SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-338r0)
Date: July 7, 2006
Time: 10:00 am - 5:00 pm
Location: Colorado Springs, CO

# Agenda

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

**2. Approval of agenda (06-135r0) [Peterson]**

**3. Approval of meeting minutes (05-434r0) [Peterson]**

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

**5. Next meeting requirements (San Jose, CA)**

**6. Review of new action items**

**7. Adjournment**

# Attendance

SSC-3 Working Group Attendance Report - July 2006

| Name | S | Organization |
|---|---|---|
| Mr. Noud Snelder | V | BDT |
| Mr. Gideon Avida | P | Decru |
| Mr. Robert H. Nixon | P | Emulex |
| Mr. Ralph O. Weber | P | ENDL Texas |
| Mr. Curtis Ballard | V | Hewlett Packard |
| Mr. Michael Banther | V | Hewlett Packard Co. |
| Mr. Kevin Butt | A | IBM Corp. |
| Mr. David Peterson | P | McDATA |
| Mr. Faisal Faruqui | AV | NeoScale Systems Inc. |
| Mr. Landon Noll | AV | NeoScale Systems Inc. |
| Mr. Frederick Knight | A | Network Appliance |
| Mr. Matthew Ball | V | Quantum Corp. |
| Mr. Paul Entzel | P | Quantum Corp. |
| Dr. Paul Suhler | A | Quantum Corp. |
| Mr. Erich Oetting | A# | Sun Microsystems, Inc. |
| Mr. Steven Sletten | V | Sun Microsystems, Inc. |
| Mr. Greg Wheeless | A | Symantec |

```
17 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 LSI Logic for hosting and people introduced themselves.

### 2. Approval of agenda (06-135r0) [Peterson]

The Agenda was modified to remove already closed items.

Dave Peterson made motion to approve agenda as modified. Greg Wheeless seconded. Voting was unanimous.

### 3. Approval of meeting minutes (06-244r0, 06-265r0, 06-292r0) [Peterson]

May SSC-3 WG Minutes (06-244r0) [Butt]

May 31 Conference Call (06-265r0) [Butt]

SSC-3 NIST Key wrapping Phone call (06-292r0) [Butt]

Dave Peterson made a motion to approve the minutes. Paul Suhler 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.

Carry-Over.

#### 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 Michael Banther: revise and post 05-140r0

Done

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

Carry-Over.

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

Carry-Over.

**4.8 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.

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

Carry-Over.

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

Carry-Over.

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

Carry-Over.

**4.12 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.

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

Carry-Over.

**4.14 Dave Peterson to incorporate SSC-3: Target Device Serial Number subpage (05-155r4) into SSC-3**

Done Rev2a

**4.15 Kevin Butt to revise and post SSC-3: Secure Data Erase (06-120r2).**

Done

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

Carry-Over - on table for rev3a

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

Carry-Over

**4.18 Matt Ball revise and post SSC-3: Using NIST AES key-Wrap for Key Establishment (06-225r0)**

Done

## 5. Old business

### 5.1 SSC-3: Physical device model (05-049r3) [Suhler]
### ADC: Device Structure Model (06-334r0) [Butt]
### SSC-3: SCSI Domain Model with Physical Device (06-333r0) [Butt]

Discussed 06-333r0. there should be no relationship between SCSI Target Device and Physical device. The Question was raised about if all the attrivutes in the Physical device should be in the same device or in different devices. Cardinality was discussed.

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

### 5.2 SSC-3: Vendor Feedback (05-351r1) [Group]

Defer

### 5.3 SSC-3: Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0) [Banther]

Defer.

### 5.4 SSC-3: Configurable EW (05-423r0) [Butt]

Defer

### 5.5 SSC-3: Using NIST AES Key-Wrap for Key Establishment (06-225r3) [Ball]

Kevin Butt from IBM raised the issue that this proposal relies on an already established security association. It is the foundation for this key wrapping and we are opposed to this without a method in SCSI defined to create a Security Association.

Greg Wheeless, Dave Peterson, and Gideon Avida agreed.

Greg suggested he might volunteer to work on creating a proposal to create a Security Association.

Discussion revolved around what level of protection is needed.

AI: Greg Wheeless will define the scope of the problem - what is to be solved.

IETF owns the copyright to RFC’s so T10 cannot use some of these things in here as they appear to be derivative works. This must be corrected. FC-SP uses bits and pieces of the RFC but says if you want to do it like RFc go see RFC.

HP cannot support the proposal until how to create an SA is established.

AES Key-wrapped key references NIST, but it is ambiguous as to what it is.

