SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-429r0)
Date: Sept 12, 2006
Time: 10:00 am - 5:00 pm
Location: Nashua, NH

# Agenda

**1. Opening remarks and introductions [Peterson]**

**2. Approval of agenda (06-426r0) [Peterson]**

**2.1 Old business**

**2.1.1 Physical device model (05-049r3) [Suhler]**

**2.1.2 SCSI Domain Model with Physical Device (06-333r0) [Butt]**

**2.1.3 ADC: Device Structure Model (06-334r0) [Butt]**

**2.1.4 Vendor Feedback (05-351r1) [Group]**

**2.1.5 Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0) [Banther]**

**2.1.6 Configurable EW (05-423r0) [Butt]**

**2.1.7 Using NIST AES Key-Wrap for Key Establishment (06-225r3) [Ball]**

**2.1.8 Add Encrypted Write Command proposal (06-207r2) [Avida]**

**2.1.9 Encrypt keys for transfer to device (06-103r2) [Black]**

**2.1.10 Position after Self-Test (05-140r1) [Banther]**

**2.1.11 TapeAlert Delineation (06-138r0) [Butt]**

**2.1.12 Discussion of key integrity validation [Butt]**

**2.1.13 Authentication Concerns for Encrypted Key Transfer (06-329r0) [Wheeless]**

**2.2 New Business**

**2.2.1 Keyless Copying of Encrypted Media and Other Topics (06-412r0) [Suhler]**

**2.2.2 Modifications to Tape Data Encryption (06-385r0) [Entzel]**

**2.2.3 Using Public-Key Cryptograhy for Key Wrapping (06-389r0) [Avida]**

**2.2.4 Remove IV fields from the Data Encryption Algorithm descriptor (06-391r0) [Entzel]**

**3. Approval of meeting minutes (06-338r0) [Peterson]**

**4. Review of old action items [Butt]**

**5. Next meeting requirements (Las Vegas, NV)**

**6. Review of new action items**

**7. Adjournment**

## Attendance

SSC-3 Working Group Attendance Report - September 2006

| Name | S | Organization |
|---|---|---|
| Mr. Noud Snelder | V | BDT |
| Mr. Gideon Avida | P | Decru |
| Mr. David Black | A | EMC Corp. |
| Mr. Robert H. Nixon | P | Emulex |
| Mr. Ralph O. Weber | P | ENDL Texas |
| Mr. Walt Hubis | V | Engenio Information Tech. |
| Mr. Curtis Ballard | V | Hewlett Packard |
| Mr. Michael Banther | V | Hewlett Packard Co. |
| Mr. Christopher Williams | V | Hewlett Packard Co. |
| Mr. Kevin Butt | A | IBM Corp. |
| Mr. David Peterson | P | McDATA |
| Mr. Larry Hofer | V | McDATA Corp |
| Mr. Frederick Knight | A | Network Appliance |
| Mr. Paul Entzel | P | Quantum Corp. |
| Dr. Paul Suhler | A | Quantum Corp. |
| Mr. Gerald Houlder | P | Seagate Technology |
| Mr. Roger Cummings | P | Symantec |
| Mr. Anders Liverud | AV | Tandberg Storage |

18 People Present

Status Key: P - Principal

```
A,A# -  Alternate
AV   -  Advisory Member
L    -  Liaison
V    -  Visitor
```

## Results of Meeting

### 1. Opening remarks and introductions [Peterson]

Dave Peterson thanked Hitachi Cable Manchester for hosting and people introduced themselves.

### 2. Approval of agenda (06-426r0) [Peterson]

The Agenda was modified to remove already closed items.

Dave Peterson made motion to approve agenda as modified. Paul Suhler seconded. Voting was unanimous.

### 3. Approval of meeting minutes (06-338r0) [Peterson]

Dave Peterson made a motion to approve the minutes. Kevin Butt seconded. Voting was unanimous.

### 4. Review of old action items [Butt]

**4.1 Dave Peterson: Bring in a White Paper on the value added with Explicit Command Set.**

Carry-Over

**4.2 Dave Peterson: Review initiator vs I_T nexus throughout document.**

Done. Editors note in document.

