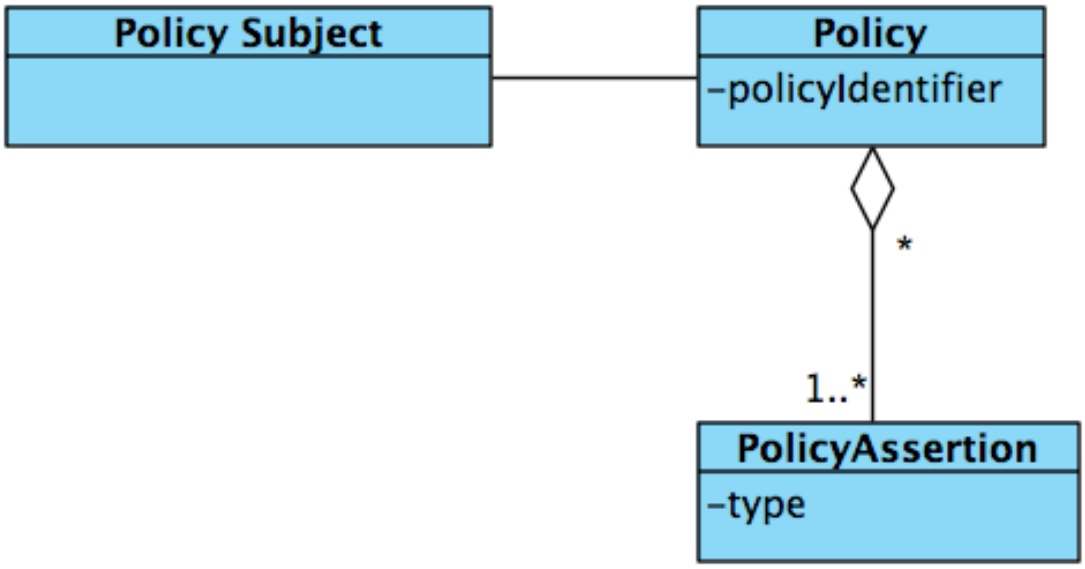
Policies – general concepts

Layered Policy Architecture – an approach to place policies within multiple layers of an architecture. For example, a policy may be placed on the access point (service interface) from which a resource may be retrieved, yet the resource itself may be also protected with a policy which must be adhered to in order to interact with the policy.



Policy Subject – an entity (e.g., an endpoint, message, resource, interaction) with which a policy can be associated.

Policy – A *policy* is a collection of policy alternatives expressing conditions that must be adhered to for a service invocation or resource inspection to be successful. If policies are not adhered to, a request to interact with a service or resource may be refused. If agreed to, it forms a contract between the parties.

Policy that is made up of several different Policy assertions may use an algebraic “AND”, “OR”, “NOR” or other types of aggregations of multiple Policy Assertions.

