Draft Minutes
Encryption Key Management Study Group
T10/06-015r0
05 December 2005
9:00 AM – 4:00 PM PST

1. Introductions — Group

Chris Williams called the meeting to order at 9:00 AM PST. He thanked Jim Nelson Northrop Grummond for providing the facilities for hosting the meeting.

2. Approval of the Agenda — Chris Williams

Chris Williams discussed the order of the discussion items. Kevin Butt 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. Fabio Maino	V	Cisco
Mr. Gideon Avida	V	Decru
Mr. Kenneth Hirata	A	Emulex
Mr. Ralph Weber	V	ENDL
Mr. Sumit Puri	V	Fujitsu
Mr. Chris Williams	V	Hewlett Packard Co.
Mr. Nobuyuki Osaki	V	Hitachi
Mr. Kevin Butt	A	IBM Corp.
Mr. John Lohmeyer	P	LSI Logic Corp.
Mr. David Peterson	AV	McDATA
Mr. Larry Hofer	V	McDATA
Mr. Paul Entzel	P	Quantum Corp.
Dr. Paul Suhler	A	Quantum Corp.
Mr. Dwayne Edling	V	Sun Microsystems, Inc.
Mr. Roger Cummings	P	Symantec
Mr. Greg Wheeless	A	Symantec
Mr. Ed D'Avignon	V	Vitesse Semiconductor
Mr. Rich Ramos	P	Xyratex

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. Approval of Previous Meeting Minutes — Chris Williams

Two corrections were made to section 5.6 to add the word “not”.

David Peterson made a motion to accept the meeting minutes as modified. Paul Suhler seconded the motion. The group passed the motion unanimously.

6. Discussion Items — Group

6.1 Presentation on P1619 requirements. [Chris Williams]

Chris Williams presented a short summary of the standard and answered several clarifying questions. The relationship between this study group and IEEE P1619 was reiterated: this study group is working towards a proposal for the management of keys used by P1619 and similar standards, and not working towards an encryption algorithm.

It was noted that the key identifier is the responsibility of the ISV to generate.

Fabio Maino, the secretary of P1619, noted that the spec is still quite preliminary.

The Auth Tag digitally signs both the plaintext and the AAD (additional authenticated data).

It was noted that P1619 is just one of many encryption algorithms with which this study group’s proposal will seek compatibility.

6.2 Symantec requirements presentation (06-012r0). [Greg Wheeless]

Greg Wheeless made a presentation on Symantec’s requirements from the perspective of a tape backup ISV.

Kevin Butt noted that from his conversation with other ISVs they want more than just bit to select, they want a tag to define which application is controlling the encryption.

Fabio Maino asked whether multiple simultaneous keys would be needed, especially to cover the special case of transitioning between keys. The group concluded that this is not necessary for tape.

Paul Entzel asked why logical unit reset was not listed in the clear key conditions. Greg Wheeless responded that keys should be cleared when multiple other tape drive parameters were clear because of an event, which is only sometimes true of logical unit reset.

6.3 Decru presentation on requirements from an enterprise security perspective. [Gideon Avida]

Gideon Avida presented information on requirements and standards needed for enterprise customers, noting that key management requirements in the field go even beyond the FIPS standard and other standards.

It was noted that there are third-party devices in the field that will emulate tape devices, and which can do more with key management than a SCSI device server would be expected to. The ability to support “load key by reference” would be important to support these devices.

The problems of both encrypted key transfer and endpoint authentication are important to these requirements. Ralph Weber notes that solving encrypted key transfer without solving endpoint authentication is problematic from a security standpoint.

6.4 Discussion – to which group should we present a proposal? [Chris Williams]

Kevin Butt asked for an explanation of the important differences between disk and tape in the requirements for this proposal. Fabio Maino replied that there were many similarities, but that disk needs to assure the integrity of the LBA of the data. It was noted that the Trusted Computing Group is the only group currently working on disk encryption, and has made some progress in that area.

Chris Williams noted that layering on the TCG commands would be an inherent problem, as we don't have all of their standards documents. Greg Wheeless noted that we can't propose a T10 standard that depends on a non-public document as part of its specification. There was discussion about whether TCG would be compatible

Paul Entzel noted that taking this to SSC, even using the TCG commands, would allow us to generate a proposal soon, but noted the risk in using a command we don't control. Greg Wheeless questioned whether taking the proposal to SSC would give it enough exposure within T10, especially for removable random-access media and transient random-access devices.

There was discussion about the ability to use the TCG spec when it's not public. Roger Cummings noted that a requirement for making the standard public coming from this group would be useful to take back to the TCG. Roget Cummings will take our requirements to the TCG and report back to the study group.

There was discussion about how to work around the TCG requirement for trusted in and trusted out to penetrate reservations. Greg Wheeless suggested that the penetration of reservations be made TCG protocol id specific. Paul Entzel noted that retrieving a CA should penetrate reservations.

