Usage Guide Proposal for KMIP HTTPS Encoding

Created by: Alan Frindell, SafeNet, Inc.
Version: 1.1
Date: 7/21/09
Purpose: The encoding of KMIP over HTTPS is not specified in the original draft.
Contributors: Mathias Bjoerkqvist

The following shows changes from the Usage Guide kmip-1.0-ug-ed-0.98-v1.doc dated 29 April 2009, section 3.2 only.

Revision History:

Version 1.0, 7/15/2009:	Initial draft
Version 1.1, 7/21/2009:	Changed recommended URI from /kmip to /

3.2 HTTPS Profile

Hypertext Transfer Protocol over Secure Socket Layer or https is a URI (Universal Resource Indicator) scheme used to indicate a secure HTTP connection, requiring an additional encryption and authentication layer, implemented by SSL/TLS, between HTTP and TCP. The establishment of the trust relationship between the client and server is the same as in the SSL/TLS profile described above.

As in the SSL/TLS profile, mutual authentication must be performed. The client certificate used in the SSL session may be included in any client-initiated KMIP messages between the client and server as the value of the Credentials object in the message, with credential type of certificate. Similarly, the server certificate used in the SSL session may be included in any server-initiated KMIP messages between the client and server as the value of the Credentials object in the message, with credential type of certificate.

3.2.1 HTTP Encoding

A client using the HTTPS profile must:

- Use the POST request method
- Specify Content-Type: application/octet-stream
- Send one TTLV KMIP message in binary form in the body of each HTTP request
- Comply with the HTTP version claimed in the request line

A client using the HTTPS profile must not:

- Use the HTTP Authorization header to transmit any authentication data

A server using the HTTPS profile must:

- Return HTTP response code 200 Success if a KMIP response was returned, including KMIP error responses
- Specify Content-Type: application/octet-stream
- Send one TTLV KMIP message in binary form in the body of each HTTP response with response code 200
- Comply with the HTTP version claimed in the status line
- Send the Cache-Control: no-cache directive to prevent clients from caching KMIP responses (HTTP/1.1 only)

Servers supporting the optional server-to-client Put and Notify messages shall behave as an HTTP client. Clients responding to these messages shall behave as an HTTP server.

A client may use the Accept-Encoding header to indicate it accepts compressed or otherwise transformed responses. Clients may also use HTTP/1.0 Keep Alive or HTTP/1.1 Connection headers to control persistent connection behavior.

The Content-Length header may be used by clients and servers to support persistent connections where allowed by HTTP. This header is not required.

The Request-URI is not specified and may be used by clients and servers in an implementation specific fashion. The value / is recommended.

KMIP servers supporting the HTTPS profile should listen on port TBD1. KMIP clients responding to optional server-to-client Put and Notify messages should listen on port TBD2.

Comment [AHF1]: KMIP over HTTPS will have different default port recommendations than standard HTTPS.

Deleted: a different default TCP port (443) and

Deleted: t

Deleted: ust

Deleted: ust

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bulleted + Level: 1 + Aligned at: 1.25" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Bulleted + Level: 1 + Aligned at: 1.25" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Bullets and Numbering

Formatted: Indent: Left: 1"

Formatted: Indent: Left: 1"

Comment [AHF2]: Version 1.1: Changed recommended URI from /kmip to /