Draft Minutes
Encryption Key Management Study Group
T10/06-010r0
Conference Call of 29 November 2005
12:00 PM – 2:00 PM EST

1. Introductions — Group

Chris Williams called the meeting to order at 12:00 PM EST.

2. Approval of the Agenda — Chris Williams

Chris Williams discussed the order of the discussion items. Michael Banther made a motion to accept the agenda. Paul Suhler seconded the motion. The group passed the motion unanimously.

3. Attendance and Membership — Chris Williams

Chris Williams reviewed the T10 attendance rules with the group and directed prospective new members to John Lohmeyer. The attendance report appears below.

Encryption Key Management Study Group Attendance:

Name	S	Organization
Mr. Tom Treadway	V	Adaptec, Inc.
Mr. Rod Wideman	V	ADIC
Mr. James Fu	V	ADIC
Mr. Robert H. Nixon	P	Emulex
Mr. David Crespi	V	Emulex
Mr. Mike Fitzpatrick	P	Fujitsu
Mr. Rob Elliott	P	Hewlett Packard Co.
Mr. Chris Williams	V	Hewlett Packard Co.
Mr. Curt Kolovson	V	Hewlett Packard Co.
Mr. Michael Banther	V	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. Paul Greco	V	IBM Corp.
Mr. Bill Colvin	V	Kasten Chase
Mr. John Geldman	P	Lexar Media, Inc.
Mr. Martin Furuhjelm	A	Lexar Media, Inc.
Mr. Pat LaVarre	A#	Lexar Media, Inc.
Mr. John Lohmeyer	P	LSI Logic Corp.
Mr. Jeff Rogers	V	LSI Logic Corp.
Mr. Greg Elkins	V	Marvell Semiconductor
Mr. Mike Witkowski	V	MaXXan Systems
Mr. Ram Iyer	V	MaXXan Systems
Mr. David Peterson	AV	McDATA
Mr. Allen Martin	V	Nvidia Corp.
Mr. Tim Symons	P	PMC-Sierra
Mr. Amr Wassal	V	PMC-Sierra
Mr. Matt Bondurant	V	ProStor Systems
Mr. Jim Jones	V	ProStor Systems
Mr. Mark Payne	V	ProStor Systems

Mr. Paul Entzel	P	Quantum Corp.
Dr. Paul Suhler	A	Quantum Corp.
Mr. Gerald Houlder	P	Seagate Technology
Mr. Dave Anderson	V	Seagate Technology
Mr. Gary Moorhead	V	Seagate Technology
Mr. Jason Cox	V	Seagate Technology
Mr. Erich Oetting	A#	Sun Microsystems, Inc.
Mr. Steven Sletten	V	Sun Microsystems, Inc.
Mr. Roger Cummings	P	Symantec
Mr. Greg Wheeless	A	Symantec
Mr. Ed D'Avignon	V	Vitesse Semiconductor
Mr. Jim Scott	V	Vitesse Semiconductor

4. INCITS Patent Policy — Chris Williams

Chris Williams directed the group to a reading of the T10 Short Summary of the INCITS Patent Policy.

5. Discussion Items — Group

5.1 Call for straw man presentations. [Chris Williams]

Chris Williams asked for any additional strawman presentations for today's meeting, or for the meeting next week. Roger Cummings indicated that Symantec would bring a requirements presentation. Dave Anderson from Seagate indicated that Seagate would be bringing one if attendance was possible.

5.2 Technical direction – clarifying the objective of this study group. [Chris Williams]

Chris Williams proposed the following technical direction for the study group:

a. Define a draft proposal for encryption/decryption control that is tape specific, but flexible enough to allow foe expansion.
b. Identify appropriate working group.
c. Present the proposal to that working group for full discussion, and disband the study group.

Greg Wheeless: we need a general solution that won't be only useful for tape.

Dave Anderson: we don't want multiple ways to do key management within T10.

Roger Cummings: we need something available soon for tape. We don't want to mechanisms that won't be needed for tape if that delays the proposal.

Michael Banther: we need to state up front with what other standards we seek to be compliant.

Kevin Butt: 06-007r0 is a useful illustration for this discussion.

Greg Wheeless: note that the scope of this study group is only the communication protocol for key management, not application-layer security practices.

Steven Sletten: the proposal should be able to be generalized to support all storage devices, disk and tape. Greg Wheeless agreed.

Matt Bondurant: removable disk and optical data at rest should also be considered.

The group discussed the subject of device authentication. The question was raised whether there was an existing IEEE standard that handled device authentication.

Martin Furuhjelm: IEEE P1667 will address authentication of devices in a transport independent way, but the focus is transient storage devices

Michael Banther asked for consensus that device/server authentication should be a follow-on project, so that this proposal could be completed in a reasonable time. There were no objections.

