP/AAs that it trusts to provide attributes suitable for use in authorization decisions.

7. The Grid Service and the IdP rely on the same metadata format and exchange this metadata out-of-band.

8. It is assumed that all X.509 End-Entity Certificates (EEC) are issued by CAs that are trusted by all parties mentioned in this document.