XACML Contributions
Hal Lockhart, Oracle Corp
Topics

• Authorization API

• Finding Input Attributes
Authorization API

• **XACML Specifies**
  – Policy language evaluation semantics
  – XML format for policy interchange
  – Abstract format for inputs and outputs, expressed in XML
  – Protocol for remote requests using XML input & output format

• **XACML does not specify**
  – API for requesting policy decision
Authorization API Benefits

• Needed for call to local PDP
  – Local PDP required for low latency calls
  – Inefficient to serialize data to and from XML
  – XML form not required by the standard

• Also useful to have standard API for remote requests
  – Common code to build message
API General Characteristics

• Java initially, C++ and perhaps others to follow
• Modeled on XACML Request/Response Contexts
• Use XACML datatypes – in format natural to language
• Mostly to be used by infrastructure components
  – Occasionally application may need to provide data
  – Infrastructure could be Container, Aspects, tool-generated code, etc.
Why not Java Authorization/JSR 115?

- Java Authorization (with or w/o JSR 115) based on Permissions
- Passive enforcement by container is a good idea
- Limitations to use of XACML features
  - No convenient, standard way to provide XACML inputs
  - No method to return outputs, e.g. Obligations, missing Attributes
  - New Resource type requires definition of new permissions class (recompile)
Draft API Overview

- Methods to build (and access) Request Context
- Methods to process Response Context
- “decide” method to invoke PDP
  - Single or bulk decisions
- “whatIsAllowed” method to obtain allowed alternatives
  - Operates in the context of some scope
  - Creates invokes a series of decisions
  - Returns allowed alternatives within scope
- Other convenience methods
The Input Attributes Problem

- XACML Policies operate on data provided
- Only PDP sees/evaluates policies
- What attributes should be provided?
- Where can attributes be obtained from?
- How can the proper instance value be obtained?
Attribute Manifest File

• File in XML format identifies attributes to be added to Request Context
• Name of Attribute, Issuer, datatype, location, access method, other attribute to use as key
• Not all fields may be present
• Two usecases:
  – PDP advertizes required attributes
  – PIPs are configured to add attributes to Request Context
Multiple PIP’s – Enhancing Request Context
Multiple PIP’s – Reacting to Missing Attributes