Michael Banther asked Gerry Houlder whether there anything in the trusted computing commands that would preclude their use for our purpose. Gerry Houlder replied that nothing would prohibit this, but it would be useful to have a discussion about whether the commands would penetrate reservations. This would be useful for more than just TCG. The commands provide for authentication but not require it. Greg Wheeless noted that commands that provide for authentication but not require it would be ideal for our purpose.

Gerry Houlder: we will try to bring a proposal.

5.3 Encryption - Layers Discussion (06-007r0). [Kevin Butt]

Kevin Butt asked for consensus that the scope of the study group be limited to the top layer in his diagram, noting that there were considerations belonging to a layer above those presented in his diagram that should also be excluded, and for consensus specifically that authentication was not to be the subject of this study group, except that we should not prevent the addition of authentication in a future proposal. There were no objections.

5.4 SSC-3: Input for Encryption Strawman 05-432r0). [Kevin Butt]

Kevin Butt summarized his proposal. Paul Suhler noted the need for the group to have more details on IEEE P1619.1. Greg Wheeless cautioned that we want to not limit any key lengths or related lengths with fixed sizes, that all lengths should be self-describing. It was noted that the algorithm identifier would suffice in some cases, but not all (some formats have differing lengths available).

Roger Cummings noted that the encryption method used for data currently on a medium and the list of potential encryption methods available for use on that medium are different issues, and should be kept distinct in encryption method enquiries.

Michael Banther asked whether the key identifier represented what was used for the data on a medium, or what algorithms could be used for writing data to a medium. Kevin Butt replied that it represented what was used, but added there was value in being able to report what could be used.

5.5 SSC Encryption Strawman (06-006r0). [Chris Williams]

Chris Williams summarized his proposal, and noted it was designed for SSC devices only. He also noted the proposal was P1619 compliant (but not limited to that).

Greg Wheeless suggested that we need to be able to include more information than just a key when setting a key, in an arbitrary way. Chris Williams agreed, but noted that additional data cannot always be handled transparently; the format of that data may need to be specified in the protocol.

Greg Wheeless noted that from an ISV perspective he saw value in key identifiers, and in the ability to read a mix of encrypted and unencrypted data with one transfer (but not a mix of differing encryption keys). Chris Williams noted that key identifiers were part of P1619 compliance.

Greg Wheeless noted that from an ISV perspective he did not see value in “raw reads” and “raw writes” of encrypted data, and that to allow external software recovery of encrypted data would require the compression algorithm used to also be clearly defined. The group noted that raw reads and writes were useful to allow data to be copied without knowing the key, and for similar data management.

The group recognized that key management for fixed block commands is important and should be addressed in some manner.

5.6 SSC-3: Add commands to control data encryption (05-446r0). [Paul Entzel]

Paul Entzel summarized his proposal, and noted that his definition of an encrypted block does to handle the case of raw encrypted write, and that such a definition will be problematic in the formal language of the standard.

The group discussed raw reads and writes of encrypted data at length. Greg Wheeless warned that this would require the copying of format-specific meta-data along with the data to enable key identifiers and encryption algorithms to be retrieved for the data. The group discussed this at length, and agreed that in any case the study group should not specify any format specific mechanisms for recording meta-data.

Group discussed reservation with regards to key loss. Paul Entzel noted that quantum had surveyed ISVs regarding this and other issues relating to his proposal, and warned that some ISVs don’t support reservations. The group concluded that the reservation case and the no-reservation case must both be handled.

Greg Wheeless noted that we must consider key retention within a device in the context of the security implications of a shared device, as an authorized user interacting with the device should not accidentally allow an unauthorized user access.

Paul Entzel noted that at least one ISV doesn’t get unit attentions, so an additional mechanism is needed to confirm that encryption is still enabled with each write.

The definition of “additional authenticated data” was sought, and the group noted the need for an error recovery mechanism when the wrong key was used.

The group agreed that a mechanism for identifying encryption algorithms should be used that does require T10 to act as a registry for encryption algorithms, especially as other such registries already exist.

5.7 Agenda for December face-to-face meeting. [Chris Williams]

Chris Williams: the agenda for the 2005/12/05 face-to-face meeting should include the following items:

a. HP will present a brief summary of P1619 requirements.
b. Symantec will present a brief summary of requirements form an ISV perspective.
c. Review the existing strawman proposals.
d. Discuss to which working group a proposal should be submitted.
e. Formulate a draft proposal.

6. Unscheduled Business Group

There was no unscheduled business presented.

7. Next Meeting Requirements — Chris Williams

The Encryption Key Management study group will meet on Monday, 5 December 2005, beginning at 9:00 AM and concluding at 4:00 PM during T11 week at the Crowne Plaza Anaheim Resort, 12021 Harbor Boulevard, Garden Grove, California 92840.

The following meeting is scheduled for Thursday, 12 January 2006, beginning at 1:00 PM and concluding at 6:30 PM during T10 plenary week in Scottsdale, AZ.

8. Adjournment — Group

Chris Williams adjourned the group at 2:10 PM EST.