Registry and Repository Face to Face
Sun Microsystems in Burlington, MA
January 5, 2001

Participants

Scott Nieman, Norstan Consulting
Farrukh Najmi, Sun
Yutaka Yoshida, Sun
Len Gallagher, NIST
Mike Kass, NIST
Sally Fuger, AIAG

Attending by teleconference:
Krishna, CISCO

Omissions From Day 1 Summary

?? Len was not in favor of supporting content based queries
?? If we use XPATH then all Objects should have the URI attribute. Decision to move URI attribute from ExtrinsicObject to Object. Recall that's where it used to be. Issue was raised whether we need UUID. It was mentioned that an object may have multiple URI. Decision to leave UUID in model for release 1 and ask TA to resolves UUID issue for release 2.
?? We will put the revised ad hoc query proposal to a team vote over the mailing list
?? The final pre-QR version of the RS document will be put up for a team vote over the mailing list

Security Discussion

We started the day with a review of the security chapter of RIM. We walked through Fig 10 and reviewed the requirements for registry security. We added "illustrative not prescriptive" to Fig 10 in response to Len's concern that the security model was too complex. We agreed to remove Security Clearance from the model.

Concerns Regarding Security

Len expressed the following concerns:

1. Model is more complex than it needs to be
2. Impossible to support custom AccessControlPolicy (ACP) because there would be separate ACP on every object instance. NAICS classification scheme has 3000+ nodes. Do they each have an ACP and associated Permissions, Privileges etc.?
3. Fig 10 does not show how ACP defines who can create/submit an object
4. Missing pre-defined role of ResponsibleOrganization

Responses To Concerns

1. We discussed that the security model is designed to support future customizable ACP capability and is general enough to allow for identity and group based privileges in the future. For release 1 a subset of the model may be implemented to support default role-based authorization based on the default ACP.
2. It was clarified that in release 1 a single default ACP instance, about 50 Permission instances and less than 10 Privelege and PrivilegeAttribute instances would be sufficient to implement the default role based authorization. In release 2 with ability to submit custom ACP, in the NAICS example it is likely that the NAICS submitter would submit somewhere between 1 to 5 ACPs for the entire scheme. While theoretically it is possible to submit an ACP for every node, in practice each submitter would have a handful of ACPs that they would use with all their submitted content.
3. In release 1 anyone can submit content.

4. Release 1 has 3 pre-defined roles based on the needs of release 1 security requirements. In release 2 submitters could define arbitrary roles and we could choose to make ResponsibleOrganization a pre-defined roles.

Summary Of Registry Security

The current security sections meet the requirements for release 1 with minimal change to the RIM and RS specifications. The security section will have a team vote over the mailing list.