ADC-3

Automation Encryption Control

Potential configuration security hole
Issue

• DT Device Management Interface is used to control encryption
• Drive is standalone or in a tape library without encryption aware firmware.
• Customer Policy is “Always Encrypt”
• A case exists where drive may write in the clear
How does it happen?

- External device sets encryption policy over some undefined management interface (likely Ethernet)
- Library or standalone drive is power cycled
- Drive powers up with default “no key request” policy
- ISV has pending backup waiting for drive to become ready. Loads tape before encryption manager can set policy
- Tape threaded in drive prevents set policy
- ISV performs backup
Potential Solutions

• Extension to encryption controls for “Persist” to be used by external control
  – Issue: What to do if the drive gets moved
• Always request key on first write after reset
  – Issue: How to differentiate “drive not in encryption aware environment” from “key manager not responding”
Question

• These are theoretical issues that may not occur in actual practice.

• Does the ADI working group feel we should address this issue?

• Do the group members have any preferences for how this should be addressed.