From: Gerry Houlder, Seagate Technology <gerry.houlder@seagate.com>
Subj: SBC-3 Model for encrypting disk drives
Date: Aug. 12, 2008

Overview

There are a number of efforts under way to create protocols for doing authorization and enabling or disabling features of an encrypting disk drive. These efforts may not agree on the methods for doing these operations, but there is a need to standardize the resulting drive behavior when these features are enabled or disabled. This proposal is a start for that effort.

This text is all new.

Rev. 1: change to an informative annex.

SBC-3 changes:

Annex D
(informative)

Sense Code Descriptions for locking or encrypting SCSI Target Devices

Sense Key	ASC	Description
DATA PROTECT	ACCESS DENIED – NO ACCESS RIGHTS	SCSI target device is locked. May occur for reads, writes, or both. May occur for entire device or an LBA range. For recovery, initiator needs to perform a security protocol specific procedure to unlock access to the target device.
ABORTED COMMAND	LOGICAL BLOCK REFERENCE TAG CHECK FAILED	May occur on a read command. These codes may indicate that an encrypting SCSI target device has changed the encryption/ decryption key and these LBAs have not been rewritten yet. Disabling protection information checking in the CDB may allow the command to complete successfully but the returned data may be incorrectly decrypted. To restore correct operation, write the LBAs with new data.
ABORTED COMMAND	LOGICAL BLOCK APPLICATION TAG CHECK FAILED	
ABORTED COMMAND	LOGICAL BLOCK GUARD CHECK FAILED	