Chris Williams suggested that it wouldn't matter whether we used the TCG command set or another command set, the meat of the proposal will be the same. General consensus was that this proposal must be taken into SSC if we want it adopted soon, whether or nor we use the TCG commands.

Greg Wheeless noted his desire for the standard to have one way to do key exchange for both disk and tape in T10, and cautioned that an SSC-specific approach would limit that unnecessarily. The group noted that disk and tape have fundamentally different requirements in the key exchange.

The group discussed the value of using the trusted in/out commands vs. a new command, and what impact that would have on the group to which we should bring the proposal. Roger Cummings noted that it might solve the problem if Trusted In penetrated reservation and Trusted Out didn't. Roger Cummings to bring the subject of our reservation issues to the TCG storage systems working group and report back to this group.

Kevin Butt made a motion that the draft proposal that results from this study group should be submitted to the SSC-3 working group. Paul Entzel seconded the motion. The motion passed 6:0:6.

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

Discussion was tabled.

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

Discussion was tabled.

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

The group discussed the terminology for the data associated with an encrypted block. Paul Entzel noted that authenticated data must be written with each block, but unauthenticated data can be stored in a directory, saving resources. The term “Key ID” would be inappropriate for the unauthenticated associated data because the proposal will not impose the restrictions on this data needed for a Key ID, so the term “Key Associated Data” is proposed.

Greg Wheeless suggested the need for a term, such as “Encryption Method”, which was more specific than “Encryption Algorithm”, that meant “all information needed to specify how encryption was done”, such as key length used.

Fabio Maino asked whether we should attempt to define the fields used to pass the key and associated at all, given there will always be an algorithm with requirements we didn’t anticipate.

The group discussed methods for identifying the algorithm used without involving T10 as a registry.

Roger Cummings expressed concern about the case where a device is power cycled, thereby clearing the key, but persistent reservation was not lost. Dwayne Edling expressed concern about key loss on vendor specific events such as firmware load.

The group discussed the sense key to return when encrypted data was unexpectedly encountered. Consensus was that DATA PROTECT was appropriate.

Paul Entzel noted that distinction between reading the KAD for the data from the most recent Set Key command, and the KAD data for the next block to be read. The latter may not always be available. Greg Wheeless noted that the KAD for the block about to be read needs to always be available if a read was just rejected with a DATA PROTECT.

The group discussed the purpose of preventing exhaustive key search. Chris Williams will bring a proposal to modify the exhaustive search section of 05-446r0.

The group discussed out-of-band methods for setting and clearing keys, and noted that out-of-band methods should be tracked by a key generation counter, as with any other means that might update the key.

Kevin Butt asked whether a pre-empt of a persistent reserve should clear the key, even though the reservation was not cleared, as the scope of the reservation changed. The group consensus was that the key should be cleared when the scope of the reservation changes.

The group discussed the key format field values, noting the need for a “key by reference” value. Dwayne Edling will provide a model clause description for “key by reference”. Gideon Avida explained that the case where the device server will generate a key as needed is a special case of “key by reference” and does not require its own format field value.

Greg Wheeless requested a bit in the Set Key page to reject write commands if the key generation changes, and that was not done explicitly done by the initiator.

Kevin Butt called the group’s attention to the following contact information for CA for T10 discussions:

Tim Chou (BrightStor Development) choti01@ca.com 631-342-6249

Mat Dickson (BrightStor Development) dicma01@ca.com 631-342-3813

6.8 Formulate a draft proposal for encryption key management. [Group]

Greg Wheeless made a motion that 05-446 be adopted as the current working draft of the study group's proposal. Paul Suhler seconded the motion. The motion passes 6:0:4.

7. Unscheduled Business — Group

There was no unscheduled business presented.

8. Next Meeting Requirements — Chris Williams

As per discussion item 6.8, work on this subject will transition to SSC3 and this study group has concluded.

9. Review New Action Items — Greg Wheeless

a. Roger Cummings to bring the concerns of this group regarding the non-public nature of the Trusted Computing Group standards to that organization, and report the results of that discussion back to this group.

b. Roger Cummings to bring the concerns of this group regarding the ability of the Trusted In and Trusted Out commands to the Trusted Computing Group per discussion item 6.4, and report the results of that discussion back to this group.

c. Chris Williams will bring a proposal to modify the exhaustive search section of 05-446r0, per discussion item 6.7.

d. Dwayne Edling will provide a model clause description for "key by reference", per discussion item 6.7.

e. Paul Entzel to revise 05-446r0 and post per discussion items 6.7 and 6.8.

f. Chris Williams to notify T10 reflector and others that the study group will not need time on Thursday during the T10 plenary week, and we will need a larger room for SSC.

10. Adjournment — Group

Kevin Butt made a motion for adjournment. Dwayne Edling seconded the motion. The group passed the motion unanimously. Chris Williams adjourned the group at 4:00 PM PST.