

SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-178r0)

Date: March 23, 2006

Time: 10:00 am - 12:00 pm

Location: Phone Conference

Attendance

SSC-3 Working Group Attendance Report - March 2006

Name	S	Organization
Mr. Paul Entzel	P	Quantum Corp.
Mr. Dwayne Edling	A#	Sun Microsystems
Chris Williams		
Mr. Greg Wheelless	A	Symantec
Mr. David Peterson	P	McDATA
Mr. Matt Ball		Quantum
Mr. Kevin Butt	A	IBM Corp.

Results of Meeting

1. Old business

1.1 The Requirement for More than One Decryption Key (06-051r6 [Edling]

Reviewed the changes from last meeting and that they were brought in correctly.

Paul Entzel moved that we accept 06-172r0 as modified and 06-051r6 as modified into SSC-3. Greg Wheelless seconded. Passed unanimously.

1.2 SSC-3: Add commands to control data encryption (06-172r0) [Entzel]

4.2.19.5 lettered list item d needed to be updated that was missed from last call.

second list on page 9, HP wants statement added to explicitly state that key is established.

Change SP_SPECIFIC to SECURITY SPECIFIC PROTOCOL

Cleaning up CKORSC to CKORSP

Second paragraph of page 21:

An authenticated key-associated data descriptor (see 8.5.4.4) shall be included if an authenticated key-associated data descriptor was included when the key was established in the device server. The AUTHENTICATED field shall be set to zero. The KEY DESCRIPTOR field shall contain the A-KAD value associated with the key.

There is an issue with AUTHENTICATED field being set to zero.

Make value in Table D3 reserved and shift other values. In the text state AUTHENTICATED field is reserved. Sweep document for changes related to this.

HP asked the question if two keys were required if you support both LOCAL and ALL I_T NEXUS. Decided to add a sentence clarifying that there may only be enough resources to store one set of parameters and it may be shared by all scopes.

Paul Entzel wanted point out and make sure everybody saw that Table E2 added Key Size field because ietf uses the same algorithm identifier for both AESGCM 128 and AESGCM 256.

Paul Entzel moved that we accept 06-172r0 as modified and 06-051r6 as modified into SSC-3. Greg Wheelless seconded. Passed unanimously.

1.3 SPC-4: Add security protocol and additional sense for tape encryption (06-108r1) **[Entzel]**

There was discussion about referenceing IEEE P1619.1. There was expressions of nervousness, but there was no other way that this could be documented.

2. Next Meeting Requirements (San Jose, CA)

Discussion about David Blacks proposal being the next encryption related item to discuss.

3. Adjournment

Call ended at 11:05 MST