Using Policy-based Management for Privacy-Enhancing Data Access and Usage Control in Grid Environments

Wolfgang Hommel
Leibniz Supercomputing Centre
Munich Network Management Team
Overview

• Enterprise and federation privacy management
  – Scenario: Leibniz Supercomputing Centre
  – Current privacy management practices

• Motivation for / differences to Grid privacy management

• Privacy policies for Grids and their management

• Architectural adaptation (home sites)
Scenario: Leibniz Supercomputing Centre

Computing centre for all Munich higher education institutions:

- Services (email, storage, VPN, ...)
  - more than 75,000 students,
  - more than 25,000 employees

- Part of German Shibboleth federation:
  - Sharing of library resources
  - E-Learning across HEI borders
  - Distribution of licensed software, e.g. Microsoft Dreamspark

- Used by researchers from all over Germany, managed via a local, LDAP-based identity & access management system

- Current flagship: sgi Altix 4700

How can privacy management approaches known from
- enterprise identity management and
- federated identity management
be adapted to Grid environments?
Privacy Management includes:

- (Online) Privacy Statement
  - Ideally also machine-readable (e.g. using P3P)
  - Version number stored with each user record (sticky policy paradigm)

- Informational self-determination
  - Users can see which data is stored about them
  - Data correction and removal on demand

- Obligation handling
  - Data retention limits, user notifications, ...
  - Obligation monitor triggers privacy related actions

- Enforcement of intended use for access on user records
  - Typically policy-based (e.g. EPAL), subject to auditing

- Graphical management interface
  - Business card metaphor for users
Why do we need privacy management in Grids?

• Protect the Grid user’s personal data
  – Same motivation as in identity federations
  – Higher dynamics regarding SP selection

• Protect the Grid job
  – Input data, e.g. large sets of medical data
  – Program code, e.g. algorithm invented by the user
  – Output data

STPG 2008 Using Policy-based Management for Privacy-Enhancing Data Access and Usage Control in Grid Environments
Handling of Grid privacy policies

• Policy layers
  – Typically relevant layers:
    • Compliance / legislative regulations (e.g., EU directive 95/46/EC)
    • Grid- or VO-wide policies
    • Service provider and service specific policies
    • Home site / identity provider default policies
    • User’s personal and Grid job specific privacy preferences
  – Layer priority is specific to each scenario

• Management interface for users
  – Personal privacy preferences
  – Research project specific privacy policies
  – Individual Grid job privacy policies
Towards a dedicated solution

- Grid privacy policy language selection, basic specification of Grid-specific vocabulary

- Architectural integration concepts
  - Adaptation of home sites / identity providers
  - Scope and focus of service provider adaptation

- Guidelines for the derivation of (scenario-specific) vocabulary

- Middleware integration and user interfaces
Using XACML as policy language

• eXtensible Access Control Markup Language
  – OASIS standard
  – Focus on access control, but privacy profile available
  – Adapted to FIM privacy management in previous work

• Rationale to use XACML:
  – Leverage existing infrastructure (PDP, frontends)
  – Grid-specific purposes and obligations do not require Policy Decision Point (PDP) modifications
  – XACML already used for Grid access control

☞ Architectural concept allows for other languages
Example policy

```xml
<Policy id="GridJobPolicyExample1" RuleCombiningAlgorithm="first-applicable">
  <CombinerParameters>
    <CombinerParameter ParameterName='PolicyPriority'>
      100  <!-- Priority in case multiple policies are relevant for a request -->
    </CombinerParameter>
  </CombinerParameters>

  <Description> Grant access to code for optimization purpose </Description>

  <Rule id="ExampleRule1" effect="permit">
    <Target>
      <Resource> <!-- Specifies grid job data according to the chosen namespace -->
        https://org1.example.com/project/username/gridjobs/id/code
      </Resource>

      <Subject> <!-- Grant access to all service providers within the VO, but... -->
        https://grid.example.com/members/VO
      </Subject>

      <Action> <!-- ... restrict access based on the specified purpose. -->
        gridjobs/code-optimization
      </Action>
    </Target>
  </Rule>
</Policy>
```
Summary and outlook

• Results achieved so far:
  – Analysis of differences between Grids and traditional inter-organizational scenarios and resulting requirements
  – Adaptation of XACML privacy policies
  – Architectural concepts for home sites and service providers

• Ongoing work:
  – Analysis of concrete Grid projects to determine the precise policy vocabulary (conditions, obligations)
  – Realization on the service provider side
  – Adaptation of a web-based management tool for Grid users