TO: T10 Membership, ADC-3 Working Group
FROM: Rod Wideman, Quantum; rod.wideman@quantum.com
DATE: May 14, 2008
SUBJECT: ADC-3 Remove Configure Encryption Policy mounted volume restriction (document T10/08-247r0)

Rev0 – Initial draft.

Related Documents
ADC-3r00b

Introduction
This document proposes a change to 6.3.5.3, Configure Encryption Policy page, to remove a restriction when a volume is mounted.

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 appears unnecessary (i.e., RMC application clients need to retrieve policy status again regardless).

This proposal removes the restriction of a mounted volume when configuring the encryption policy.

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, then ~~or has a volume mounted~~ 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.