From: Matt Ball, Sun Microsystems

To: OASIS KMIP TC

Date: 2009-06-25

Subject: Conformance Keywords Proposal

History

version 1 (2009-06-25): Initial Version

version 2 (2009-07-02): Changed 'MUST' to 'SHALL' and added forbidden words: 'must', 'can', and 'will'

Formatte

Formatte

Overview

This proposal proposes adding RFC 2119 as a normative reference and stating what the conformance keywords are.

The following text includes proposed changes (with changebars) against the June 25, 2009 version of the KMIP 0.98 specification.

1 Introduction

This document is intended as a specification of the protocol used for the communication between clients and servers to perform certain management operations on objects stored and maintained by a key management system. These objects will be referred to as *Managed Objects* in this specification. They include symmetric and asymmetric cryptographic keys, digital certificates, and templates used to simplify the creation of objects and control their use. Managed Objects are managed with *operations* that include the ability to generate cryptographic keys, register objects with the key management system, obtain objects from the system, destroy objects from the system, and search for objects maintained by the system. Managed Objects also have associated *attributes*, which are named values stored by the key management system and which can be obtained from the system via operations. Certain attributes may be changed, added or deleted, again by operations.

The protocol specified in this document includes several certificate-related functions for which there are a number of existing protocols – namely Validate (e.g. SVP or XKMS), Certify (e.g. CMP, CMC, SCEP) and Re-certify (e.g. CMP, CMC, SCEP). The protocol does not attempt to define a comprehensive certificate management protocol such as would be required for a certification authority. However, it does include functions that are needed in proxying certificate management functions through a key server.

In addition to the normative definitions for managed objects, operations and attributes, this specification also includes normative definitions for the following aspects of the protocol:

- Message contents and formats
- Authentication profiles for clients and servers
- Message encoding, including enumerations
- Error handling

This specification is complemented by two other documents. The Usage Guide provides illustrative information on using the protocol. The Test Specification provides samples of protocol messages corresponding to a set of defined test cases.

1.1 Document Roadmap

TBD

1.2 Goals and Requirements

TBD

1.3 Notational Conventions

TBD

1.4 Namespaces

TBD

1.5 Terminology

TBD

1.6 Normative References

~~TBD~~RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997.

1.7 Non-normative References

TBD

1.8 Compliance

~~TBD~~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.

Formatte
Numberin
Alignment
0.5" + In

Formatte
Numberin
Alignment
0.5" + In