Specification Changes from KMIP Template Examples Discussion
Bruce Rich / Tim Hudson - October 4th, 2012

Tim: templates are treated using the same rules as other managed objects and the distinction between attributes associated with or of a template and the attributes that a template provides to objects that reference it is explicitly set by the user

Tim: the register-with-no-object option is removed

Note: shown first with change tracking and then with changes accepted.

2.2.6 Template

A *Template* is a named Managed Object containing the client-settable attributes of a Managed Cryptographic Object ~~(i.e., a stored, named list of attributes)~~. A Template is used to specify the attributes of a new Managed Cryptographic Object in various operations. ~~It is intended to be used to specify the cryptographic attributes of new objects in a standardized or convenient way.~~

~~None of the client-settable a~~Attributes specified in a Template ~~except the Name attribute apply to the template object itself, but instead~~ apply to any object created <u>that references the</u> ~~using the~~ Template <u>by name using the Name object in any of the Template-Attribute structure in section 2.2.9</u>.

<u>The name of a Template (as it is for any Managed Object) is specified as an Attribute in the Template-Attribute structure in the Register operation where the Attribute Name is "Name" and the Attribute Value is the name of the Template Managed Object.</u>

~~The Template MAY be the subject of the Register, Locate, Get, Get Attributes, Get Attribute List, Add Attribute, Modify Attribute, Delete Attribute, and Destroy operations.~~

~~An attribute specified in a Template is applicable either to the Template itself or to objects created using the Template.~~

~~Attributes applicable to the Template itself are: Unique Identifier, Object Type, Name, Initial Date, Archive Date, and Last Change Date.~~

~~Attributes applicable to objects created using the Template are:~~

- ~~Cryptographic Algorithm~~
- ~~Cryptographic Length~~
- ~~Cryptographic Domain Parameters~~
- ~~Cryptographic Parameters~~
- ~~Certificate Length~~
- ~~Operation Policy Name~~
- ~~Cryptographic Usage Mask~~
- ~~Digital Signature Algorithm~~
- ~~Usage Limits~~
- ~~Activation Date~~
- ~~Process Start Date~~
- ~~Protect Stop Date~~
- ~~Deactivation Date~~
- ~~Object Group~~
- ~~Application Specific Information~~
- ~~Contact Information~~
- ~~Custom Attribute~~

Object	Encoding	REQUIRED
Template	Structure	
Attribute	Attribute Object, see 2.1.1	Yes. MAY be repeated.

Table 1: Template Object Structure

4.3 Register

This operation requests the server to register a Managed Object that was created by the client or obtained by the client through some other means, allowing the server to manage the object. The arguments in the request are similar to those in the Create operation, but ~~also MAY~~ contain the object itself for storage by the server. ~~Optionally, objects that are not to be stored by the key management system MAY be omitted from the request (e.g., private keys).~~

The request contains information about the type of object being registered and some of the attributes to be assigned to the object (e.g., Cryptographic Algorithm, Cryptographic Length, etc). This information MAY be specified by the use of a Template-Attribute object.

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

Request Payload		
Object	**REQUIRED**	**Description**
Object Type, see 3.3	Yes	Determines the type of object being registered.
Template-Attribute, see 2.18	Yes	Specifies desired object attributes using templates and/or individual attributes.
Certificate, Symmetric Key, Private Key, Public Key, Split Key, Template Secret Data or Opaque Object, see 2.2	~~No~~Yes	The object being registered. The object and attributes MAY be wrapped. ~~Some objects (e.g., Private Keys), MAY be omitted from the request.~~

Table 2: Register Request Payload

2.2.6 Template

A *Template* is a named Managed Object containing the client-settable attributes of a Managed Cryptographic Object. A Template is used to specify the attributes of a new Managed Cryptographic Object in various operations.

Attributes specified in a Template apply to any object created that references the Template by name using the Name object in any of the Template-Attribute structures in section 2.2.9.

The name of a Template (as it is for any Managed Object) is specified as an Attribute in the Template-Attribute structure in the Register operation where the Attribute Name is "Name" and the Attribute Value is the name of the Template Managed Object.

Object	Encoding	REQUIRED
Template	Structure	
Attribute	Attribute Object, see 2.1.1	Yes. MAY be repeated.

Table 3: Template Object Structure

4.3   Register

This operation requests the server to register a Managed Object that was created by the client or obtained by the client through some other means, allowing the server to manage the object. The arguments in the request are similar to those in the Create operation, but contain the object itself for storage by the server.

The request contains information about the type of object being registered and some of the attributes to be assigned to the object (e.g., Cryptographic Algorithm, Cryptographic Length, etc). This information MAY be specified by the use of a Template-Attribute object.

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

Request Payload		
Object	**REQUIRED**	**Description**
Object Type, see 3.3	Yes	Determines the type of object being registered.
Template-Attribute, see 2.1.8	Yes	Specifies desired object attributes using templates and/or individual attributes.
Certificate, Symmetric Key, Private Key, Public Key, Split Key, Template Secret Data or Opaque Object, see 2.2	Yes	The object being registered. The object and attributes MAY be wrapped.

Table 4: Register Request Payload