Proposal for changes to KMIP Profiles related to conformance (29-Oct-2011)

KMIP conformance requirements are currently spread across both the KMIP Specification and the KMIP Profiles document. This is required to some degree, in that the conformance statement needs to be included in the Specification. However, the KMIP Specification includes more than is required for a conformance statement, including definition of profiles that more properly belongs in the KMIP Profiles document. Moreover, the KMIP Profiles V1.0 did not allow for client profiles and for authentication other than SSL/TLS.

This proposal suggests six changes (in **bold**) to the current draft of KMIP Profiles V1.1 (kmip-profiles-1.1-draft-02.doc), intended to simplify the conformance-related language in the KMIP Specification and to consolidate profiles in the KMIP Profiles document. A separate but related proposal ("KMIP Specification conformance proposal 3Oct11.pdf") defines the corresponding changes to the KMIP Specification V1.1 document.

1. **Require client authentication for Discover Versions**

Section 2.2, to read as follows:

2.2 Guidelines for Specifying Authentication Suites

1. Channel Security ~~–~~ For all operations, communication between Client and~~to~~ Server ~~communication~~ SHALL establish and maintain channel confidentiality and integrity.

2. Channel Options – Options like protocol version and cipher suite.

3. Server and Client Authenticity – For all operations, communication between Client and~~to~~ Server ~~communication~~ SHALL provide assurance of server authenticity and client authenticity.

Section 3, first paragraph to read as follows):

This section contains the list of protocol versions and cipher suites that MAY be used by KMIP profiles.

Change Section 3.1 to read as follows (first paragraph only):

This authentication set stipulates that a KMIP client and server SHALL use TLS to negotiate a mutually-authenticated connection.

Change Section 3.1.3 (lines 118-120) to read as follows:

3.1.3 Client Authenticity

For authenticated services KMIP servers SHALL require the use of channel (TLS) mutual authentication to provide assurance of client authenticity.

Change Section 3.2 (lines 134-137 inclusive) to read as follows:

3.2 TLS 1.2 Authentication Suite

This authentication set stipulates that a KMIP client and server SHALL use TLS to negotiate a mutually-authenticated connection.

2. **Add new Discover Versions server and client profiles.**

4.1 Basic Discover Versions Server Profile

A profile that consists of the tuple {Discover Versions Server Conformance Clause, Basic Authentication Suite}

4.12 Discover Versions Server TLS 1.2 Authentication Profile

A profile that consists of the the tuple {Discover Versions Server Conformance Clause, TLS 1.2 Authentication Suite}

4.22 Basic Discover Versions Client Profile

A profile that consists of the tuple {Discover Versions Server Conformance Clause, Basic Authentication Suite}

4.32 Discover Versions Client TLS 1.2 Authentication Profile

A profile that consists of the tuple {Discover Versions Server Conformance Clause, TLS 1.2 Authentication Suite}

3. **Add new Discover Versions server and client conformance clauses.**

5.1 Discover Versions Server Clause

This proposal builds on the KMIP server conformance clauses to provide the most basic functionality that would be expected of a conformant KMIP server – the ability to provide the server version.

5.1.1. Implementation Conformance

An implementation is a conforming Discover Versions Server Clause if it meets the conditions as outlined in the following section.

5.1.2 Conformance of a Discover Versions Server

An implementation conforms to this specification as a ~~Secret Data~~Discover Versions Server if it meets the following conditions:

1. Supports the Discover Versions client-to-server operation (**[KMIP-Spec] 4.26**)

5.12 Discover Versions Client Clause

This proposal builds on the KMIP server conformance clauses to provide the most basic functionality that would be expected of a conformant KMIP client – the ability to request the server version.

5.12.1 Implementation Conformance

An implementation is a conforming Discover Versions Client Clause if it meets the conditions as outlined in the following section.

