



Resource Access Decision Service (TM)

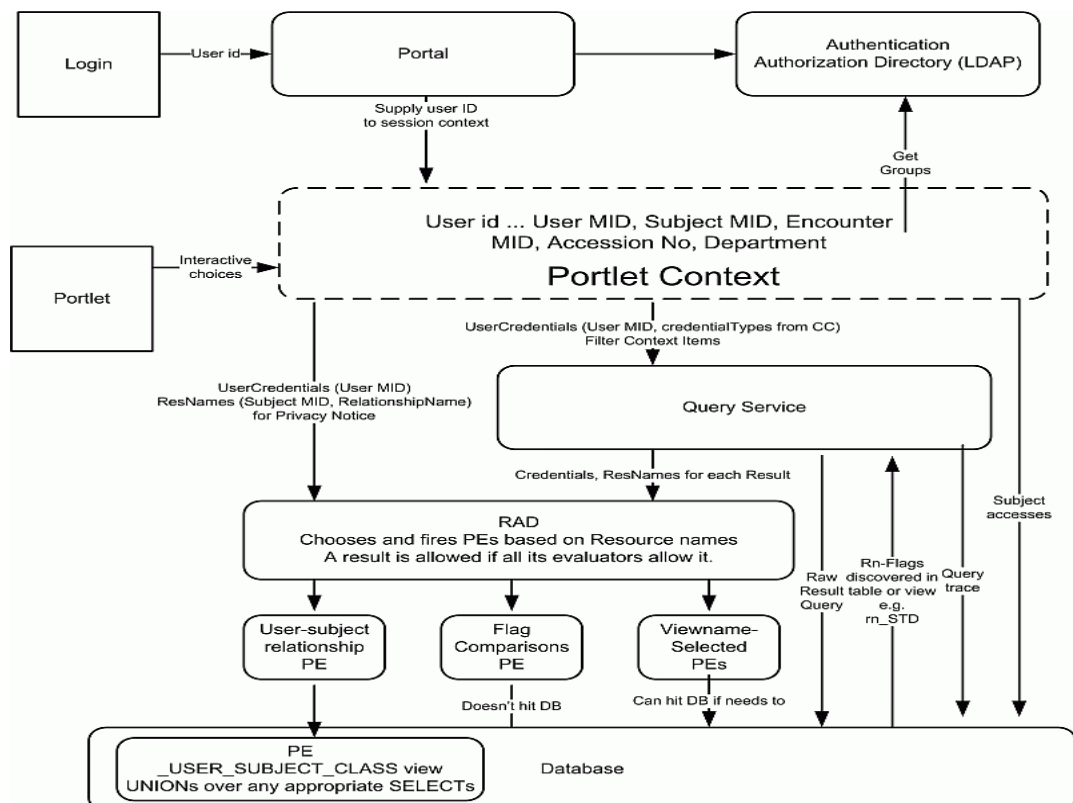
A SOA component that centralizes all access decisions for portal query data, based on a broad variety of access control policy structures

How it Works

You select and activate the policy evaluators that are appropriate to your policies. You then feed your data stamps according to your LDAP credentials schema

Deployment Modes

- You can use the RAD to make access decisions for data or for process (UI actions). In both cases, the application calls the RAD with the pertinent resource names and credentials, and the RAD returns the verdict for the application to enforce
- A RAD-compliant application (one that complies with the OMG standard specification) can use the RAD readily. The Care Data Query Service and the Care Data Correlation Channel are both RAD-compliant



For a Web Portal application, the RAD can direct filtering of query results (by Query Service) and also approve function accesses by the portal.



Features and Benefits

Manageability, Flexibility, and Interoperability

- ★★★★★ Access control logic is fragile. Adding new logic could break it. The solution: standardize on installable policy evaluators - custom policy evaluators can be written as Java Classes standardized by OMG RAD specification
- ★★★★☆ We need to maintain this centrally and use it from everywhere The solution: available for IIOP - can be called from any programming language (need a simple WSDL wrapper)

Privacy/Regulatory Compliance

- ★★★★★ We don't want anybody accessing just anybody's record The solution: use the user-subject relationships evaluator - verifies that the user has on record a recorded relationship with the subject, i.e. has-treated
- ★★★★★ Our credentials schema changes over time. How to avoid having to reprogramming the apps? The solution: use the flags-comparison evaluator, which need not be modified as credentials schema changes - easily restrict access based on roles or facilities, comparing credentials to data stamps
- ★★★★★ How to enforce specific overrides? The solution: use the authorizations and restrictions evaluator - supports consumer-specified access restrictions or overrides
- ★★★★★ We need to specially restrict just this particular view of the data. The solution: use the view-name-selected evaluator - custom access control logic to be activated upon query of a particular database table or view

Expertise

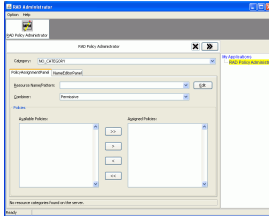
- ★★★★★ Access control is complex!... The solution: provide the staff expertise - we helped create the standard at the OMG and have applied it for a decade. It's actually not that complex once you, well, understand it! We will easily educate you beyond your industry peers in this crucial area.

Cost Savings

- ★★★★☆ We have dozens of applications to secure, and the vendors are all demanding source code customizatn contracts The solution: demand RAD compliance and wire them all to one RAD component - stop paying vendors to tweak their proprietary code. (for ORB independence we pass credentials through the API rather than through connection context)

User Interfaces

Policy Combination Editor



maintains policies that are combinations of other policies

Operations Monitor

monitors distribution of access decision outcomes

Operations Log

monitors distribution of access decision outcomes

RAD Decision and Enforcement Phases

illustrates protocol between RD and its clients

Infrastructure

Logging



Logging is handled at both operation- and trace- levels via log4j including all important context, credentials, the per-policy outcomes (verdicts), and the result row counts - It's all efficiently captured in an efficient and easy-to-harvest format

Monitoring



A moving window of access decision outcome distributions and average response times is displayed in an Excel-based monitor. It is refreshed from operation logs each minute. - see the anomalies precipitated by snoopers (need automated trend detection, not just manual)

Audit



Logs are harvested, cached, and restructured for analysis on an automated, periodic basis. A web portal page supports integrated case review. - see all facets of activity by user or by subject (need to connect the watchlist feature and add th trait changes for identity of userid)

Dependencies

Basic: CORBA Name Service

Facility: Log4J Logger

Platform: JRE

Platform: OS/Linux

Schema: cdr_owner

Pricing

We negotiate enterprise licenses of various forms. Call for current pricing models.