KMIP Server Conformance Proposal

Subject: Proposal to create a baseline conformance profile for the KMIP Server Conformance Target

Date: 2009-09-02

Contact: Matt Ball, Sun Microsystems, Inc.

Contributors: See authors of [Sym] and [ConSec]

Revision History

- 2009-09-02: Initial version based on “Base Symmetric Key Profile Proposal” by Bruce A. Rich (IBM), which in turn was derived from “Proposal for Modification to Conformance Section” by Bob Lockhart, et al.

Overview

OASIS requires a conformance section in an approved committee specification (see [TCProc], section 2.18 Specification Quality):

> A specification that is approved by the TC at the Public Review Draft, Committee Specification or OASIS Standard level must include a separate section, listing a set of numbered conformance clauses, to which any implementation of the specification must adhere in order to claim conformance to the specification (or any optional portion thereof).

This proposal intends to meet this OASIS requirement by proposing a baseline profile for the KMIP Server Conformance Target (see [Conform]).

This proposal is a subset of the work produced by [Sym] and [ConSec], with the intention that the group can add these previous proposals at a later time, possibly into a new document.

References

[Conform] OASIS Guidelines to Writing Conformance Clauses. See http://docs.oasis-open.org/templates/TCHandbook/ConformanceGuidelines.html

[TCProc] OASIS Technical Committee Process. See http://www.oasis-open.org/committees/process.php

[Sym] Bruce A. Rich, “Base Symmetric Key Profile Proposal”. See https://www.oasis-open.org/apps/org/workgroup/kmip/download.php/33818/Conformance_Clause_Proposal_V3_Base_SymmetricKey_V2.doc

[ConSec] Bob Lockhart, et al, “Proposal for Modification to Conformance Section”, See https://www.oasis-open.org/apps/org/workgroup/kmip/download.php/33327/Conformance_Clause_Proposal_V3.doc

Proposed Changes against KMIP Usage Guide

Remove clause 5 (Conformance) of the KMIP Usage Guide (version from July 28, 2009 or later).

Proposed Changes against KMIP Specification

The following text proposes additions to KMIP draft revision 0.98, dated August 27, 2009.

1 Introduction

1.8 Implementation Conformance

The key words "SHALL", "SHALL NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. The words ‘must’, ‘can’, and ‘will’ are forbidden.

An implementation is a conforming KMIP Server if the implementation meets the conditions in 1.8.1.

An implementation SHALL be a conforming KMIP Server.

If an implementation claims support for a particular clause, then the implementation SHALL conform to all normative statements within that clause.

{Editor’s Note: If we later add a KMIP Client Conformance Clause, then we would change the previous statement to something like this: “An implementation SHALL be a conforming KMIP Server, a conforming KMIP Client, or both a conforming KMIP Server and a conforming KMIP Client”. If we add multiple KMIP Server Conformance Clauses, then we’ll have to rework this language again}

1.8.1 Conformance as a KMIP Server

An implementation conforms to this specification as a KMIP Server if it meets the following conditions:

1. Supports the following objects (see clause 2):
    a. Attribute (see 2.1.1)
    b. Credential (see 2.1.2)
    c. Key Block (see 2.1.3)
    d. Key Value (see 2.1.4)
    e. Transparent Key Structure (see 2.1.7)
    f. Template-Attribute Structure (see 2.1.8)
2. Supports the following attributes (see clause 3):
    a. Unique Identifier (see 3.1)
    b. Name (see 3.2)
    c. Object Type (see 3.3)
    d. Cryptographic Algorithm (see 3.4)
    e. Cryptographic Length (see 3.5)
    f. Cryptographic Parameters (see 3.6)
    g. Digest (see 3.10)
    h. Default Operation Policy (see 3.11.2)
    i. Cryptographic Usage Mask (see 3.12)
    j. State (see 3.15)
    k. Initial Date (see 3.16)
    l. Activation Date (see 3.17)
    m. Process Start Date (see 3.18)
    n. Protect Stop Date (see 3.19)
    o. Deactivation Date (see 3.20)
    p. Destroy Date (see 3.21)
    q. Compromise Occurrence Date (see 3.22)
    r. Compromise Date (see 3.23)

s. Revocation Reason (see 3.24)
t. Archive Date (see 3.25)

3. Supports the following client-to-server operations (see clause 4):
    a. Create (see 4.1)
    b. Locate (see 4.8)
    c. Check (see 4.9)
    d. Get (see 4.10)
    e. Get Attribute (see 4.11)
    f. Get Attribute List (see 4.12)
    g. Add Attribute (see 4.13)
    h. Modify Attribute (see 4.14)
    i. Delete Attribute (see 4.15)
    j. Activate (see 4.18)
    k. Revoke (see 4.19)
    l. Destroy (see 4.20)
    m. Query (see 4.24)
4. Supports the following message contents (see clause 6):
    a. Protocol Version (see 6.1)
    b. Operation (see 6.2)
    c. Maximum Response Size (see 6.3)
    d. Unique Message ID (see 6.4)
    e. Time Stamp (see 6.5)
    f. Asynchronous Indicator (see 6.7)
    g. Result Status (see 6.9)
    h. Result Reason (see 6.10)
    i. Result Message (see 6.11)
    j. Batch Order Option (see 6.12)
    k. Batch Error Continuation Option (see 6.13)
    l. Batch Count (see 6.14)
    m. Batch Item (see 6.15)
5. Supports Message Format (see clause 7)
6. Supports Authentication (see clause 8)
7. Supports the TTLV encoding (see 9.1)
8. Supports the following transports (see clause 10):
    a. HTTP1.1 port for Query operations
    b. Raw port for Query operations
    c. HTTP1.1 port for operations other than Query, using HTTPS and client-side certificates for authentication
    d. SSLv3/TLSv1 port for operations other than Query, using client-side certificates for authentication
9. Supports Error Handling (see clause 11) for any supported object, attribute, or operation
10. Optionally supports any clause within this specification that is not listed above
11. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, conformance profiles) that do not contradict any requirements within this standard