To: INCITS Technical Committee T10

From: Kevin Butt, IBM

Date: November 7, 2005 10:16 pm

Document: T10/05-432r0

Subject: SSC: Encryption Strawman

# 1. Revisions

# 2. Introduction

In light of HP's stated intent to bring in a proposal on encryption and being willing to accept comments prior to doing so, IBM would like to submit the following strawman to assist in this effort. The proposal should be interoperable with IEEE P1619.1. and meet the intents of Table 1

**TABLE 1. IBM Thoughts on Encryption Standards for Tape**

| Item | Information Needed to Appropriately Cover Encryption | IBM Recommended method |
|---|---|---|
| 1 | Query of Drive capability (e.g. is Drive Encryption capable, what Algorithm Identifiers are supported) | Inquiry Page |
| 2 | Query if mounted medium is of a type that is able to be encrypted | Read Attribute |
| 3 | Query if data on the mounted medium is Encrypted. | Read Attribute |
| 4 | Method for an application to tell the drive what Algorithm Identifier, Key, and Key Index to use.<br>1) Key (Write Only?).<br>Format depends on Algorithm Identifier (e.g. 32 Byte Value for AES-256).<br>Value set to zero should be Reserved.<br>2) Key Index needs to be determinable from medium(there may be multiple keys/key indexes per medium). 16 Byte Value.<br>3) Algorithm Identifier needs to be determinable from medium. (e.g. RSA, AES, etc.) Single Algorithm for entire medium? or multiple? | Write Attribute or<br>Mode Parameters<br>(Key is device server specific; Key Index and Algorithm identifier need to be determinable from medium)<br>This should be a set that is transferred together |
| 5 | Method for an application to Read the Key Index and the Algorithm Identifier. | Read Attribute |
| 6 | Indication to the application should be generated on a Read when a Key change occurs (e.g. Read into a different Key) or on a Write when a Key is Required | Check Condition/Unit Attention |
| 7 | Encryption Specific TapeAlerts<br>1) Tape is encrypted<br>2) Encryption fault detected<br>3) Decryption fault detected<br>etc. | |

**TABLE 1. IBM Thoughts on Encryption Standards for Tape**

| Item | Information Needed to Appropriately Cover Encryption | IBM Recommended method |
|---|---|---|
| 8 | Check Conditions for other errors related to Encryption. (e.g. Wrong Key being used, Encryption Error, Decryption Error, etc) | |
| 9 | Query of Key Status<br>1) Key Needed<br>2) Key Pending (waiting for write to activate)<br>3) Key Active | Mode Sense<br>(these are device server specific and not medium specific)<br>How these are defined depends on what the scope of the Key is - per I_T Nexus or one for all I_T Nexuses |
| 10 | What is the scope of the Key?<br>1) All I_T Nexuses, or<br>2) Per I_T Nexus | Easier if Global but more protective and more issues if per I_T Nexus |
| 11 | A method for retrieving Audit information should be provided | Log Sense(for drive audits)<br>Read Attribute(for medium audits) |