gLite Java Authorisation Framework (gJAF) and Authorisation Policy coordination

Yuri Demchenko
University of Amsterdam

MWSG meeting
EGEE’06 Conference, September 27, 2006, Geneve
Outline

• Observations
  – AuthZ in EGEE/LCG and gJAF
  – Difficulties and problems in implementing common AuthZ FW
  – Activities and Initiatives on AuthZ coordination

• gJAF Overview

• GT4-AuthZ overview

• Next steps – Discussion

• Additional - GAAA-AuthZ framework by UvA
• **Wide diversity between sites**
  – Typically based on LCAS/LCMAPS (C-based)

• **Foundation for gLite Java AuthZ Framework (gJAF)**
  – DJRA3.1 (updated in DJRA3.3) – EGEE Security Architecture
  – gJAF Developer’s guide -
    [https://edms.cern.ch/document/501718](https://edms.cern.ch/document/501718)

• **gJAF initially was developed to be compatible with Globus AuthZ framework**
  – Version 1.0 released end 2004, some extensions later
    ▪ Supports VOMS attributes (VOMS PDP), GridMapFile, BlackList
  – Now GT4-AuthZ significantly developed
    ▪ More flexible configuration and better user creds handling
Difficulties and problems in implementing common AuthZ FW

• Human and Legacy type (Developers and implementers)
  – Successful only when smoothly migrated and easier achieved obvious benefits
    ▪ “When implementing/debugging security solution is too hard, developers will do it in their own way” – GGF16 AuthZ Workshop
  – Working with the distributed computing paradigm (computer clusters and pool accounts)

• Technical
  – Coordination and application specific (incl. legacy solutions)
  – Fine-grained and consistent access control with ACL
    ▪ Local security and resource context is often implicit
    ▪ Problem with replica data access policy
  => Common PEP and context/environment aware Policy
Activities and Initiatives

• **EGEE AuthZ Policy Coordination**
  – Meeting in Bologna June 6-7, 2005

• **GGF-AuthZ Working Group**
  – EGEE interest – bring EGEE reality to GGF standardisation

• **Other GGF/EGEE/LCG activities**
  – LCG AuthZ workshops – interoperability between current solutions
  – GIN – Grid Interoperation Now
    ▪ Use of VOMS attributes for AuthZ in Grid
  – TONIC – Taskforce Organizing Near-term Interoperation for Credentials
gJAF Overview

- **Provided as org.glite.security.authz Java package**
- **Called from applications via interceptor**
  - SOAP/Axis or application specific
  - Presumably orthogonal to application and easy integrated
- **Contains a configured chain of PIP and PDP modules**
  - PIP collects/extracts information to be sent to PDP
  - Each PDP evaluates its relevant attributes against its own Policy
  - Chain is configured to apply PDP decisions combination
- **Problems**
  - Requires application specific manual chain configuration
  - Unchanged but GT4-AuthZ is evolving
  - Limited use up to now
    - CE (and some interest from DM)
gJAF components and connection to the Grid Service

Grid Service

Service Gateway (SOAP Msg Interceptor)

PEP

PIP chain

AuthZ Decision Combination

PDP chain

AuthZ Decision

Srv Request

Call from SrvGw or Msg Interceptor

AuthZ Attr/Data

User/Local Attr

VO Attr

External Attr Call

Ext. AttrAuth (e.g. Shibboleth)

Ext. AttrAuth (e.g. Shibboleth)

Ext. AttrAuth (e.g. G-PBox)
• Can potentially be configured for Container, Message, Service/Resource
  – But all based on SOAP/Axis msg processing by Axis interceptor
• AuthZ processing sequence includes
  – New! Bootstrapping X.509 PIP – retrieves request parameters from the message
    ▪ Subject, Resource, Action
  – Sequence of pre-configured PIP’s, including SAML
  – Sequence of (specialised) PDP’s
  – Different PDP decisions combination algorithms by AuthZ engine
    ▪ However, multiple policy decision’s consistency is not resolved
• Available PDP’s
  – ACL and GridMap
  – HostAuthorization and UserNameAuthorization
  – SAML AuthZ callout and SAML AuthZ Assertion
  – SelfAuthorization – based on shared/trusted Resource credentials
  – Simple XACML PDP (provided as a placeholder for extension)
• Compatibility and integration with other and 3rd party solutions
  – Integration with the G-PBox
  – Compatibility and integration with (or move to) the GT4-AuthZ
    ▪ Can get workforce support from GT4 Security team
  – Other issues found important
    ▪ Enable PDP chain to respond with Obligated decision
    ▪ PDP answer with AuthZ ticket to provide extended/full decision context in response to gJAF/PDP
Next steps (2)

- **AuthZ Policy compatibility and coordination**
  - *Common or mapped attributes semantics*
  - Policy formats mapping

- **Using XACML for policy expression**
  - Standard, Context aware
    - Used in G-PBox
  - Can be added as XACML PDP plugin to gJAF or GT4-AuthZ
  - Need policy management tool (simple or complex)

- **SAML/Shib Credentials support**
  - Coming in GT4-AUthZ with GridShib
  - Will rely on effective cooperation with SWITCH
• Any other issues?
Overview GAAA-AuthZ framework by UvA

• Major focus – *AuthZ for dynamic services and CRP*
  – Implemented in GAAA_tk but moving just to provide specific extensions to GT4-AuthZ

• Major application areas
  – Grid-based Collaborative systems
  – Complex Resource Provisioning (CRP), e.g. Optical LightPath Provisioning (OLPP) as service on demand

• Projects and cooperation
  – EGEE, NextGRID, PHOSPHORUS
  – GT4-AuthZ Team, TF-EMC2

• Recent developments – GAAAPI package
  – SAML and XACML v2.0 and v3.0
  – Dynamic security context management
  – Authorisation Session support
    • AuthZ tickets (both proprietary and SAML-based)
    • Delegation and roles management/restrictions
Functionality provided by GAAP

- Specific functionality provided by GAAPI package
  Considered as extension to GT4-AuthZ
  - Authorisation tickets and tokens handling for performance optimisation and advanced Authorisation Session management
    - SAML and Proprietary AuthZ tickets format
      - Support extended AuthZ session context and Delegation
  - Complex XACML policies evaluation to provide fine-grained access control
    - Supports hierarchical resource management and administration policy management (including delegation)
      - With XACML RBAC and Hierarchical Resources special profiles and XACML 3.0 Administrative Policy
  - Flexible trust domains and request/attributes semantics configurations and management