Fedora XACML Attributes

These are the standard attributes that are supplied by the Fedora XACML AuthZ Delegate. As a point of reference, here are the standard fedora attributes from the FeSL implementation of XACML.

Subject Attributes

ID	DataType	Source	In Request?	Notes
`urn:oasis:names:tc:xacml:1.0:subject:subject-id`	string	user principal	Yes	
`urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier`	string	TBD		name-space for the subject-id
`urn:oasis:names:tc:xacml:1.0:subject:request-time`		AuthZ delegate	Yes	time when this action was requested
`urn:oasis:names:tc:xacml:1.0:subject:session-start-time`		ModeShape session	Yes	time when Fedora transaction began
`urn:oasis:names:tc:xacml:2.0:subject:group`	string	all principals except user	Yes	extensible via Principal Factory
`fcrepo-xacml:subject-role`	string	effective access roles	Yes	Fedora access roles for this user /group† XACML Role-Based Access Control Profile
`urn:oasis:names:tc:xacml:1.0:subject:authn-locality:authentication-method`	string	TBD	Yes	what style of AuthN? (OAuth /Tomcat/Shibboleth)
~~`urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-address`~~	~~string~~	~~TBD~~	~~Yes~~	address of authenticating agent: • OAuth authorization server • SSO server • fedora server (tomcat users)
`urn:oasis:names:tc:xacml:1.0:subject:authn-locality:dns-name`	string	TBD	Yes	See above description of ip-address.

† Hydra rights metadata may be dynamically crosswalked to Fedora roles via a sequencer.

Action Attributes

ID	Data Type	Source	In Request?	Notes
`urn:oasis:names:tc:xacml:1.0:action:action-id`	string	ModeShape action	Yes	See ModeShapePermissions list
`urn:oasis:names:tc:xacml:1.0:action:action-namespace`	string	preset	Yes	A TBD namespace referring to modeshape actions.

Resource Attributes

Question: What kind of URI shall we use for pointing at resources in Fedora/ModeShape policies? This decision will mostly be of concern to ResourceAttributeFinders, since policies will not usually refer to individual resource IDs directly.

ID	Data Type	Source	In Request?	Notes
`urn:oasis:names:tc:xacml:1.0:resource:resource-id`	string	Fedora path	Yes	The full Fedora path to the resource or propery (with extra hierarchy compressed away)
~~`urn:fedora:xacml:2.0:resource:resource-uri`~~	~~URI~~	~~Fedora URI~~	~~Yes~~	~~Fedora graph subject URI for this resource~~
~~`urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor-or-self`~~	~~string~~	~~Fedora path~~	~~Yes~~	~~Set of paths for this resource and its ancestors~~
`fcrepo-xacml:resource-parent`	string	Fedora path	Yes	Path of the parent of the resource (always an existing resource, in session if not saved to workspace)
~~`urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor`~~	~~string~~	~~Fedora path~~	~~Yes~~	~~Set of paths of all ancestor resources~~

`fcrepo-xacml:resource-workspace`	string	ModeShape session	Yes	Name of the workspace
`urn:oasis:names:tc:xacml:1.0:resource:scope`	string	AuthZ Delegate	Yes	If the action impacts child resources, then value will be "Descendants", otherwise it will be "Immediate". A "remove" is an example of such an action.‡

‡ Further research is needed to figure out the semantics of a ModeShape move operation and how policies shall be enforced.

RDF Predicates as Dynamic Resource Attributes

There are many RDF predicates that are available in the graph for Fedora resources. These include numerous properties like mime-type, binary size, and even checksum. Without trying to predict which of these will be useful in policies, Fedora XACML can reference any predicate URI as a resource attribute ID.

Here are some examples of these resource attributes:

ID	Data Type	Source	In Request?	Notes
http://www.w3.org/1999/02/22-rdf-syntax-ns#type	URI	ModeShape property (via RDF property)	No	Primary Types and mixin types defined in CNDs will be returned in this attribute

Environment Attributes

ID	Data Type	Source	In Request?	Notes
`urn:oasis:names:tc:xacml:1.0:environment:current-time`	time	AuthZ Delegate	Yes	
`urn:oasis:names:tc:xacml:1.0:environment:current-date`	date	AuthZ Delegate	Yes	
`urn:oasis:names:tc:xacml:1.0:environment:current-dateTime`	dateTime	AuthZ Delegate	Yes	
`urn:fedora:xacml:2.0:environment:original-ip-address`	string	request IP or header	Yes	the IP of the original client (may be forwarded by a proxy application