Entitlements: Definition and Use Cases

– Anil Saldhana, Red Hat Inc

Version 1.0.0a

**Definition**
Entitlement in the context of an access control decision is a privilege for an user or a process to perform or have rights to an action on a resource.

**Use Cases**

**Cloud Entitlements**

![Diagram: Cloud Enforcement versus Entitlement model]

There are two typical cloud authorization scenarios. This is highlighted in the diagram.

In the first scenario which is termed as the “Cloud Enforcement Scenario”, there is a need to authorize a cloud action on a resource by an identity (user, process or server). The scenario involves an
authorization check with the possible answers to be Permit, Deny or NotApplicable (in the XACML terms). This is the scenario that has been worked on by the Oasis XACML as well as the IETF OAuth2 committees.

The second scenario called the “Cloud Entitlements Scenario” involves the use of entitlements. There are entitlement points in the cloud architecture that are trying to determine all the entitlements an identity (user, process or server) has, at any given instance of time. This particular scenario has not been undertaken by any standards bodies, even though it is a common use case in the cloud paradigm. In this scenario, a Cloud Entitlement Point (CEP) asks a Cloud Authorization Server for the entitlements a subject or identity has within a family $F$. The Cloud Authorization Server (based on configured policies) will return a set of entitlements that belong to the family $F$, that the subject/identity has.

There is a need to define a family of entitlements $F$ that contains a collection of entitlements $E$. 