**4.3 Michael Banther: Bring in proposal to improve handling of cleaning and firmware upgrade cartridges.**

Carry-Over

**4.4 Michael Banther: Bring in proposal for Requested Recovery log page from ADC.**

Carry-Over

**4.5 Kevin Butt: Bring proposal following direction related to clean behavior.**

Carry-Over

**4.6 Kevin Butt: add cleaning bits from 05-213 to his proposal and find log page for them.**

Carry-Over

**4.7 Roger Cummings: produce a proposal to describe the events that shall activate and deactivate the cleaning related tape alert flags and to add a second flag for predictive failure of the medium.**

Carry-Over

**4.8 Banther: Revise and post SSC-3 Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0)**

Carry-Over

**4.9 Kevin Butt: Provide associated text, inside the cleaning proposal for 2.1.1 of 05-351r2.**

Carry-Over

**4.10 Kevin Butt: revise and post Configurable EW (05-423r0)**

Done

**4.11 Micheal Banther: Create a proposal to add additional activation conditions to TapeAlert. See note in 05-154r3 to bring in new proposal for this additional info.**

Carry-Over

**4.12 Dave Peterson: Create a proposed document for feedback to the ISV's.**

Done 05-351.

**4.13 Dave Peterson to incorporate 06-120r3 into SSC-3.**

Done

**4.14 David Black to revise and post 06-141r0.**

Error in document number. Can't find what it should be. Remove.

**4.15 Paul Suhler to revise and post SSC-3: Physical device model (05-049r3)**

Done

**4.16 Kevin Butt to revise and post 06-138r0**

Done

**4.17 Gideon Avida to revise and post SSC-3: Add Encrypted Write Command proposal (06-207r1)**

Done

**4.18 Greg Wheeless will define the scope of the problem - what is to be solved to replace the Security Association derivation proposal.**

Greg no longer works for Symantec. This action needs a new owner. David Black will create an unathenticated SA proposal. Overtaken by events.

**5. Old business**

**5.1 Physical device model (05-049r4) [Suhler]**

Paul went over changes from last time. Some minor changes were made.

Reference SPC-4 and ADC-2.

Paul Suhler made a motion and Michael Banther seconded to include 05-094r4 as modified into SSC-3.

### 5.2 Vendor Feedback (05-351r1) [Group]

Defer

### 5.3 Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0) [Banther]

Defer

### 5.4 Configurable EW (05-423r1) [Butt]

Kevin presented changes. Corrections and suggestions made. Kevin to contact ISV's other than CA and determine if the prefer the UA approach or the No Sense approach. Create new revision.

### 5.5 Using NIST AES Key-Wrap for Key Establishment (06-225r3) [Ball]

Defer

### 5.6 Add Encrypted Write Command proposal (06-207r2) [Avida]

Gideon went over the changes. Kevin Butt asked for description to be added for Check Condition that will be returned for Write command when lock field is set to 11b. A new ASC/Q is needed. Paul Entzel asked for cross-reference in Write and Write Encrypted commands to the lock table.

Dave Peterson had Gidean change "Data" to "Logical Blocks"

Add text to Write(6) and Write(16) commands about how the lock field effects them and add cross-reference.

Chris Williams is concerned that nobody will implement this command and is not convinced of its necessity.

Kevin Butt does not think this will be implemented. History has shown that new items that have other ways of doing things don't get implemented.

Roger Cummings thinks that this is useful. When asked if they will twist tape vendors arms to implement it, he said no because they have no marketing requirements to do this.

Chris Williams believes that this will be overtaken by the fully authenticated method.

Roger kind of agrees with Chris, because they are interested in getting authenticated between applications and devices.

Straw Poll: Does anyone see any value of continuing this proposal? 1:6:5

[Agenda item not complete.]

Paul Suhler - What is required to get authenticated to applications? Some kind of protocol changes and other difficult things. A study group would be needed.

### 5.7 Position after Self-Test (05-140r1) [Banther]

Defer

### 5.8 TapeAlert Delineation (06-138r1) [Butt]

Kevin presented the rewrite and Michael Banther had issues with not allowing thresholding. The suggestion is to go back and put into a new log page that can be expanded for additional information related to each tapealert.

### 5.9 Authentication Concerns for Encrypted Key Transfer (06-329r0) [Wheeless]

Defer. Greg no longer works for Symantec. Roger and others will discuss offline and we will discuss what is to be done next meeting cycle.

