KMIP Server and Client Port Applications

Prepared by: Alan Frindell, SafeNet, Inc.
Version: 1.0
Date: 12/9/2009

Purpose: The KMIP specification describes two services that would benefit from well known ports assigned by IANA. The IANA website has an online application form with several questions regarding the proposed use of the port (http://www.iana.org/cgi-bin/usr-port-number.pl). This document contains the answers to the questions for the KMIP Server and the KMIP Client Service.

Contributors: Steve Wierenga, HP; Matt Ball, Sun

KMIP Server Port Application

Your Name:

OASIS KMIP Technical Committee

1. What is the protocol-number between the user machine and the server machine?

TCP

2. What message formats are used?

The sequence of fields is Tag, Type, Length and Value (TTLV). The type field can specify a structure, which itself contains zero or more elements of the same TTLV format.

3. What message types are used?

KMIP has both request and response message types.

4. What message op codes are used?

There are 26 operations defined for the KMIP server in the KMIP 1.0 draft specification (http://docs.oasis-open.org/kmip/spec/v1.0/cd06/kmip-spec-1.0-cd-06.doc):

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
Archive

Recover
Validate
Query
Cancel
Poll

5. What message sequences are used?

Both synchronous and asynchronous messages are allowed for KMIP servers in the KMIP 1.0 draft. For synchronous messages, the client sends a request and the server sends a corresponding response. To use asynchronous messages, the client sets an indicator in the request. If the server supports asynchronous messaging, it will immediately return a response including an Asynchronous Correlation Value. The client may then pass this value to the Poll and Cancel operations to manipulate the request.

Batching of certain requests is also supported. It is designed to reduce the number of round trips between the client and server required for common functions. For example, a very common sequence is to query for an object using the ‘Locate’ operation an object and then retrieve it using the ‘Get’ operation. An ID Placeholder value is used by the client in the request sequence to refer to the ID of objects resulting from the previous operation.

For more detail, please refer to the KMIP 1.0 draft specification.

6. What functions are performed by this protocol?

KMIP is 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 include symmetric and asymmetric cryptographic keys, digital certificates, and templates used to simplify the creation of objects and control their use.

7. Is either broadcast or multicast used?

No

If yes, how and what for?

8. Please give us a technical description of your proposed use of the user port number. (At least 2 paragraphs)

KMIP servers will listen on the port by default for connection requests from KMIP clients. Clients will then send requests to locate, create, import, retrieve and otherwise manage key material on the KMIP server. Communications over this channel for all opcodes except one (Query) must be authenticated and encrypted using TLS. The messages for the protocol are defined in the KMIP 1.0 Specification.

The protocol is designed to foster interoperability among vendors of encryption endpoints such as tape and storage devices and key managers.

9. What is the proposed name of the user port number? (For example: Super User Message Service)

KMIP Server

10. What SHORT name (14 CHARACTER MAXIMUM) do you want associated with this port number? (For example: sums)

kmip_server

KMIP Client Service Port Application

Your Name:

OASIS KMIP Technical Committee

1. What is the protocol-number between the user machine and the server machine?

TCP

2. What message formats are used?

The sequence of fields is Tag, Type, Length and Value (TTLV). The type field can specify a structure, which itself contains zero or more elements of the same TTLV format.

3. What message types are used?

KMIP has both request and response message types.

4. What message op codes are used?

There are two operations defined for the KMIP client service in the KMIP 1.0 draft specification (http://docs.oasis-open.org/kmip/spec/v1.0/cd06/kmip-spec-1.0-cd-06.doc):

Notify
Put

5. What message sequences are used?

Only synchronous messaging is supported for the KMIP client service in the KMIP 1.0 draft. The Key Management server will send a request to a Key Management client that is listening on the KMIP client port. The client shall send a response message containing no payload, unless both the client and server have prior knowledge (obtained via out-of-band mechanisms) that the client cannot respond. Batching and asynchronous messaging are not supported by the KMIP client service.

For more detail, please refer to the KMIP 1.0 draft specification.

6. What functions are performed by this protocol?

KMIP is 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 include symmetric and asymmetric cryptographic keys, digital certificates, and templates used to simplify the creation of objects and control their use. The client service is used to notify clients of events and distribute cryptographic objects to clients using a ‘push’ model.

7. Is either broadcast or multicast used?

No

If yes, how and what for?

N/A

8. Please give us a technical description of your proposed use of the user port number. (At least 2 paragraphs)

KMIP clients that are capable of receiving unsolicited server-to-client messages will listen on the port by default for connection requests from KMIP servers. The server will send notification of changes to cryptographic objects that may be of interest to the client, or push the actual cryptographic objects themselves. All communications over this channel will be authenticated and encrypted using TLS. The messages for the protocol are defined in the KMIP 1.0 Specification.

The protocol is designed to foster interoperability among vendors of encryption endpoints such as tape and storage devices and key managers.

9. What is the proposed name of the user port number? (For example: Super User Message Service)

KMIP Client Service

10. What SHORT name (14 CHARACTER MAXIMUM) do you want associated with this port number? (For example: sums)

kmip_client