SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-170r0)
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. David Black
Ralph O. Weber                   P  ENDL Texas
Chris Williams
Rob Elliott
Mr. Matt Ball Quantum
Mr. Kevin Butt                       A  IBM Corp.
Mr. David Peterson                   P  McDATA
Mr. Paul Entzel                      P  Quantum Corp.
Mr. Dwayne Edling                    A# Sun Microsystems
Mr. Roger Cummings                   P  Symantec
Mr. Greg Wheeless                    A  Symantec
```

Results of Meeting

1. Old business

1.1 The Requirement for More than One Decryption Key (06-051r5 [Edling]

CKORSC needs added in.

Modified some wording.

This proposal needs to go in 05-446 before it’s approved or Sun cannot vote for 05-446. The discussion is that we can try to vote on both at the same time.

1.2 SSC-3: Add commands to control data encryption (05-446r9) [Entzel]

Went through IBM email comments.

TECHNICAL:

1) Section 4.2.9.13, pg 6, last sentence of 2nd to last paragraph, "The device server shall establish the logical position at the BOP side the encrypted block." should be "The device server shall establish the logical position after the failed encrypted block." This will make the behavior consistent with reading a corrupted block.

[Paul Entzel] I disagree for two reasons:

1. ***This will add an extra step to the recovery process. The expected recovery for this type of error is to send a SPIN command requesting the Next Block Encryption Status page, send a SPOUT command with a Set Data Encryption page configuring the encryption accordingly, and the re-issue the read. If the tape is positioned behind the block in error it will add another command to this recovery process to re-position in front of the block first. <<Kevin Butt>> It was my understanding that this was known to be a bad block (i.e. corrupted) as opposed to just a wrong key or algorithm. Is my understanding in error?***

2. ***The Sense Key used to report the error is DATA PROTECT. Not change the logical position when reporting this error is consistent with other conditions that use this Sense Key. <<Kevin Butt>> If my understanding stated above is correct (i.e. the block is corrupted) then this Sense Key should be MEDIUM ERROR instead. However, if I am in error, then I agree with your comments.***

   <phone conf.>> In some implementations this may be the only way to report that the key is wrong. Consensus is to leave it as written in proposal.

   2) Section 4.2.19.5, pg 8. All the statements about establishing a UA for all other I_T Nexus that are affected by....

   If this is the behavior that we take, then this will severely inhibit being able to use a third party device - like a Decru EKM transparent to the application. The UA's will cause the applications or host on which the applications reside, to handle these UA's that it knows nothing about.

[Paul Entzel] I have never been a big fan of UAs. As a developer of SCSI devices I have always found them to be a complete pain in the rear. They're difficult to deal with when protocol bridges are used. They get eaten by the driver stack on the host side. Yuck. However, this is how we manage asynchronous event reporting in SCSI. This will be an interesting discussion topic tomorrow.

I think the UA's should be restricted to those I_T Nexus over which a Security Protocol Out/In command has been received and not to any body else. This will allow using an External EKM transparent to applications.

[Paul Entzel] Interesting idea you have there. It will need to be developed a bit more before it will work, but it has potential. I interpret your idea as adding a Boolean variable to the per I_T Nexus database defined in subclause 4.2.19.6 that indicates if a SPIN or SPOUT command has been executed from the I_T Nexus. Only I_T Nexus that have this variable set to True would get UAs associated with encryption. I have two questions:

1. ***When does it get set to False (resets, I_T Nexus loss, de-mount)?***

2. ***How do we document this precedence setting feature?***

<<Kevin Butt>> I was thinking about how Persistent Reserve handles UA's and some of the UA's only get established for those I_T Nexus that are registered. I was think this would be similar to that.

<<phone conf.>> The suggestion is to have I_T Nexus to register for UA's related to Encryption. There was discussion about UA's and if this would be general or only SPOUT. Anything we do on an I_T Nexus basis does not work well behind bridges. The question was asked if there were any objections to registering for UA's.

There were concerns about removing UA's all together.

The issue of LOCK and who gets notified was e-raised. There probably should be a method to have the I_T nexus who sets encryption to be able to designate that the application on a different I_T Nexus gets the Check Condition.

A lot of discussion about LOCK and how that is or could be used varying from per I_T Nexus to one lock per device server. The LOCK as it is currently written is what will be moved. If anyone thinks it should be different, then please bring in a proposal.

Agreed to change UA such that, SPOUT or SPIN command that specifies Tape Data Encryption protocol implicitly registering for UA.

{Paul Entzel} Scratch the phrase "set by a Set Data Encryption page" and change "scope" to "key scope"

everyone agreed.

<<Phone conf: HP>> In 4.2.19.5 lists add option c "Establish data encryption parameters sent by the page"

Everyone agreed.

<Roger> Need to add something about if scope is local.

3) Section 4.2.19.6, pg 8, second list. Should a "Prohibit Encryption" be added?

[Paul Entzel] Not necessarily. If the SCOPE field is set to PUBLIC then control of data encryption for that I_T Nexus is passed to other initiators and may or may not be enabled. <<Kevin Butt>> With PUBLIC and no PROHIBIT ENCRYPTION there is no way for an I_T Nexus to make sure encryption is not used (i.e. guarantee that if there is encryption being used in the SAN, that they will not be effected by it.) I do not know which direction should be taken but I think it should be discussed and a explicit decision made on it.

<Phone Conf> covered by using LOCAL with disable.

4) Section 4.2.19.7, pg 9. Please add "CKORSC" to list.

[Paul Entzel] Agreed.

5) Section 4.2.19.7, pg 9. Item c) of list - key scope. I was confused here and it took me some time to realize that "key scope" is referring to a value in Table Y2 for the "scope" field of the set data encryption page. Please add a definition and/or cross reference for this term.

[Paul Entzel] Everything in this structure comes from fields in the Set Data Encryption page or from knowledge the device server has about the I_T Nexus that sent the Set Data Encryption page. Of course, I supposed it is possible to use an out-of-band method for establishing the data encryption parameters (see comment 6).

<<Kevin Butt>> I remember this discussion from the last conference call, but I still struggled with it. Is there something that can be done to make it more clear? I think if I am this thick headed, there will be other readers just as thick headed as I am.

<<Phone Conf.>> No change needed.

6) The following changes are desired by IBM. We do not want to prohibit any out-of-band methods from being used.

Section 8.5.2.7, pg 19, last paragraph. Remove the text "by processing a Set Data Encryption page."

Section 8.5.2.7, pg 20, first three paragraphs, change the text

"in the Set Data Encryption page that established the key in the device server."

to

"when the key was established in the device server."

<<Phone Conf>> agreed. Last paragraph has two instances.

[Paul Entzel] I think that would work. Or, I thi8nk both of these paragraphs could be re-written to reference the Data Encryption Parameters since the data they are reporting is in that structure. <<Kevin Butt>> That would probably be better.

<<Phone Conf.>> pg 25, second to last para. Does CKORSC mean SCOPE or TYPE of PR?

Should this be changed to PREEMPT or PREEMPT AND CLEAR? CKORP. Agreed.

2. Next Meeting Requirements (San Jose, CA)

Conference calls Thurs. 30th at 11:00 Central.

3. Adjournment

Call ended at 11:50 MST