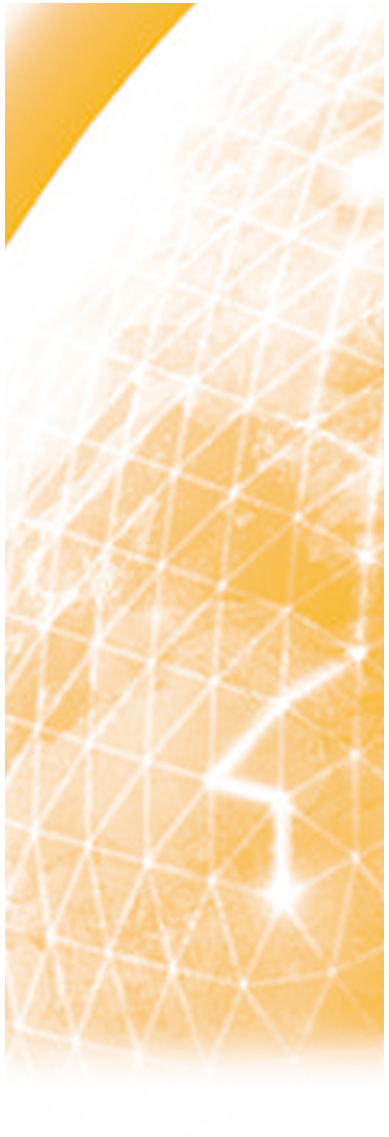

EGEE Policy Coordination Meeting
(Bologna June 6-7, 2005) - Overview and follow-on activities

MWSG – 14-15 September 2005, CERN

Yuri Demchenko <demch@science.uva.nl>
AIRG, University of Amsterdam

www.eu-egee.org

Information Society

Outline

- Meeting overview
  - Goals and discussions
  - Conclusions
- Follow-on developments and further steps
- Related activities in TF-EMC2, GEANT2 and Internet2/NMI

Policy Coordination Meeting - Goals

- **Discuss major technical developments and implementation issues**
  - Those of which require technical policy/solutions coordination and efforts combination/distribution
  - Attributes and policy namespaces and schemas
  - Common policy and attributes management tools
  - Use of SAML and XACML for AuthZ and security context exchange
- **Coordination and compatibility - not only inside EGEE and also with allied projects/activities and other application areas**
  - There are many areas from which EGEE can benefits, e.g. TF-EMC2/GEANT2 (e.g., AAI, AARR, SCHAC), Internet2/NMI (e.g., Shibboleth, GridShib), etc.
- **Meeting style/convention**
  - Topics for this meeting were set very technical – to exchange experience and agree on issues to ensure future compatibility

Discussed issues (1)

Developments/Tools available

- **INFN-CNAF**
  - G-PBox: a policy management/distribution/aggregation framework based on XACML
  - VOMS: a PKI attributes management and distribution tool
- **AIRG/UvA:**
  - AAA AuthZ Toolkit and simple AAA and XACML policy management tools
  - XACML demo implementation for collaborative applications in the Collaboratory.nl (CNL) project
    - GAAAPI RBAC profile
  - SAML tickets and tokens handling tools for performance optimisation and trust management in distributed access control systems

Discussed issues (2)

- **Other developments and experience:**
  - Conceptual GAAA distributed AuthZ infrastructure models
    - Combined pull-push-agent models for multidomain scenarios
    - Trust management issues
  - Experience of using XACML and SAML for AuthZ and Policy enforcement
  - Possibility of using available products and experience for common AuthZ/PE framework/infrastructure in EGEE/gLite and further needs for coordination and collaboration

Conclusion – Cooperative actions

- **Accept SAML attributes namespace definition for SAML and XACML attributes and investigate further its suitability for ongoing works and EGEE/gLite in general**
- **Agree on the following key steps and stages in adopting common namespace for EGEE (and coordinating projects)**
  - (1) attribute naming schema
  - (2) registries and resolvers
  - (3) special profiles
- **Define policy and policy set templates for basic usecase in EGEE and affiliated projects at INFN and AIRG/University of Amsterdam**
- **Investigate compatibility and possible coordination with GridShib**
- **Consider possible coordination and collaboration on policy and attributes compatibility with other active NRENs' initiatives and projects, in particular, TF-EMC2 AAI, JRA5/GN2, Internet2 NMI**

