

The lobster authorization model

Lobber *authentication* follows the usual pattern for federated identity: the lobster web application is a relying party (aka SP) to one or more identity providers (possibly part of one or more identity federations). Each identity provider is expected to provide a small set of attributes for each user: eduPersonPrincipalName or eduPersonTargetedId, displayName or cn and mail.

The eduPersonPrincipalName or eduPersonTargetedId values are used as permanent user identifiers in Lobber. In addition the Lobber web application also uses the eduPersonEntitlement attribute for its authorization model.

The eduPersonEntitlement attribute contains a set of URNs, each can be thought to represent a 'right' or 'membership'. Lobber expects the eduPersonEntitlement values to be unique within the scope of the identity providers trusted by Lobber to provide this attribute.

The Lobber web application essentially stores a single object: a *Torrent* which represents metadata about a dataset. Each time a user uploads data to Lobber a Torrent object is created. Should the same dataset be uploaded twice, two separate Torrent objects are created. This means that if two users upload the same file (the same in the sense that their Torrent infohash are identical), two Torrent files are nevertheless created. Only when the last Torrent object referring to a dataset is removed will the actual datasets be purged from storage nodes holding it.

One of the reasons for this model is so that users may separately assign rights to the same underlying data.

Torrent objects has a list of access control entries (or ACEs) associated with it (forming an access control list or ACL). Each ACE is on the form:

```
ace = entitlement '#' right
right = 'r' / 'w' / 'd'
```

Where entitlement corresponds to an entitlement held by a user. The 'r' right gives permission to read, the 'w' permission to write and 'd' permission to delete the Torrent object. As an example, the ACE urn:x-lobber:foo#w would grant permission to write to any user with urn:x-lobber:foo among the set of values of the eduPersonEntitlement attribute.

In order to be able to assign rights to individual users ACEs of the form user '#' uid is used to represent the user with Lobber user identifier uid. For instance user:test@example.org#d would grant delete permission to the Lobber user with eduPersonPrincipalName test@example.org.

Finally the entitlement "" (the empty string) represents all users. To illustrate, the ACE #r grants read access to all users.