Client Controlled Identifiers

Tim Chevalier

Problem

- Some KMIP “compatible” devices (example Key Per IO, or KPIO) will need to have objects (keys/wrapped keys) “pushed” into them
- The “client” may be the one producing the objects, or the objects may have been generated on an external KMIP server
- The “client” would like to Register the key on the KPIO device, but needs to control the UUID field associated with the object (i.e we don’t want the device generating the UUID)

Solution

- Allow Register (and other objects) to specify the UUID in the set of attributes associated with the object
- If specified, the server (KPIO device, for example), uses that as the UUID
- If the KMIP client's suggested UUID conflicts with a UUID already being used by the server, then the server returns an error
- Servers shall recognize a standard format for a UUID and may choose to accept other UUID formats

Example spec changes

6.1.49 Register

…

If the client provides a Unique Identifier value in the set of attributes, the server SHALL use the provided Unique Identifier value unless the Unique Identifier value is already in use within the server (and in which case the server SHALL return a Result Reason of Object Already Exists). A server SHALL accept Unique Identifier values specified as universally unique identifiers represented as 32 hexadecimal (base-16) digits, formatted in five groups of digits separated by hyphens, in the form 8-4-4-4-12 for a total of 36 characters (32 hexadecimal characters and 4 hyphens). A server MAY also accept other formats of Unique Identifier values.

The response contains the Unique Identifier assigned by the server or specified by the client to the registered object. The server SHALL copy the Unique Identifier returned by this operation into the ID Placeholder variable. The Initial Date attribute of the object SHALL be set to the current time.

Example error handling

1.1.1.1 Error Handling – Register

Result Status	Result Reason
Operation Failed	Attribute Read Only, Attribute Single Valued, Bad Password, Encoding Option Error, Invalid Attribute, Invalid Attribute Value, Invalid Object Type, Non Unique Name Attribute, Server Limit Exceeded, Attestation Failed, Attestation Required, Feature Not Supported, Invalid Field, Invalid Message, Object Already Exists, Operation Not Supported, Permission Denied, Protection Storage Unavailable, Response Too Large