Conclusion – Coordinated actions

- **PBox**
  - adding Web Services functionality
  - investigating which attributes (of a Grid environment) are relevant to express policies
  - investigating the use of XACML with SAML
  - implementing RBAC model using XACML
- **VOMS**
  - adding SAML format for attributes
  - adding Web Services interface
- **GAAA and GAAAPI**
  - simple trust/key management tools
  - simple policy management tools
  - adding Web Services interface
  - attaching policy to WSDL
- **gLite AuthZ Framework**
  - try to integrate PBox and GAAAPI into gLite AuthZ Framework

Common namespace for EGEE

(1) attribute naming schema

Options:

AttributeID = urn:oasis:names:tc:xacml:1.0:subject:subject-id (:voms:subject:subject-dn)

Or

use optional element “Issuer” of the “xs:string” type

Examples from MACE (RFC3613):

Registry – http://middleware.internet2.edu/urn-mace/urn-mace.html

urn:mace:shibboleth:1.0:metadata

urn:mace:washington.edu:dir:attribute-def:uwEmployeeID

(2) registries and resolvers

(3) special profiles

Follow-on development - AIRG

- **GP-NG-RoN GSX Gap Analysis – use of GAAA AuthZ Framework and Grid for dynamic resource provisioning**
  - Optical Light Path Provisioning (OLPP) as major usecase
  - Currently in the final drafting stage
- **GAAA AuthZ framework – two basic profiles are defined**
  - GAAA-RBAC for Collaborative Environment
  - GAAA-P for interdomain network/resource provisioning
- **VO conceptual model revisited**
  - VO as a framework for dynamic security associations

GAAA-P – GAAA profile for Provisioning

- **Major GAAA-P components/extensions**
  - Workflow control in he GAAA based provisioning model
    - WSFL and WSBPEL as upper layer to (stateless) WS/WS-Security
  - Special Policy profile for provisioning
    - Policy combination and aggregation
  - Attributes and metadata resolution and mapping
    - VO and Identity management usecase/profile
    - Compatibility with GridShib-SAAS
  - Different types of secure credentials and validation callouts
  - Dynamic trust management using federated trust model
    - Based on dynamic VO federation model
    - WS-Trust/WS-SecureConversation Secure Token Service (STS)
  - Integration with GT4 Authorisation Framework
    - (1) External AuthZ service using OGSA AuthZ interface
    - (2) GAAA callout
    - (3) internal GAAA PDP

Follow-on development - INFN

- **See Vincenzo Ciaschini's presentation**

Related Activity – Internet2/NMI

Internet2 NMI (NSF Middleware Initiative) – convergence between Internet2 and Grid infrastructure and tools

- **SAAS (Shibboleth's Attribute Authority service) and GridShib**
  - GridShib - A Policy Controlled Attribute Framework - http://grid.ncsa.uiuc.edu/GridShib/
- **Attributes management tools**
  - Grouper - http://middleware.internet2.edu/dir/groups/grouper/
  - Signet - http://middleware.internet2.edu/signet/
- **MyProxy and PubCookie integration**
  - NMI project at Univ. Virginia (and NCSA)
  - http://www.pubcookie.org/

Related Activity – TF-EMC2 and GEANT2

TERENA TF-EMC2 and GEANT2 – European NREN's coordination and infrastructure

- **TF-EMC2 (Task Force for European Middleware Coordination) – major activities and projects**
  - SCHAC - SCHema for ACademia - http://www.terena.nl/tech/task-forces/tf-emc2/schac.html
  - AA-RR - Authentication and Authorization Requester-Responder (http://www.rediris.es/app/aarr/)
  - TACAR (TERENA Academic CA Repository) - http://www.tacar.org/
  - CertiVeR (http://www.certiver.com) – OCSP service for TACAR and Grid (?)
- **JRA5 Roaming and Authorisation in the GEANT2**
  - Cross-NREN federation based AA(A) (super-)infrastructure
    http://www.geant2.net/server/show/nav.00d00a005
    - Architecture is rather Shibboleth centric

Additional information

- Conceptual VO model
- GridShib Profile

VO Controversy

- **Problems with the VO use outside of Grid**
  - Virtualisation
  - Dynamics
  - Trust management
  - Setup and configuration
  - Discovery (and population)
  - Tools

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 do 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 is specially designed to support this kind of federations (e.g. InCommon or InQueue)*

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

Using VO for Dynamic Resource Provisioning (1)

- **Issues to be taken into account when considering VO 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 (with GT) suggests using Proxy Certificate
    - VOMS client-server protocol is not clearly defined
    - Current 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
      - *(Use Grouper and Signet tools for Attribute/group/roles management/editing)*

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).

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

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.