January 27, 2006 **06-050r2 Pass Key by Reference Model**

To: T10 Technical Committee
From: Dwayne Edling (dwayne.edling@sun.com)
Date: 27 Jan 2006
Subject: T10/06-050r2 Pass Key by Reference Model

Revision History

Revision 0 (7 Jan 2006) First Revision
Revision 1 (18 Jan 2006) Put into better T10 format

Related Documents

05-446r3 - SSC-3: Add commands to control data encryption

Overview

This proposal incorporates changes that would be necessary to implement passing keys by reference in proposal 05-446r1.

Revision 1

Changes

- Put proposal in more acceptable T10 format.
- Added T10 vendor ID as the first 8 bytes of the key reference.
- Added VENDOR SPECIFIC KEY REFERENCE NOT FOUND as a new ASC.

Revision 2

Changes

- Removed unique in the description of the key reference.
- Reject a key reference is the Vendor ID does not match.
- Add SPC references for the Vendor ID.
- Updated to use 05-446r3.

Suggested Changes

4.2.19.5 Managing keys within the device server

The security provided by data encryption is only as good as the security used when managing the keys. For this reason, the data encryption key and mode are volatile in the device server and the data encryption keys are never reported to an application client. The device server also may have limited resources for storage of keys.

A device server that supports encryption shall support at least one of the following methods for an application client to send the keys used for encrypting or decrypting data;

a) Sending the Key; or
b) sending a Vendor Specific Key Reference.

A Vendor Specific Key Reference is an ~~unique~~ identifier for a specific Key that is known by the device server. If this method is used to send a key to the device server the KBR_C bit shall be set in the Data encryption algorithm descriptor page shown at Table E2.

The method by which keys and key reference numbers become known to the device server is outside the scope of this standard.

If a device server processes a Set Data Encryption page with the ENCRYPTION MODE field set to DISABLE and DECRYPTION MODE field set to DISABLE or RAW, the device server shall release any resources that it had allocated to store a key value for the I_T nexus associated with the SECURITY PROTOCOL OUT command and shall clear all memory containing the key value. A unit attention condition with the additional sense of DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR shall be establish for all other I_T nexus that are affected by the loss of the key, (i.e., any I_T nexus that is using a scope of PUBLIC and sharing the key.)

Editor's note: DATA ENCRYPTION MODE CHANGED BY ANOTHER INITIATOR is a new ASC.

Table Y5 and the following text:

Table Y5 – KEY FORMAT field values

Value	Description
00h	Key is in plain text
01h	Vendor Specific Key Reference
02h – FFh	Reserved

The KEY LENGTH field indicates the length of the key field in bytes.

The KEY field contains the encryption key to use when encrypting and decrypting data.

If KEY FORMAT field is 00h, the KEY field contains the Key to be used to encrypt or decrypt data.

If the KEY FORMAT field is 01h, the KEY field shall contain the T10 VENDOR INDENTIFCATION field, specified in "T10 Vendor ID Based Designator Format" section of SPC-4, followed immediately by a Vendor Specific Key Reference identifying the Key to be used to encrypt or decrypt data.

If KEY FORMAT is 01h and the KEY field contains a Vendor Specific Key Reference that is unknown to the device server or the VENDOR IDENTIFICATION field does not match the VENDOR IDENTIFICATION provided by the device server, Check Condition status shall be returned. The Sense Key shall be set to ILLEGAL REQUEST and the ASC/ASCQ shall be set to "KEY REFERENCE NOT FOUND".

Editors Note: VENDOR SPECIFIC KEY REFERENCE NOT FOUND is a new ASC.

If the ENCRYPTION MODE field is set to ENCRYPT the device server shall save the key-associated descriptors in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field and associate them with every logical block that is encrypted with this key by the device server. If more than one key-associated data descriptor is include in the page, they shall be in increasing numeric order of the value in the DESCRIPTOR TYPE field. If the ENCRYPTION MODE field is not set to ENCRYPT and key-associated descriptors are included in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field, the device server shall terminate the command with CHECK CONDITION, with the Sense Key shall be set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.