To: IEEE P1619.3 Task group of the Security In Storage Working Group

From: Matt Ball, Sun Microsystems, Inc.

Date: July 9, 2009~~July 8, 2009~~

Purpose: Proposed changes against P1619.3/D6 to use OASIS KMIP as the basis for the P1619.3 binary encoding

Introduction

This proposal suggests the following changes to P1619.3/D6:

- Incorporate the OASIS copyright statement and indicate that this is a derivative work of OASIS KMIP. This will be in addition to the IEEE copyright statement.
- Propose adopting the OASIS KMIP binary encoding, by reference. This would allow for P1619.3-specific extensions
- Remove sections that contradict the OASIS KMIP object and operations model.

OASIS Copyright Notice

I'm currently working with both OASIS and IEEE to get a letter-of-understanding for ways that P1619.3 may create derivative works from OASIS KMIP. This agreement will likely require that this draft include the following statement in the front matter somewhere:

> Note: In the following copyright and section from the OASIS KMIP Editor's Draft 0.98 [KMIP], references to "this document" refer to KMIP itself. In this context, IEEE P1619.3 is a derivative work of KMIP.
>
> Portions Copyright © OASIS Open 2009. All Rights Reserved.
>
> This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

Additions, Changes or Deletions to Draft 6

1. Overview

{leave unchanged}

2. Normative references

{Add following reference}

OASIS Key Management Interoperability Protocol (KMIP), Editor's Draft 0.98, May 2009. Available at http://www.oasis-open.org/committees/download.php/32620/kmip-1.0-spec-ed-0.98-nochangetracking.pdf.

3. Definitions, acronyms and abbreviations

{leave unchanged – although we'll need to scrub this later}

4. General concepts and models

4.1 Overview

4.2 Key management architecture model

4.3 Key management conceptual model

4.4 Key lifecycle model

Add: [Editor's Note: We will need to revisit this model and bring it more in line with NIST SP 800-67 and OASIS KMIP. This could be accomplished by removing the entire section and stating something like "See SP 800-57 (or KMIP) for a description of the key lifecycle model, or we could propose a way to layer on the extra states on top of the SP 800-57 model]

4.5 Key management sequence models

{Remove this section – it has no content. If we add this content, it should be in an informative annex}

4.6 Key Management Operations Model

{remove this subclause}

4.7 Key Management Object Model

{remove this subclause}

5. Key management namespace

{Leave unchanged}

Add: {Editor's Note: May need to change terminology to match nomenclature used by KMIP}

Comment [wah1]: May need to change terminology to match nomenclature used by KMIP.

6. Key management objects

{Remove this entire clause and replace with the following text:}

{Editor's Note: Need to review the following objects and determine which are needed by P1619.3}

6.1 Base objects

The following base objects defined in OASIS KMIP are supported by P1619.3.

Comment [wah2]: Should match the KMIP object and attributes. A review of these is needed to determine which ones need to be here, although probably have everything here (not all need to be required; some can be optional based on the profile).

- Attribute
- Credential
- Key Block
- Key Value
- Key Wrapping Data
- Key Wrapping Specification
- Transparent Key Structures
- Template-Attribute Structures

6.2 Managed objects

The following managed objects defined in OASIS KMIP are supported by P1619.3.

- Certificate
- Symmetric Key
- Public Key
- Private Key
- Split Key
- Template
- Secret Data

— Opaque Object

6.3 Object extensions

This subclause defines P1619.3-specific extensions to the KMIP object model.

[Content TBD]

7. Key management policies

{~~Remove this clause and renumber subsequent clauses~~Keep this clause intact}

Add: {Editor's Note: Need to revisit these policies and bring them in line with KMIP}

Comment [wah3]: There is disagreement. We still need policies; there are policies in KMIP but they're not called that.

Formatted: Font color: Auto

8. Key management operations

{Delete entire clause and replace with the following text:}

8.1 Base client to server operations

The following operations defined in OASIS KMIP are ~~supported~~ included by P1619.3

Comment [wah4]: Maybe "included" rather than supported, can be mandatory or optional.

— Create
— Create Key Pair
— Register
— Re-key
— Derive Key
— Certify
— Re-certify
— Locate
— Check
— Get
— Get Attributes
— Get Attribute List
— Add Attribute
— Modify Attribute
— Delete Attribute
— Obtain Lease
— Get Usage Allocation

— Activate
— Revoke
— Destroy
— Validate
— Query
— Cancel
— Poll

8.2 Base server to client operations

— The following operations are defined by KMIP and are optionally supported.

— Notify
— Put

~~8.2~~8.3 Operation extensions

This subclause defines P1619.3-specific extensions to the operations defined by OASIS KMIP.

9. Message encoding

{Delete entire clause and replace with this text:}

9.1 Binary encoding

The KM Server shall support the binary encoding as defined by KMIP. The KM Client may support the binary encoding as defined by KMIP.

9.2 XML SOAP encoding

This subclause defines an XML encoding that is based on the KMIP binary encoding.

The KM Server shall support the XML encoding defined in this subclause. The KM Client may support the XML encoding defined in this subclause.

[Editor's Note: Need to define an XML WSDL that is a mechanical translation of the KMIP binary encoding]

10. Key Management Transport

{ ~~Remove this clause~~keep this clause}

Formatted: Indent: Left: 0.14", Hanging: 0.31"

Formatted: IEEEStds Level 2 Header, Indent: Left: 0", First line: 0"

Comment [wah5]: Separate out client to server and server to client. The latter are all completely optional.

Comment [wah6]: Gets real ugly. See above note.

Comment [wah7]: We need to define specific transports. KMIP specifies only that the transport is secure. Define TLS and a default port, with other ports optional. Auto-negotiation and discovery may also require additional Ports.

Add: {Editor's Note: We need to define TLS and a default port for P1619.3}

Formatted: Font color: Auto

Annex A

(normative)

Minimum requirements to meet P1619.3

{Leave unchanged}

Annex B

(informative)

Bibliography

{Leave unchanged}

Annex C

(informative)

Example use cases

{Leave unchanged}

Annex D

(informative)

XML schema definitions

{Remove this annex and add the following note}

[Editor's Note: ~~Need to~~Optionally add XML WSDL based on KMIP binary encoding]

Comment [wah8]: Do we? Lots of work to do this.

Annex E

(informative)

Comparison of P1619.3 key lifecycle model with other standards

{Leave unchanged}

Annex F

(informative)

Discussion of SO_GUID formats

{Leave unchanged, although we'll need to revisit this later}