

**T10/06-162r0: Minutes of  
SCSI Stream Commands (SSC-3) Working Group  
Conference Call of March 16, 2006  
11:00 AM – 1:00 PM CST**

**1. Introductions**

**Group**

David Peterson called the meeting to order at 11:00 AM CST. Greg Wheelless agreed to serve as the secretary for the conference call.

**2. Attendance**

**David Peterson**

SSC-3 Working Group conference call attendance:

Name	S	Organization
-----	---	-----
Mr. Gideon Avida	AV	Decru
Mr. Ralph O. Weber	P	ENDL Texas
Mr. David Black	A	EMC Corp.
Mr. Rob Elliott	P	Hewlett Packard Co.
Mr. Chris Williams	V	Hewlett Packard
Mr. Kevin Butt	A	IBM Corp.
Mr. David Peterson	P	McDATA
Mr. Paul Entzel	P	Quantum Corp.
Mr. Matt Ball	V	Quantum Corp.
Mr. Dwayne Edling	A#	Sun Microsystems
Mr. Greg Wheelless	A	Symantec

**3. Discussion Items**

**Group**

**3.1 Add commands to control data encryption (05-446r7).**

Paul Entzel

Ralph Weber noted that the value of the data encryption security protocol identifier number should be made explicit in the SECURITY PROTOCOL IN and OUT commands, and that the OUT command needs to reference SPC-4.

Greg Wheelless noted that the format of the supported page list entries should be made explicit in the “supported tape data encryption in/out pages” pages.

The group discussed the format of the supported key formats – Ralph Weber noted that the fact that this is a single-byte field should be made explicit.

Kevin Butt noted that some implementations might require that a tape be at BOP in order to enable encryption for the tape, and requested a bit for that purpose in Table M1. Paul Entzel noted that there was no mechanism for the functionality described, and that we should see a proposal for that before adding a bit.

The suggestion to remove table S4 and S5 was discussed, replacing them with references to 4.2.19.6 and 4.2.19.7 instead; there was no objection.

Table S3 was discussed, especially the usage of the term “metadata”. Paul Entzel suggested removing both S2 and S3 and replacing them with references to tables Y3 and Y4. Ralph

Weber noted that we still have to fix the wording for “RAW” and proposed wording that didn’t contain “metadata”. It was noted that the data returned by a RAW read will be very vendor specific, and therefore of limited use (such as a media copy without knowing the key).

David Black asked the status of the algorithm registry. Paul Entzel noted that strings identifying an algorithm have been replaced in the proposal with a 4-byte field to eliminate ambiguity. The 4-byte coded values for that field will be defined in SPC. How to assign values was discussed; the consensus was that these values should be chosen to match IETF values where appropriate, but that’s a note and not a normative requirement,

It was noted that the approach taken for specifying the key-associated data descriptors list in table S1 would prohibit reporting of U-KAD and A-KAD descriptors that were established by a mechanism outside the scope of this standard. Paul Entzel noted that this was the intent.

The group discussed whether table N2 should reference the next logical block, or the next logical object. The next logical object might be a file mark. The consensus was that the phrase “next logical block” is inappropriate and should be replaced with a reference to the logical object number field. Greg Wheelless suggested that a value be assigned for the case where the next logical object is not a block to make that case explicit. Paul Entzel noted that he would change table N3 similarly.

It was noted for both table N2 and N3 that we need to clarify that it’s device server encryption and compression that we’re describing, as application client encryption and compression would be unknown to the device server.

Chris Williams noted that some algorithms need a separate encryption and decryption key, and questioned whether table Y1 could accommodate this. The consensus was that the space available was adequate, and other details could be addressed in a future proposal.

The phrase “participants in a reservation” in table Y2 was discussed. Paul Entzel noted that “reservation holders” was not a good replacement because of the case of an “all registrants” reservation. Paul Entzel proposed removing RESERVATION GROUP as a scope value entirely from the proposal, as the ALL I\_T NEXUS scope plus the CKORL bit should solve the related problems.

The group discussed the wording of the definitions of the CKOD and CKORL bits. Ralph Weber proposed adding a glossary entry for “reservation loss”. The situation where a reservation was pre-empted was discussed, and the consensus was that a Clear Key On Reservation Scope Change bit would provide the appropriate flexibility.

The group discussed editorial changes to table Y5. David Black discussed the need for a value in Y5 to be used for wrapped keys. Ralph Weber suggested that a proposal for developing a shared secret between an application client and a device server might belong in SPC-4, not SSC-3. David Black agreed to bring suggested changes in a future proposal against SSC-3, not as changes to 05-446.

Paul Entzel to produce a draft with all changes except the removal of RESERVATION GROUP scope, and an additional draft with RESERVATION GROUP scope removed.

#### **4. Next Meeting Requirements**

**David Peterson**

There will be a conference call from 11:00 AM to 1:00 PM CST, March 23, 2006, to continue discussion on 05-446.