KMIP v1.3 Plugfest Results

Testing summary

The KMIP v1.3 Plugfest was completed over one week in October 2014 and involved participation from 4 organisations:
-Cryptsoft
-IBM
-P6R
-Semper Fortis Solutions

All identified tests were run successfully and the findings are noted below.

Testing scope

Locate with Offset

Confirm support for using OffsetItems (combined with MaximumItems) to specify a range of items to return.

Client Registration

Support returning client registration information using a one-time-password for the initial credentials

One Time Pad

Support use of a one-time-pad where the one-time-pad value is never made available to the client. The codebook used and the specific algorithm is not relevant to the testing although for this example test case a simple XOR

Client to Server Query

Client querying the Server capabilities.

Server to Client Query

Server querying the Client capabilities.

Streaming Cryptographic Operations

Testing multi-part operations. Currently only testing the mechanisms with a simple Hash.

RNG Attribute

Server accepts details from client as to which RNG was used or records its own details as to the RNG used for generation.

Results

Inclusion of “Client” or “Server” in the table below indicates the test has been completed successfully by a client or server implementation against at least one other participating client or server implementation.

Test Case	Organization			
Identifier	Cryptsoft	IBM	P6R	Semper Fortis Solutions
Client Registration				
tc-creg-2-13	Client : Server	:	Client :	Client : Server
Locate With Offset				
tc-offset-1-13	Client : Server	Client : Server	Client :	Client : Server
One Time Pad				
tc-otp-1-13	Client : Server	:	Client :	Client : Server
tc-otp-2-13	Client : Server	:	Client :	Client : Server
tc-otp-3-13	Client : Server	:	Client :	Client : Server
tc-otp-4-13	Client :	:	Client :	Client :
tc-otp-5-13	Client : Server	:	Client :	Client : Server
Client to Server Query				
tc-q-cap-1-13	Client :	Client : Server	Client :	Client :
tc-q-cap-2-13	Client : Server	:	Client :	Client : Server
tc-q-creg-1-13	Client : Server	:	Client :	Client : Server
tc-q-prof-1-13	Client :	Client : Server	Client :	Client :
tc-q-prof-2-13	Client : Server	:	Client :	Client : Server
tc-q-prof-3-13	Client : Server	:	Client :	Client : Server
tc-q-rngs-1-13	Client :	Client : Server	Client :	Client :
tc-q-rngs-2-13	Client :	:	Client :	Client :
tc-q-rngs-3-13	Client : Server	:	:	Client : Server
tc-q-rngs-4-13	Client :	:	:	Client :
tc-q-rngs-5-13	Client :	:	:	Client :
tc-q-val-1-13	Client : Server	:	Client :	Client : Server
tc-q-val-2-13	Client :	Client : Server	Client :	Client :
Server to Client Query				
tc-q-s2c-1-13	Client : Server	:	:	: Server
tc-q-s2c-2-13	: Server	:	Client :	: Server
tc-q-s2c-prof-1-13	Client : Server	:	:	: Server
tc-q-s2c-prof-2-13	: Server	:	Client :	: Server
Streaming Cryptographic Operations				
tc-stream-hash-1-13	Client : Server	Client : Server	Client :	Client : Server
tc-stream-hash-2-13	Client : Server	Client : Server	:	Client : Server
tc-stream-hash-3-13	Client : Server	Client : Server	Client :	Client : Server
RNG Attribute				
tc-rng-attr-1-13	Client : Server	:	Client :	Client : Server
tc-rng-attr-2-13	Client : Server	:	Client :	Client : Server