Proposal for Conformance

Propose removing Clause 1.8 (Compliance) in the Specification and Usage Guide

Specification Lines 40 to 41

Usage Guide Lines 31 to 32

Propose removing clause 5 of the Usage Guide, adding conformance clause (clause 13) of the specification and to include four sub-clauses. Sub-clauses include defining claim of conformance using current verbiage listed in Clause 13 (moved to sub-clause 13.1), defining a standard for referencing KMIP within other standards (sub-clause 13.2), defining a standard for using portions of KMIP within another standard without claiming conformance (sub-clause 13.3) and defining extensions to KMIP objects, attributes, operations and profiles (sub-clause 13.4).

Propose addition of conformance table in either the conformance section or for server and client requirements to remove ambiguities (having to read) of what is required versus what is not. In this proposal it is shown as an appendix. Consider placing this in the Usage Guide as informational in place of clause 5.

It may also be desirable to add a single line table to each object, attribute, operation and message that contains Client and Server requirements for the specific object, attribute, operation and message so there is no misunderstanding about what is required to claim conformance.

5 Conformance

TBD

5.1 Claiming Conformance with KMIP Standard

Server implementations of the KMIP protocol must support all objects, attributes, operations and profiles not specified as “optional” in the KMIP Specification in order to be conformant to the specification. Server implementations that do not support objects, attributes, operations and profiles defined as “optional” can claim KMIP conformance, though they may be limited in terms of interoperability with other KMIP implementations.

Client implementations of the KMIP protocol may implement any subset of the KMIP protocol. For example, a client may implement only the Get and Locate operations for symmetric keys. In order to claim conformance, however, such a client must implement all aspects of any elements of the protocol (objects, attributes, operations, profiles) that it claims to support. In the example of Get/Locate support for symmetric keys, therefore, a conforming client implementation must support all required attributes for symmetric keys.

For a complete list of conformance requirements see Appendix A.

5.2 Referencing KMIP Standard in Other Standards

When referencing KMIP as a component of a different standard in order to claim conformance all requirements of clause 5.1 must be maintained and attribution must be given to OASIS and the KMIP Technical Committee.

When mapping functions between KMIP and other standards, tables must be created to show mapping both to and from KMIP into the other standard.

5.3 Using Portions of KMIP Standard in Other Standards without Claiming Conformance

When using a subset of elements of the KMIP Standard including objects, attributes, operations or profiles it is mandatory to support all required components (objects, attributes, operations and profiles) of the element being utilized.

KMIP optional components may be required at the discretion of the specific standard as long as it is noted that the component is not required for support in KMIP.

In this case claiming conformance may not be an issue but in order to make use of any portion of KMIP attribution must be given to OASIS and the KMIP Technical Committee for all elements used.

5.4 Defining Extensions to KMIP Standard for Use in Other Standards

Defining extensions to KMIP within other standards is approved if the extensions fall within defined extension ranges of the KMIP specification.

If compliance is to be claimed then all requirements found in clause 5.2 apply. If compliance is not claimed then all requirements in clause 5.3 apply.

TBD item: registration of extensions

A. Conformance Requirements

The following table lists requirements for Server and Client for objects, attributes and operations. For Object, Attribute and Operation requirements see the appropriate clause.

Element (Object, Attribute or Operation)	Clause	Required	
		Server	Client
Attribute	2.1.1	Yes or No	Yes, No or N/A
Credential	2.1.2		
Key Block	2.1.3		
Key Value	2.1.4		
Key Wrapping Data	2.1.5		
Key Wrapping Specification	2.1.6		
Transparent Key Structure	2.1.7		
Template-Attribute Structure	2.1.8		
Certificate	2.2.1		
Symmetric Key	2.2.2		
Public Key	2.2.3		
Private Key	2.2.4		
Split Key	2.2.5		
Template	2.2.6		
Policy Template	2.2.7		
Secret Data	2.2.8		
Opaque Object	2.2.9		
Unique Identifier	3.1		
Name	3.2		
Object Type	3.3		
Cryptographic Algorithm	3.4		
Cryptographic Length	3.5		
Cryptographic Parameters	3.6		
Certificate Type	3.7		
Certificate Issuer	3.8		
Certificate Subject	3.9		
Digest	3.10		

Element (Object, Attribute or Operation)	Clause	Required	
		Server	Client
Operations outside of operation policy control	3.11.1		
Default Operation Policy	3.11.2		
Cryptographic Usage Mask	3.12		
Lease Time	3.13		
Usage Limits	3.14		
State	3.15		
Initial Date	3.16		
Activation Date	3.17		
Process Start Date	3.18		
Protect Stop Date	3.19		
Deactivation Date	3.20		
Destroy Date	3.21		
Compromise Occurrence Date	3.22		
Compromise Date	3.23		
Revocation Reason	3.24		
Archive Date	3.25		
Object Group	3.26		
Link	3.27		
Application Specific Identification	3.28		
Contact Information	3.29		
Last Changed Date	3.30		
Custom Attribute	3.31		
Create	4.1		
Create Key Pair	4.2		
Register	4.3		
Re-key	4.4		
Derive Key	4.5		
Certify	4.6		
Re-certify	4.7		
Locate	4.8		
Check	4.9		
Get	4.10		

Element (Object, Attribute or Operation)	Clause	Required	
		Server	Client
Get Attributes	4.11		
Get Attribute List	4.12		
Add Attribute	4.13		
Modify Attribute	4.14		
Delete Attribute	4.15		
Obtain Lease	4.16		
Get Usage Allocation	4.17		
Activate	4.18		
Revoke	4.19		
Destroy	4.20		
Archive	4.21		
Recover	4.22		
Validate	4.23		
Query	4.24		
Cancel	4.25		
Poll	4.26		
Notify	5.1		
Put	5.2		