5.12.2 Conformance of a Discover Versions Client

An implementation conforms to this specification as a ~~Secret Data~~Discover Versions Client if it meets the following conditions:

1. Supports the Discover Versions client-to-server operation (**[KMIP-Spec] 4.26**)

4. Incorporate KMIP Server Baseline Profile from KMIP Specification Section 12 into Profiles document as new subsection in Sections 4 (Base Server Profile), 5 (conformance clauses) and 6 (test scenarios), changing all current references to this profile from KMIP Specification Section 12 to the new section in the KMIP Profiles document.

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

Supports the following objects:
66 a. Attribute (see 2.1.1)
67 b. Credential (see 2.1.2)
68 c. Key Block (see 2.1.3)
69 d. Key Value (see 2.1.4)
70 e. Template-Attribute Structure (see 2.1.8)
71 2. Supports the following attributes:
72 a. Unique Identifier (see 3.1)
73 b. Name (see 3.2)
74 c. Object Type (see 3.3)
75 d. Cryptographic Algorithm (see 3.4)
76 e. Cryptographic Length (see 3.5)
77 f. Cryptographic Parameters (see 3.6)
78 g. Digest (see 3.12)
79 h. Default Operation Policy (see 3.13.2)
80 i. Cryptographic Usage Mask (see 3.14)
81 j. State (see 3.17)
82 k. Initial Date (see 3.18)
83 l. Activation Date (see 3.19)
84 m. Deactivation Date (see 3.22)

85 n. Compromise Occurrence Date (see 3.24)
86 o. Compromise Date (see 3.25)
87 p. Revocation Reason (see 3.26)
88 q. Last Change Date (see 3.33)
89 3. Supports the ID Placeholder (see 4)
90 4. Supports the following client-to-server operations:
91 a. Locate (see 4.9)
92 b. Check (see 4.10)
139
93 c. Get (see 4.11)
94 d. Get Attribute (see 4.12)
95 e. Get Attribute List (see 4.13)
96 f. Add Attribute (see 4.14)
97 g. Modify Attribute (see 4.15)
98 h. Delete Attribute (see 4.16)
99 i. Activate (see 4.19)
100 j. Revoke (see 4.20)
101 k. Destroy (see 4.21)
102 l. Query (see 4.25)
103 m. Discover Versions (see 4.26)
104 5. Supports the following message contents:
105 a. Protocol Version (see 6.1)
106 b. Operation (see 6.2)
107 c. Maximum Response Size (see 6.3)
108 d. Unique Batch Item ID (see 6.4)
109 e. Time Stamp (see 6.5)
110 f. Asynchronous Indicator (see 6.7)
111 g. Result Status (see 6.9)
112 h. Result Reason (see 6.10)
113 i. Batch Order Option (see 6.12)
114 j. Batch Error Continuation Option (see 6.13)
115 k. Batch Count (see 6.14)
116 l. Batch Item (see 6.15)
117 6. Supports Message Format (see 7)
118 7. Supports Authentication (see 8)
119 8. Supports the TTLV encoding (see 9.1)
120 9. Supports the transport requirements (see 10)
121 10. Supports Error Handling (see 11) for any supported object, attribute, or operation
122 11. Optionally supports any clause within this specification that is not listed above
123 12. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
124 conformance profiles) that do not contradict any requirements within this standard
125 13. Supports at least one of the profiles defined in the KMIP Profiles Specification **[KMIP-Prof**

5. Add KMIP port number assigned by IANA.

For the KMIP port number information in the Profiles document, create a new subsection in each of the two authentication suite descriptions, such as the following:

3.1.5 KMIP Port Number

KMIP servers using the Basic Authentication Suite ~~SHALL~~ SHOULD use TCP port number 5696, as assigned by IANA, to receive and send KMIP messages. KMIP clients using the Basic Authentication Suite MAY use the same 5696 TCP port number.

3.2.5 KMIP Port Number

Same as the basic authentication suite (See Section 3.1.5)

6. **Add client conformance clause and profiles, include Storage Client conformance clause and profile**

Conformance clauses and profiles for clients, comparable to those for servers, have been added in the most recent draft of the KMIP Profiles document. In addition, a profile for a storage client, referencing and consisting of other client profiles, has also been included in the current draft.