To: INCITS T10 Committee
From: Paul Entzel, Quantum
Date: 7 November 2006
Document: T10/06-502r0
Subject: SSC-3 Alternative method for keyless tape copy

1 Revision History

Revision 0:

2 Reference

T10/SSC-3 revision 3a
T10/06-0462r0, SSC3, Keyless Copy of Encrypted Data [Butt]

3 General

T10 document 06-462r0 proposes changes to SSC-3 to provide details on how to use the EXTERNAL encryption mode and RAW decryption mode to enable copying data from an encrypted tape to another tape without knowledge of the encryption key. Quantum agrees that more detail is required in this regard, but recommends a different approach to solving this problem for several reasons:

1. 06-462r0 introduces a new state machine into the device server to manage the RAW read process. The proposal does not define all of the state transitions and some of the missing transitions will be complicated to add.
2. 06-462r0 will not work with Explicit Mode commands without extensive re-work. While Quantum is not a big fan of the Explicit mode commands, we prefer they be removed from SSC-3 due to lack of support rather than because they were broken inadvertently.
3. 06-462r0 defines several variations in the operation for the application client that vary based on the tape format, but does not define a method for the application client to discover the mode that is required.
4. It is completely unclear as to how the process is managed in the source device server if more than one I_T nexus is accessing the device.
5. 06-462r0 defines a model for two distinct classes of medium formats:
    a. One where the format places a requirement on the destination device server that it be notified when transition between encrypted data and unencrypted data by changing the encryption mode from EXTERNAL to DISABLED. In this model, in addition to encryption mode changes, all changes in KAD data detected by the source device server must be reported to the application client so they can be passed on to the destination device's device server.
    b. Another where the format does not have the requirement described above such that transitions between encrypted data and unencrypted data do not required a change in the encryption mode use by the destination device's device server.

    Some tape formats used by Quantum tape drives do not fit into either of these models.
6. The approach used in 06-462r0 is more complex than necessary to solve the problem it is addressing.

Quantum would prefer an alternative approach be used to solve this problem. This approach should work with the medium format models described in 06-462r0 (although we see little value in the second model) in addition to other medium models. This approach eliminates the new state machine in favor of the application client taking a more explicit role in the overall process.

06-462r0 assumes that the medium format includes metadata associated with an encrypted block that will not be passed to the application client when a RAW read is performed. This assumption may not be true for all medium formats. Quantum approach provides a mechanism for the device server to report if there is any metadata required to be passed between the source and destination device servers outside of the RAW block. It also provides a mechanism for the application client to explicitly set the state of the source device to eliminate all of the implicit state changes suggested by 06-462r0.

The tape copy sequence would follow the following steps:

1. The application client sends a SECURITY PROTOCOL IN command requesting a new page of data called the Keyless Copy Metadata page. This page includes KAD descriptors containing any additional metadata that the medium format requires be associated with the EXTERNAL and RAW modes of operation.
2. The application client sends a SECURITY PROTOCOL OUT command to the source device containing a Set Data Encryption page. The DECRYPTION MODE is set to RAW. The page contains a zero length key. The page includes all KAD descriptors included in the Keyless Copy Metadata page.
3. The application client sends a SECURITY PROTOCOL OUT command to the destination device containing a Set Data Encryption page. The ENCRYPTION MODE is set to EXTERNAL. The page contains a zero length key. The page includes all KAD descriptors included in the Keyless Copy Metadata page from the source device.
4. The application client issues READ(6) or READ(16) commands to the source device. For each block read, the device server checks the metadata associated with the encrypted block against the KAD data it received in the Set Data Encryption page. If there is a mismatch, an error is reported as described in 06-462r0.
5. SPACE, LOCATE, and REWIND commands have no impact on the process since the metadata was established explicitly by the application client.
6. Any key clearing event will also clear the metadata associated with the mode RAW of operation. Other events will not.

4 Changes to SSC-3

Quantum can provide details if the working group prefers this approach to the approach described in 06-462r0.