Gideon: why are you using NIST instead of GCM? especially since you are adding two integrity checks.

Matt: I will change from NIST to an algorithm we defined that is based on GCM as specifid by NIST and IETF as far as how to integrate with a protocol (ESP). We can reference NIST. Will use a frame similar to RFC4303 for the frame. Use just SHA-512.

### 5.6 SSC-3: Add Encrypted Write Command proposal (06-207r1) [Avida]

Discussion centered around if the Write Encrypted (16) should be removed (i.e. only put this in Explicit command set).

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

### 5.7 SSC-3: Encrypt keys for transfer to device (06-103r2) [Black]

Defer

### 5.8 SSC-3: Position after Self-Test (05-140r1) [Banther]

Defer

## 6. New Business

### 6.1 SSC-3: TapeAlert Delineation (06-138r0) [Butt]

Greg Wheeless wants Kevin to correspond with him. direction is to remove the Set/Clear columns and add a method to inform Application client about the “Recoverability” and “Severity” of the error. Inq VPD page suggested but not necessarily static. New flags was rejected. Add log page that dynamically specifies these.

Kevin Butt to revise and post 06-138r0.

### 6.2 SSC-3: Vendor-specific Service Actions for MAINTENANCE IN/OUT (06-223r0) [Banther]

Removed - Overcome by events

### 6.3 SSC-3: Align clean notification names (06-235r1) [Banther]

This was already accepted by the ADI WG.

Michael Banther moved for inclusion into SSC-3 and Paul Entzel seconded. Passed Unanimously.

### 6.4 Discussion of key integrity validation [Butt]

Key Corruption - Can interlock to its own hashing. App puts in db and then its corrupted. If drive messes up transformation.

Need is because if corrupted cannot read anything on tape.

Utility: Could store the Hash it is simpler than AES. 4-byte CRC with a known algorithm. Like 4-byte Reed-Solomon could actually correct the data if less than 255 bytes. We can provide algorithm from ECMA 319 if desired. 32-byte Key.

Cryptographic CRC (e.g. SHA-1, SHA-256) - Maybe do SHA-256 and use first 8 bytes. (Can use as Signature and check if this signature matches what was sent previously - is not reversable or guess anything about key)

(Any linear CRC can be leaky - if keys sent with one bit different then the CRC will change by a known algorithm. Signature would have to be done separately)

Reed-Solomon CRC (can use to autocorrect data if less than 255 bytes)

Binary CRC (e.g. Fibre CRC)

The group as a whole believe this is stupid. Suggestion from group are:

Should we put this into the wrapped-key.

Not thrilled about 32-bit CRC.

Do not use a transport layer CRC. Unique CRC only.

Suggested pass Key twice.

xor'ing all bytes.

### 6.5 ADC-2: Reporting Microcode download in progress thru DT Activity and other fixes (06-180r1) [Marks]

Michael Banther moved to include in SSC-3 and Kevin Butt seconded. Passed Unanimously.

### 6.6 SSC-3: Modification of the REPEAT bit behavior in the Tape Diagnostic Data log (06-293r0) [Marks]

Discussion revolved around reporting of Medium ID number.

Kevin Butt moved to incorporate into SSC-3 SSC-3: Modification of the REPEAT bit behavior in the Tape Diagnostic Data log (06-293r0) as revised and Michael Banther seconded. Passed Unanimously.

### 6.7 SSC-3: Authentication Concerns for Encrypted Key Transfer (06-329r0) [Wheeless]

Concerned about not authenticating the end-points. Threats to be mindful of. Need to authenticate the endpoints and the messages. A lot of discussion ensued about the information in this proposal. concerns about using the same key for wrapping as authentication. This discussion led to some strong arguments about what level of encryption was necessary and/or acceptable. No real resolution was achieved. Quantum pointed out that there is an interface to the library that has enthernet and ipsec so he has the secret channel to get a key.

One key point Greg wants to make is that there is a customer base who cannot afford the public key scenario and we need to not forget them.

(Sun) You want to have a third party authenticator.

### 6.8 P1619 Status Report (06-339r0)[Ball]

This proposal show a web page that can be referenced for seeing the latest.

http://ieee-p1619.wetpaint.com

Next meeting July 19 for P1619.1. Can get info at webpage.

Latest draft P1619.1-D8.

## 7. Next Meeting Requirements (Nashua)

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

**8. Review of new action items**

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

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

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

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

**9. Adjournment**

Dave Peterson made a motion for adjournment at 5:35 pm central. Seconded by Kevin Butt.