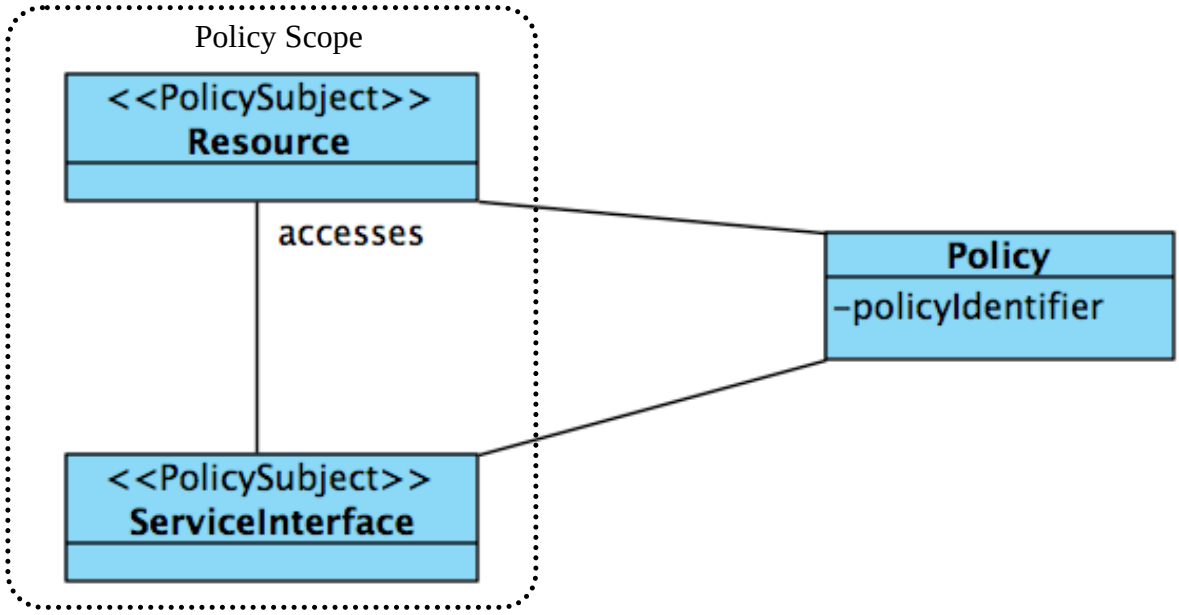


Figure XX – a layered architecture where policies are attached to both resources and access points themselves.

Policies may be associated with multiple resources of different types. This diagram depicts a policy being associated with the access mechanism (Service interface) as well as the Resource itself. Such a scenario establishes a Policy Scope.

Policy Scope – A *policy scope* is a collection of policy subjects to which a policy may apply.

Policy Identifier – a unique identifier to act as a pointer to a specific instance of a policy.

Policy Assertion – A *policy assertion* represents an individual requirement, capability, or other visible property or action of an actor, resource or

.

Policy Assertion Type – represents a specialized policy instance with assertion-specific semantics. Examples of policy assertion types are security scope, mutability rights, access rights or other special types of constraints on a policy subject.

Expressing and Attaching Policies so others can understand them is done via the following mechanisms:

Policy Vocabulary – The *policy vocabulary* of a policy is a conceptual collection of terms that can be used to build all policy assertions and any types used in the policy. This is essentially a taxonomy that can be used to make declarations of policies.

Policy Expression – an representation of a policy, readable by either human actors, application actors of both. A policy expression may be in a natural language or machine process able format such as XML.

Policy Attachment – an association class for attaching or linking a policy with one or more policy scopes.

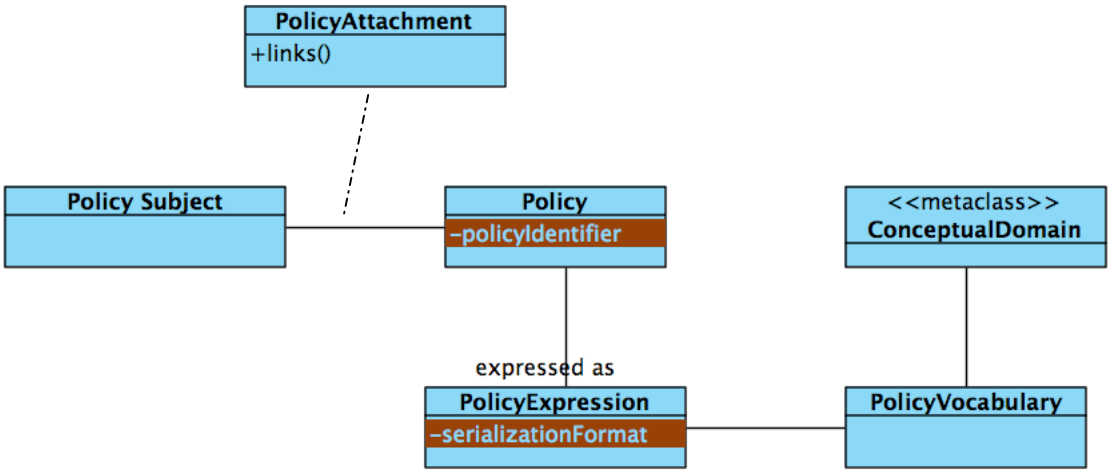


Figure X.X – a Policy Attachment used to associated a policy with a specific Policy Subject. The policy is expressed via a controlled vocabulary with agreed upon semantics from a conceptual domain.

