60-day Public Review for KMIP Profiles Version 1.1 COS01

Submitted by censign on Thu, 2012-10-11 13:54
Type:
Public Review

Members of the OASIS Key Management Interoperability Protocol (KMIP) TC [1] have recently approved a Special Majority Ballot [2] to advance Key Management Interoperability Protocol Profiles Version 1.1 as a Candidate OASIS Standard (COS). The COS now enters a 60-day public review period in preparation for a member ballot to consider its approval as an OASIS Standard.

Key Management Interoperability Protocol Profiles Version 1.1
Candidate OASIS Standard 01
21 September 2012

Specification Overview:
The Key Management Interoperability Protocol (KMIP) establishes a single, comprehensive protocol for communication between enterprise key management servers and cryptographic clients. By defining a protocol that can be used by any cryptographic client, from the smallest automated electric meters to the most complex disk-arrays, KMIP enables key management servers to speak a single protocol to all cryptographic clients supporting the protocol. Through vendor support of KMIP, an enterprise will be able to consolidate key management in a single key management system, reducing operational and infrastructure costs while strengthening operational controls and governance of security policy.

KMIP includes three primary elements:
- Objects. These are the symmetric keys, asymmetric keys, digital certificates and so on upon which operations are performed.
- Operations. These are the actions taken with respect to the objects, such as getting an object from a key management system, modifying attributes of an object and so on.
- Attributes. These are the properties of the object, such as the kind of object it is, the unique identifier for the object, and so on.

At its most basic level, KMIP consists of placing objects, operations and/or attributes either into a request from a cryptographic client to a key management server or into a response from a key management server to a cryptographic client. The protocol also supports other elements, such as the use of templates that can simplify the specification of attributes in a request or response.

As a transport-level protocol, KMIP is complementary to other key management standards efforts, including OASIS EKMI and the W3C Web Cryptography API. Both those standards express application-level interfaces

for key management and, in the case of the W3C effort, cryptographic operations. KMIP on the other hand specifies a wire format on which these application-level interfaces could be layered.

KMIP also leverages other standards whenever possible. For example, it uses the key life-cycle specified in NIST Special Publication 800-57 to define attributes related to key states. It uses network security mechanisms such as TLS to establish authenticated communication between the key management system and the cryptographic client. It relies on existing standards such as PKCS #11, FIPS 180, FIPS 186 and X.509 for encryption algorithms, key derivation and many other aspects of a cryptographic solution, focusing on the unique and critical problem of interoperable messages between key management servers and cryptographic clients.

Public Review Period:

The 60-day public review starts 11 October 2012 and ends 10 December 2012.

This is an open invitation to comment. OASIS solicits feedback from potential users, developers and others, whether OASIS members or not, for the sake of improving the interoperability and quality of its technical work.

URIs:

The prose specification document and related files are available here:

Editable Source (Authoritative):
http://docs.oasis-open.org/kmip/profiles/v1.1/cos01/kmip-profiles-v1.1-c... [1]

HTML:
http://docs.oasis-open.org/kmip/profiles/v1.1/cos01/kmip-profiles-v1.1-c... [2]

PDF:
http://docs.oasis-open.org/kmip/profiles/v1.1/cos01/kmip-profiles-v1.1-c... [3]

Additional information about the specification and the OASIS Key Management Interoperability Protocol (KMIP) TC may be found at the TC's public home page:

http://www.oasis-open.org/committees/kmip/ [4]

Comments may be submitted to the TC by any person through the use of the OASIS TC Comment Facility which can be located via the button labeled "Send A Comment" at the top of the TC public home page, or directly at:

https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=kmip [5]

Comments submitted by TC non-members for this work and for other work of this TC are publicly archived and can be viewed at:

http://lists.oasis-open.org/archives/kmip/ [6]

All comments submitted to OASIS are subject to the OASIS Feedback License, which ensures that the feedback you provide carries the same obligations at least as the obligations of the TC members. In connection with this public review of Key Management Interoperability Protocol Profiles Version 1.1, we call your attention to the OASIS IPR Policy [3] applicable especially [4] to the work of this technical committee. All members of the TC should be familiar with this document, which may create obligations regarding the disclosure and availability of

a member's patent, copyright, trademark and license rights that read on an approved OASIS specification.

OASIS invites any persons who know of any such claims to disclose these if they may be essential to the implementation of the above specification, so that notice of them may be posted to the notice page for this TC's work.

==========
[1] OASIS Key Management Interoperability Protocol (KMIP) TC
http://www.oasis-open.org/committees/kmip/ [4]

[2] Candidate OASIS Standard ballot
https://www.oasis-open.org/committees/ballot.php?id=2285 [7]

[3] http://www.oasis-open.org/who/intellectualproperty.php [8]

[4] http://www.oasis-open.org/committees/kmip/ipr.php [9]
RF on RAND mode
https://www.oasis-open.org/policies-guidelines/ipr#s10.2.2 [10]

Associated TC:
Key Management Interoperability Protocol (KMIP)
Deadline:
Thu, 2012-10-11 - Mon, 2012-12-10

Links:
[1] http://docs.oasis-open.org/kmip/profiles/v1.1/cos01/kmip-profiles-v1.1-cos01.doc
[2] http://docs.oasis-open.org/kmip/profiles/v1.1/cos01/kmip-profiles-v1.1-cos01.html
[3] http://docs.oasis-open.org/kmip/profiles/v1.1/cos01/kmip-profiles-v1.1-cos01.pdf
[4] http://www.oasis-open.org/committees/kmip/
[5] https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=kmip
[6] http://lists.oasis-open.org/archives/kmip/
[7] https://www.oasis-open.org/committees/ballot.php?id=2285
[8] http://www.oasis-open.org/who/intellectualproperty.php
[9] http://www.oasis-open.org/committees/kmip/ipr.php
[10] https://www.oasis-open.org/policies-guidelines/ipr#s10.2.2