To
INCITS T10 Committee

From
Curtis Ballard, HP
Michael Banther, HP
Rob Elliott, HP

Subject
Automation Controlled Encryption Corrections

Date
22 February, 2008

Revision History
Revision 0 – Initial document.

Related Documents
spc4r09 – SCSI Primary Commands
adc2r07c – Automation/Drive Interface Commands
08-029r2 – ADC-3 Automation Encryption Control

Background
After 08-029r2 was voted on and approved for incorporation into ADC-3 a few issues in the proposal were identified which should be corrected. This proposal presents the identified issues and proposes corrections for them.

In the proposed changes that follow, new text appears in blue, deleted text appears in red-strikeout comments appear in green.

Proposed Changes to ADC-3 08-029r2
Table y puts too strict of requirements on the values that should be reported in an Encryption Algorithm Support page. The table requires that when the policy type is ADI exclusive, then the ENCRYPT_C field and the DECRYPT_C field shall be set to capable with external control but that is only the appropriate response if the command is received over the primary port. For a page returned in response to a command received over the ADI port the device server should report that the device is capable with software encryption or hardware encryption. The table also requires that devices support receiving parameters over all interfaces because it uses a shall statement in the footnote.

**Table y – Data encryption parameters control policy**

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Policy Code</th>
<th>Description</th>
<th>Parameters Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Specific</td>
<td>0000b</td>
<td>Vendor specific</td>
<td>VS</td>
</tr>
<tr>
<td>Open</td>
<td>0001b</td>
<td>No interface has taken exclusive control of data encryption parameters. This is the default setting for the data encryption parameters control policy.</td>
<td>A</td>
</tr>
<tr>
<td>ADC exclusive</td>
<td>0010b</td>
<td>The ADC device server has exclusive control of the ability to establish or change data encryption parameters and shall report all data encryption algorithms in the list of algorithms reported by the DT device with the ENCRYPT_C field set to capable with external control and the DECRYPT_C field set to capable with external control.</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>0011b</td>
<td>The ADC device server has exclusive control of the ability to establish or change data encryption parameters and all algorithms are removed from the list of algorithms reported by the DT device (see SSC-3).</td>
<td>A</td>
</tr>
<tr>
<td>RMC exclusive</td>
<td>0100b</td>
<td>The RMC device server has exclusive control of the ability to establish or change data encryption parameters.</td>
<td>P</td>
</tr>
<tr>
<td>DT device</td>
<td>0101b</td>
<td>The DT device management interface has exclusive control of the ability to establish or change data encryption parameters.</td>
<td>P</td>
</tr>
<tr>
<td>management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>0110b – 1111b</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

**Parameters Control Key:**

- **A** = Allowed
- **P** = Prevented

If this device server or DT device management interface supports establishing or changing encryption parameters, then the DT device shall process a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.

The ADC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED.

The RMC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters. See the appropriate command set standard (e.g., SSC-3).

The commands for establishing or changing a set of data encryption parameters via a DT device management interface are beyond the scope of this standard.

The method for rejecting a command from a DT device management interface is beyond the scope of this standard.