Upcoming OMG HealthCare Resource Access Control Facility

Konstantin Beznosov
<beznosov@baptisthealth.net>
Baptist Health Systems of South Florida
What Will Be Presented

• CORBA in 5 minutes
• CORBA security model
• Why HRAC
• HRAC concepts
• HRAC framework design
• Work status
CORBA Foundations

Common Object Request Broker Architecture

• specifies a system which
  – provides interoperability between objects in a heterogeneous, distributed environment and in a way that is transparent to the programmer.

• based on OMG Object Model
CORBA Communication Model

Client

Dynamic Invocation
IDL Stubs
ORB Interface

Object Implementation

Static IDL Skeleton
Dynamic Skeleton
Object Adapter

ORB Core

Interface identical for all ORB implementations
Up-call interface

There may be multiple object adapters

There are stubs and a skeleton for each object type
Normal call interface

ORB-dependent interface

1/26/99

Courtesy of OMG
CORBA Services, Facilities, Domains, and Applications

Common Services

CORBA

Common Facilities

Vertical Domain Services

Applications
Common Services

• Security
• Event Notification
• Transactions
• Naming
• Licensing
• Trader
• Properties
• Collections

• Externalization
• Time
• Persistence
• Query Service
• Lifecycles
• Concurrency Control
• Relationships
• Change Management
CORBA Access Control Model
CORBASEC Does Not Cover Non-Object Entities
HRAC Compliments CORBASEC
HRAC High Level View

1. Application Request
2. Authorization request
3. Reply to authorization request
4. Reply to application request
Scope of the HRAC Service

1. ADO client
2. AccessDecision
3. DynamicAttributeService
4. PolicyEvaluator Locator
5. PolicyEvaluator
6. DecisionCombinator
7. AttributeEvaluator
8. Policy
9. SecuredResource
10. ResourceName
11. Operation

Relationships:
- ADO client consults DynamicAttributeService
- DynamicAttributeService consults AccessDecision
- AccessDecision consults PolicyEvaluator Locator
- PolicyEvaluator Locator consults PolicyEvaluator
- PolicyEvaluator consults DecisionCombinator
- DecisionCombinator consults AttributeEvaluator
- AttributeEvaluator consults Policy
- Policy consults SecuredResource
- ResourceName and Operation have SecuredResource
- Policy defines access policy represented by PolicyName
- PolicyEvaluator Locator locates Policy
- PolicyEvaluator locates DecisionCombinator
- DecisionCombinator locates ResourceName
- ResourceName has Operation
HRAC Framework
Scope of the HRAC Service

HRAC client

PolicyEvaluator

LocatorAdmin : PolicyLocator

PolicyEvaluator

0..*

PolicyEvaluator

1..*

PolicyEvaluator

Decision Combinator

ResourceName

1

PolicyName

0..*

Operation

1

SecuredResource

1

Policy

0..*

assigns access policy

represented by

has

represented by

assigns policy

applies policy

associates

associates

administers

administers
HRAC Status

• Initial submission
  – Submitted October 19 1998
  – presented November 10 1998, Burlingame, CA

• Revised Submission
  – Due March 1 1999
  – Presentation March 22 1999, Philadelphia

• Evaluation <hrac-eval@omg.org>