SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-265r0)
Date: May 31, 2006
Time: 10:00 am - 12:00 pm Central Time
Location: Conference Call

Agenda

1. Opening remarks and introductions [Peterson]

2. Approval of agenda (06-056r0) [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 - May 2006

Name	S	Organization
Mr. Gideon Avida	P	Decru
Mr. David Black	A	EMC Corp.
Mr. Michael Banther	V	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. David Peterson	P	McDATA
Mr. Matthew Ball	V	Quantum Corp.
Mr. Paul Entzel	P	Quantum Corp.

7 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]

The intent of this conference call is to cover 06-225 and 06-103.

2. Approval of agenda [Peterson]

No formal agenda.

3. Approval of meeting minutes [Peterson]

Not done since this is a conference call.

4. Review of old action items [Butt]

Action Items not reviewed.

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

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

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

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

4.5 Michael Banther: revise and post 05-140r0

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

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

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.

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

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

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

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.

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

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

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

4.16 David Black to revise and post 06-141r0.

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

5. Old business

5.1 SSC-3: Physical device model (05-049r2) [Suhler]

5.2 SSC-3: Vendor Feedback (05-351r2) [Group]

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

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

5.5 SSC-3: Add Encrypted Write Command Proposal (06-207r0) [Avida]

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

5.7 SSC-3: Using NIST AES key-Wrap for Key Establishment (06-225r1) [Ball]

David Black referenced RFC4306 document as having IKE SA. Section 2.17 references using child SA's which might be an advantage to ignore some keys.

Matt says this version allows independent keys. NIST KVM function is desired.

David: you have picked up the IKE generation - differences between 2.14 and 2.17 of RFC4306.

Matt: Key wrap uses just one key. It is set up such that we don't need to gen the keys we don't need. Discussion about how we can certify this as FIPS-140 if it is not included in FIPS-140.

David Black prefers to use an existing protocol. I think we will run into trouble for the nonce and dh exponent reuse. Some discussion about elliptic curve may be better to use. Need to add in that NIST KVM allows you to generate only the keys that will be used. Discussion about requiring a minumen of 256 bit keys.

Matt: I strongly prefer not to introduce SHA_1 to the SCSI standards.

David Black:We need to be able to have large amounts of data in the payload.

Kevin Butt: I thought we were going to rely on the transport layer to encrypt the data.

David Black: I agree but I am trying to think about what others might be tempted to use this for. Maybe SAM will desire to use something at the SCSI layer.

Michael Banther: What is our resolution on 256 bit keys and higher?

Matt Ball: We will use 256 bit keys but if other protocols use something less, thats OK.

David Black: I think the answer is yes and we should allow changing the PRF.

Matt: I am not opposed to allowing other key generation functions.

David Black: We want to generate the entire KDF because we don't like the prf+. We should have the pure NIST kdf plus....

Michael Banther: You have a "shall be 256 bits" but that does not match what was said earlier.

This wrapping key is using a KEK (Key Encryption Key) to encrypt the key.

X9.102 draft proposal from working group X9F1.

David Black: Table Y9 is almost a reinvention of ESP.

There was a lot of discussion using a lot of acronymns that non-security people had a hard time following.

Matt: Please review. I would like to at least get the key wrap into SSC-3. Do we move to get this all into SSC-3 and then into CAP or initially into CAP?

Paul Entzel: What is to be moved into CAP? All of 4.2.20?

David Black: Yes.

Paul: That means it will be at least 6 to 9 months until key wrapping can get into SSC-3.

A discussion followed on the risk of changes in SPC to this if we put it into SSC-3. Will it change and how much and how. Will it just be a superset?

Discussion about maybe getting a study group together for this and taking it into CAP.

Kevin Butt: I think this should go into CAP so that tape is not different than the rest of the world again. This will keep the software common for tape with disk instead of having to have special software for tape.

Section 8 needs to stay in SSC-3.

Matt to send source in MS Word to David Black so he can get 4.2.20 and put it with his proposal.

Matt: My preference is to use this doc as it stands into SSC-3.

Kevin Butt: Why don't you take 4.2.20.1 - 4.2.20.4 to CAP and get it into SPC-4. This part can probably be done fairly easily.

Matt: I want to get something voted into SSC-3 by next conference call.

Michael: Please specify the lengths in a manner that those values that may grow in the future are "at least" and those that shall be henceforth and forever this size use shall be this size.

Matt: Please send me comments so I can get a version out in one week so I can meet the 2-week rule.

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

5.9 SSC-3: Align clean notification names (06-235r0) [Banther]

5.10 Discussion of key integrity validation [Butt]

6. Next Meeting Requirements (San Jose, CA)

Conference call June 21, 10 am - 12 pm Central time.

Same time.Tuesday after FCP-4.

7. Review of new action items

Not Reviewed.

8. Adjournment