## 6. New Business

### 6.1 Modifications to Tape Data Encryption (06-385r0) [Entzel]

Question was raised about if the Random Number was OK to pass in the clear accross the interface before it is used for a NONCE or IV.

David Black is concerned that this be a truely random number that can not be used to figure out how the number is generated (i.e. cannot find a way to predict it). There will need to be a note to warn against using the random number for some uses.

Discussion about length of RandomNumber was that the author was addament that 32 bytes is what will be returned.

Ralph Weber presented example text from 06-369r3 section 5.13.3 and suggested the second paragraph. Paul Entzel will pull the Random Number portion of the proposal and create a separate proposal for this.

Minor corrections in other sections were made.

Paul Entzel made a motion and Chris Williams seconded to include 06-385r0 as modified into SSC-3.

[INCORPORATE into SSC-3 and remove from agenda]

### 6.2 Remove IV fields from the Data Encryption Algorithm descriptor (06-391r0) [Entzel]

These fields were added before there was a P1619.1 and were for work-arounds if IV not done correctly. No changes were made. Paul Entzel made motion and Chris Williams seconded to incorporate 06-391r0 into SSC-3.

[INCORPORATE into SSC-3 and drop agenda item.]

### 6.3 Using Public-Key Cryptography for Key Wrapping (06-389r0) [Avida]

Gideon presented the proposal. David Black asked about replay prevention. He wants that added.

David wants this to go to CAP. Paul Entzel wants to get to symetric keys because of the time expense to unwrap the public key. The portion to pass the public key needs to go into SPC-4.

### 6.4 SCSI Communications Security (06-431r0)[Black]

This document was not posted. This goes with 06-369 and the threats proposal 06-388.

David Black will send the secretary the document number once he posts it.

David Black went over the document which describes security issues.

### 6.5 Keyless Copying of Encrypted Media and Other Topics (06-412r0) [Suhler]

Paul presented the proposal.

For section 3, returning CC the ISV needs to work out what the specific drive needs. This could make the algorithm interesting in the future. The KAD needs to be fully self-describing (Roger). May just need to add bit in algorithm to specify that algorithm needs to pad.

Section 4.3: No changes.

Section 5.3: some will check.

Can we use Security Meta-data term for M-KAD.

Need to cover the case where change of encrypted to unencrypted needs notification but not KAD data. (i.e. all crypto information transitions with the raw block.)

### 6.6 I_T Nexus basis encryption text vs. LUN[Peterson]

Worried about clause 4.2.19.2 and not having L in I_T Nexus. Agreed to add L to I_T Nexus in this paragraph except not to ALL I_T NEXUS. The “N” in I_T Nexus s/b “n”.

### 6.7 Editors Notes from SSC-3 Discussion [Peterson]

Dave took the group through some Editors Notes that needed group attention.

## 7. Liason reports

### 7.1 P1619.1 Status report [Ball]

## 8. Next Meeting Requirements (Las Vegas)

Same time.Tuesday after FCP-4. 11-7

## 9. Review of new action items

**9.1 [Roger Cummings; David Black] Decide what to do about item 5.9 (06-329r0)**

**9.2 [David Peterson] Incorporate “Remove IV fields from the Data Encryption Algorithm descriptor (06-391r0)” into SSC-3**

**9.3 [Paul Entzel] Revise and post “Modifications to Tape Data Encryption (06-385r0)”**

**9.4 [Dave Peterson] Incorporate “Modifications to Tape Data Encryption (06-385r0)” into SSC-3**

**9.5 [Dave Peterson] Sweep SSC-3 for I_T Nexus and change to I_T nexus.**

Done

**9.6 [Dave Peterson] Modify clause 4.2.19.2 of SSC-3r3a to add L per discussion item 6.6.**

**9.7 [Kevin Butt] Query ISV’s about UA vs No Sense in Configurable EW (05-423r1)**

**9.8 [Kevin Butt] Revise and post Configurable EW (05-423r1)**

**9.9 [Kevin Butt] Revise and post TapeAlert Delineation (06-138r1)**

## 10. Adjournment

Dave Peterson made a motion for adjournment at 6:18 pm eastern. Seconded by Kevin Butt.