Authorisation Policy coordination and
gLite Java Authorisation Framework (gJAF)

Yuri Demchenko
University of Amsterdam

JRA1 All Hands meeting, July 10-12, 2006, Pilsen
Outline

- Observations
  - AuthZ in EGEE/LCG and gJAF
  - Activities and Initiatives on AuthZ coordination
  - Difficulties and problems in implementing common AuthZ FW
- gJAF Overview
- GT4-AuthZ overview
- GAAA-AuthZ framework by UvA
- Next steps – Discussion
Observations – AuthZ in EGEE/LCG

- **Wide diversity between sites**
  - Typically based on LCAS/LCMAPS (C-based)
- **Foundation for gLite Java AuthZ Framework**
  - DJRA3.1 (updated in DJRA3.3) – EGEE Security Architecture
  - Developer’s guide - [https://edms.cern.ch/document/501718](https://edms.cern.ch/document/501718)
- **gJAF 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
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
• **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 account)

• **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
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 has evolved
  - Limited use up to now
    - CE (and some interest from DM)
GT4 Authorisation Framework

- Can potentially be configured for Container, Message, Service/Resource
  - But all based on SOAP/Axis msg processing by Axis interceptor

- AuthZ processing sequence includes
  - Bootstrapping X.509 PIP – retrieves request parameters from msg
    ▪ 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)
Generic AuthZ FW development for SOA applications

- **Major focus** – AuthZ for dynamic services
- **Major application areas**
  - Grid-based Collaborative systems
  - Complex Resource Provisioning (CRP), e.g. Optical LightPath Provisioning (OLPP) as service on demand
- **Cooperation and projects**
  - EGEE, NextGRID, LUCIFER=> PHOSPHOR
  - GT4-AuthZ Team, TF-EMC2
- **Recent developments**
  - XACML and SAML
  - Dynamic security context management
  - Authorisation Session support
    - AuthZ tickets (both proprietary and SAML-based)
    - Delegation and roles management/restrictions
Extending GAAA Toolkit - Adding new functionality to GT4-AuthZ

- **Specific functionality provided by GAAA-AuthZ Toolkit**
  - 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
TicketID="cba06d1a9df148cf4200ef8f3e4fd2b3">
  <AAA:Decision ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</AAA:Decision>
  => <AuthorizationDecisionStatement Decision="*" Resource="*"
    <AAA:ConditionAuthzSession PolicyRef="PolicyRef-GAAA-RBAC-test001" SessionID="JobXPS1-2006-001">
      <extension>
        EXTENDED <SAMLConditionAuthzSession PolicyRef="*" SessionID="*"/>
      </extension>
    </AAA:ConditionAuthzSession>
  </AAA:Conditions>
</AAA:AuthzTicket>
Next steps – Discussion

- **Compatibility and/or move to GT4-AuthZ**
  - Benefits
  - Problems
- **AuthZ Policy compatibility and coordination**
  - Common or mapped attributes semantics
  - Policy formats mapping
- **Using XACML for policy expression**
  - Standard, Context aware
  - Can be added as XACML PDP plugin to gJAF or GT4-AuthZ
  - Need policy management tool (simple or complex)
- **SAML/Shib Credentials support**
  - Coming also with GridShib
  - Will rely on good cooperative contact with SWITCH
• Any other issues?