The following mechanisms tie in to SOA Governance:

Policy Decision Point (PDP) – a point upon which an application, human or other actor must make a determination if the policy has been substantially complied with by another application, human or other actor. PDP is an important aspect for monitoring in terms of Service governance.

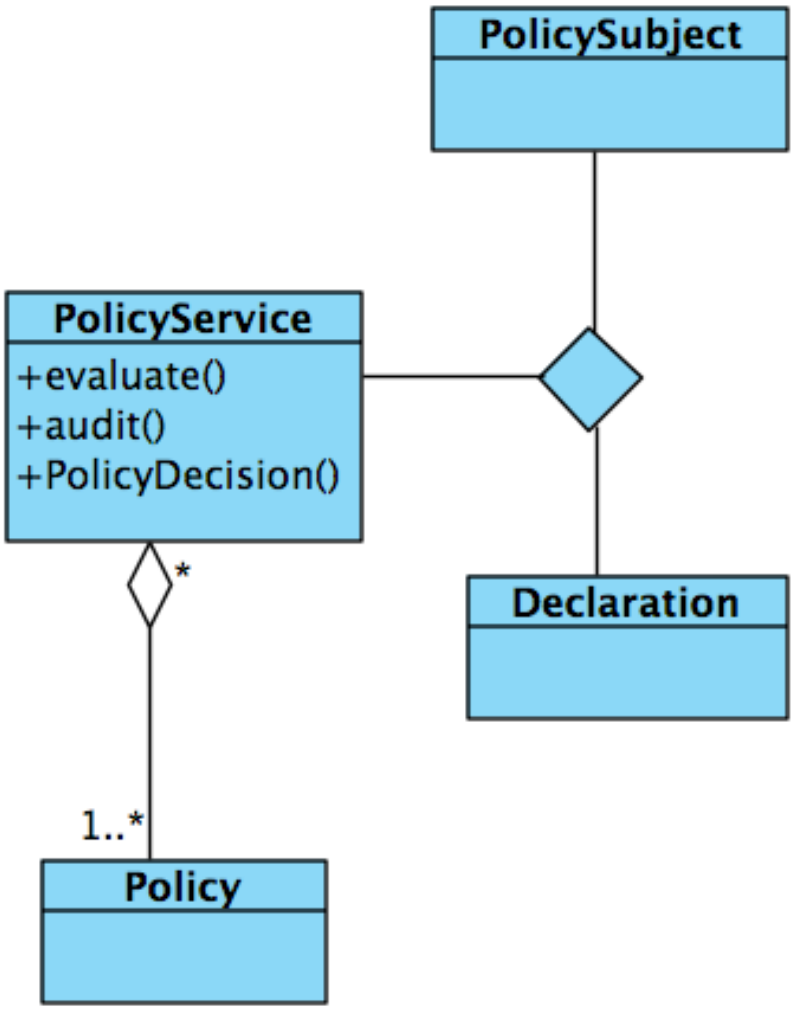


Figure X.X – governance of the policy can be done via a specific server. A policy decision point will either pass or fail based on the evaluation of the declarations to satisfy the policy. All interactions may be logged and used for governance.

Policy Service – a specialized type of service which may be tasked with accepting input and calculating whether or not a policy has been complied with in a manner acceptable to grant further access. A policy service may be used to log attempts to access resources, either directly or via access points, and report attempts, either successful or unsuccessful to a mechanism for SOA governance. See also Policy Decision Point.

Declaration – a claim made by an entity wishing to interact with a resource or endpoint in order to satisfy a Policy. Declarations may

also be logged and used for SOA Governance to help identify potential fraudulent attempts to access a resource.

Policy Audit – an audit trail of policies including meta and instance information combined to form a set of governance data for