TO: T10 Membership, ADC-3 Working Group
FROM: Rod Wideman, Quantum; rod.wideman@quantum.com
DATE: July 9, 2008
SUBJECT: ADC-3 Remove Configure Encryption Policy mounted volume restriction (document T10/08-247r1)

Rev0 – Initial draft.
Rev1 – Updated to accommodate feedback received on initial draft; now includes provision for use of offline and appropriate unit attention.

Related Documents
ADC-3r00b

Introduction
This document proposes a change to 6.3.5.3, Configure Encryption Policy page, to modify a restriction when a volume is mounted, as well as a change to 6.2.2.3.2, RMC logical unit descriptor format, to clarify what happens on a transition from offline.

Discussion
Subclause 6.3.5.3 currently states that if the DT device has a saved set of data encryption parameters or has a volume mounted the ADC device server shall terminate the command. This restriction creates a problem for automation devices, particularly in power-on scenarios. If one or more volumes are mounted in DT devices (i.e., drives), and a power cycle occurs, then this restriction would require the automation device to unmount each mounted volume prior to configuring each drive again, which can be impractical in certain automation products.

Following a power cycle, there would not be a saved set of data encryption parameters anyway, so this additional restriction for this scenario appears unnecessary (i.e., RMC application clients need to retrieve policy status again regardless). However, removing this restriction entirely may create a problem for applications that retrieved encryption control information when a volume was mounted, and expect it to remain unchanged for the duration of the volume mount.

Subsequent discussion noted that this may be alleviated via strategic use of the sense code NOT READY TO READY CHANGE, MEDIUM MAY HAVE CHANGED (i.e,. 28h/00h), which should cause applications to again retrieve information important to them. Based on this, a statement is added to existing text that specifies the behavior when the OFFLINE bit in the RMC logical unit descriptor changes from one to zero (which was probably lacking anyway). This proposal then also modifies the restriction of a mounted volume when configuring the encryption policy.

As a result, automation products should be able to re-establish encryption control following a power cycle without having to unmount each volume.

Proposed Changes to ADC-3

Proposed new text is shown in blue. Proposed deletions are shown in ~~red strikeout~~.

Changes to 6.3.5.3
(Third paragraph following table 72)

The CONTROL POLICY CODE field specifies the data encryption parameters control policy for the DT device (see 4.10.1). If the DT device has a saved set of data encryption parameters or has a volume mounted and the OFFLINE bit is set to zero in the RMC logical unit descriptor (see 6.2.2.3.2), then the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

Changes to 6.2.2.3.2, RMC logical unit descriptor format
(First paragraph following table 55)

If the OFFLINE bit is set to one, then the RMC device server shall return CHECK CONDITION status with the sense key set to NOT READY and the additional sense code set to LOGICAL UNIT NOT READY, OFFLINE to all commands that require the RMC logical unit to be in the ready state. If the OFFLINE bit is set to zero, then the RMC device server shall respond normally to commands. If the OFFLINE bit is changed from one to zero, then the RMC device server shall establish a unit attention condition with an additional sense code of NOT READY TO READY CHANGE, MEDIUM MAY HAVE CHANGED.