SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-085r0)
Date: January 25, 2006
Time: 1:00 pm - 3:00 pm MST
Location: Phone Conference

Agenda

1. Old Bussiness

1.1 SSC-3: Add commands to control data encryption (05-446r3) [Entzel]

1.2 SSC-3: Pass key by Reference Model (06-050r1) [Edling]

1.3 The Requirement for More than One Decryption Key (06-051r2) [Edling]

2. Next meeting requirements

3. Review of new action items

4. Adjournment

Attendance

SSC-3 Working Group Attendance Report - January 2006

Name	S	Organization
Mr. Ron Roberts	A	Broadcom Corp.
Mr. Gideon Avida	V	Decru
Mr. Chris Williams V		Hewlett Packard
Rob Elliot		HP
Mr. Kevin Butt	A	IBM Corp.
Mr. David Peterson	AV	McDATA
Mr. Paul Entzel	P	Quantum Corp.
Dr. Paul Suhler	A	Quantum Corp.
Sandy Stewart		Sun
Dwane Edling		Sun
David Cuddihy		ATTO Technology

11 People Present

Status Key:
- P - Principal
- A,A# - Alternate
- AV - Advisory Member
- L - Liaison
- V - Visitor

Results of Meeting

5. Old Bussiness

5.1 SSC-3: Pass key by Reference Model (06-050r1) [Edling]

Paul Entzel is concerned about the term unique in 4.2.19.5

Several people were concerned that it might not be testable. However, the requiremnet is that the identifier is unique within the scope of this environment. Remove unique so we don't get nailed in letter ballot.

The question was raised if the 8 byte vendor identification field is part of the vendor specific key reference or not. How is the 8 byte vendor ID field used.

Paul Entzel, please put description of fields into the table.

The intent is to use the 8 byte vendor id field from SPC.

Chris Williams concerned about UA's being generated. Will discuss in 05-446 discussion.

AI: Dwayne to make changes and send to Paul Entzel for inclusion into 05-446.

5.2 The Requirement for More than One Decryption Key (06-051r2) [Edling]

Dwayne gave an overview of what the number of keys fields.

Kevin Butt: I don't understand how the device server knows which key to use. Dwayne said this is done in a vendor-specific method. This statement will be added to the proposal.

Paul Entzel would like the description of the counts to be "the number of keys that can be stored with a key value of encrypt..."

Paul Entzel would be willing to consider reducing all the number of scopes and reducing the complexity.

Table S1 needs to have the description of number of keys to match the verbage suggested above.

The number fields should be related to the "source" field or "scope" field that this I_T nexus is referring to. It is really total that is desired so get rid of the mode and scope in the description.

Paul Entzel: Is there value in an "Encrypt Only" key use? No is the response. This can simplify to COMBINED and ADDITIONAL DECRYPT.

The combined key can be used to clear all other decryption keys and then can set the additional key bit for the additional decrypt keys. It is down to one bit.

Chris Williams: Are we setting one decryption key or multiple?

Kevin wanted to have it configurable that you could limit total number of keys to one. Paul's response was to write a proposal against -5-446.

Chris Williams requires ability to guarnatee there is only one key in use.

Paul Entzel - maybe we should go back and remove the Scopes.

Rob Elliott suggested that we change things such that the scope is a subset of the key instead of the current key is a subset of scope.

5.3 SSC-3: Add commands to control data encryption (05-446r3) [Entzel]

Question about having both incorrect data encrypiton key and data authentication key. Won't it help somebody crack the key.

Default mode is to not encrypt.

How do you guarantee that the write is encrypted?

KBR_C bit needs to be expanded. Discussion revolved around moving this and adding an entire page for how you can do keys, etc. To describe methods of key management like wrapping keys.

Add key management capabilities page now to allow for exapnsion in the future and move the KBR_C bit into that page as more detail.

Discussed Kevin's email subject line "SSC-3: Comments to 05-446r3" Kevin will provide text for the external with verify.

Unit Attentionns discussion. there is a hole because in many environments they will get intercepted below the applications. We should be OK with read because if you read with wrong key or encryption turned off there will be an error. In the Write there is an issue because you might not know and write in wrong mode. Lock is supposed to take care of this, but there is still concern.

Need to add wrapping of generation and should wrap to one not zero.

6. Next meeting requirements (Feb. 8 Phone Conference)

7. Review of new action items

7.1 Dwayne to make changes to 06-050r1 and send to Paul Entzel for inclusion into 05-446

7.2 Dwayne to make changes to 06-051r2 and post

7.3 Paul Entzel to rev and post 05-446r3

7.4 Kevin write proposal to limit to one key

7.5 Kevin write text for External with verify

8. Adjournment

Call ended at 2:59 MST.