Krishna Yellepeddy

30 June 2010

Draft proposal for Group as a new managed object in KMIP

Use cases for group as a new managed object in KMIP

1. Allow creation of groups of heterogeneous or homogeneous managed objects.
   - Example: Create a homogeneous group of symmetric keys. This set of symmetric keys is treated as a resource and access control is enforced on it. E.g. a set of tape drives of a particular type have access to this group of keys.
   - Create a heterogeneous group of cryptographic objects consisting of asymmetric keys, certificates and secret data. This heterogeneous group may represent a user's credentials for logging on to different applications such as their Gmail account, Facebook account, relational database etc. The user/owner retrieves this group and uses the credentials in the group for signing on to different applications.

2. Assign properties to the group governing how elements in the group are served out for use. This could be thought of as a cursor pattern which is specified at the time of creation of the group. For example:
   a) for a group of symmetric keys, security policy for FIPS compliance may dictate that a key should be served out only once for use by a client for encrypting data. When all the keys have been served out from a group, server returns an error that there are no new keys available. Note that a key can be used any number of times to decrypt data
   b) for a different group of symmetric keys, keys may be served out in a round robin fashion. In this example a key may be served out more than once for encrypting data

3. For a heterogeneous group of elements (e.g. credentials) being managed for a user, user may cache this group of objects and want to be notified by the server if any of the elements in the group have been modified. If they have been modified, then the user refreshes the cache.

Definition of a Group

- A group contains zero or more managed objects, excluding other groups.
- Objects in a group may be heterogeneous or homogeneous. When a group is created, we define whether the group will have heterogeneous or homogeneous objects.
- Group members are represented by uuids for objects that exist on the KMIP server where the group is being created
- Should an object be allowed to belong to more than one group ? This complicates access control. Would like to discuss this at the TC and get feedback on whether this should be allowed.

BACKUP

KMIP Operations permitted on a Group object

KMIP Operation	Supported for Group ?	Comments
Create	N/A	
AddToGroup	New operation for Group objects	Add member to a group by specifying the uuid of the member.
Create Key Pair	N/A	
Register	Y. Extended to support Groups	Register a group. It has no members at this point. During registration specify whether Group will have heterogeneous objects or homogeneous objects and what the cursor pattern to use is.. For homogeneous objects, client would have to specify the managed object type. Use AddToGroup to add members to a group
Re-key	N/A	
Derive Key	N/A	
Certify	N/A	
Locate	Y	
Check	N/A	Check should be against individual members of a group, and only if it is meaningful
Get	Y	Returns the Group managed object including the uuids of members, but does not perform 'get' of the members. (Issue: what happens if the list of members is huge? We need a way to get sub-lists of members back).

KMIP Operations permitted on Group object continued…

KMIP Operation	Supported for Group ?	Comments
Get Attributes	Y	Return the attributes for the group, not for individual members of the group
Get Attribute List	Y	Returns attribute list for the group, not for individual members of the group
Add Attribute	Y	Add attribute to the group object, not for individual members of the group
Modify Attribute	Y	Modify attribute for the group, not for individual members of the group
Delete Attribute	Y	Delete attribute for the group, not for individual members of the group
Obtain Lease	N/A	
Get Usage Allocation	N/A	
Activate	Y	Activate does not apply to Templates. So what happens if a group containing just Templates ? One option is to say that activate is a no-op for template members of a group.
Revoke	N/A	

KMIP Operations permitted on Group object continued…

KMIP Operation	Supported for Group ?	Comments
Destroy	Y	Destroy on a group does not destroy members of the group, just the group object; the server would need to remove all links from member objects to the destroyed group. This is an asynchronous call
Archive	Y	All members of the group are archived. If a client wants to archive a single member of a group, they still have the option to do so. Each member's archive flag is set. This is an asynchronous call.
Recover	Y	All members of the group are recovered. If a client wants to recover a single object as opposed to the entire group, they still have the option to do so. This is an Asynchronous call.
Validate	N/A	
Query	Y	
Cancel	N/A	
Poll	N/A	
Notify	Y	
Put	Y	