OASIS ebXML Registry

Proposal: Authorization Policy Administration

Category: New functionality to draft specifications

Date: July 9, 2001

Author: Farrukh Najmi

Status of this Document

This document is a draft proposal whose purpose is to solicit additional input.

1 Abstract

This document proposes focused enhancements to the ebXML Registry Services specification that will define a normative interface to defining authorization policies based on identity, role and group that may be associated with registry requests.

Currently [ebRIM] supports such capability at the information model level. However, there are no interfaces defined in [ebRS] to take advantage of these information model elements. In [ebRS] V1 only pre-defined roles and implicit authorization policies were specified.

The proposal is to provide a normative specification for authorization policy specification, submission and management that is based upon [ebRIM].

2 Motivation

The primary motivation is make the ebXML registry more capable and useful by providing powerful security (authorization) mechanisms. Authorization policies enable sharing of private information with selected partners in a public registry. This is a compelling feature that builds upon the advanced security capabilities of the ebXML Registry V1.

3 Proposed Deliverables

The following concrete deliverables are proposed:

1. Updating ebRIM only if necessary.

2. Update Rgeistry.dtd to include specification of Authorization policies.
3. Update security chapter in [ebRS] to include normative specification of how to submit and manage authorization policies.

It is anticipated that authorization rules will be defined as XML elements and will be submitted and managed like any other data using the ObjectManager interface.

4 Use Cases

4.1 Limiting Read-Only Access

A company submits data to a public registry and wishes that data to be read only by its selected partners. It submits an Authorization policy associated with the data that allows only User's from partner companies to have read-only access to the data.

This is currently not possible in V1. In V1, any one is allowed to read anyone else's content. Data submitted to the registry is treated as public data that is visible to all.

4.2 Granting Write Access to Others

A company submits data to a public registry and wishes that data to be modifiable (and delete-able) by its selected partners. It submits an Authorization policy associated with the data that allows any User from partner companies to have write access to the data.

This is currently not possible in V1. In V1, only the submitter is allowed to modify that data.