To: Interested parties in 07-454r3 SMC-3 permission bits
From: Rod Wideman, Quantum; rod.wideman@quantum.com
Date: 12/18/07
Subject: T10/08-035r0, Comments on 07-454r3 SMC-3 permission bits

New Proposed table for the SMC-3 portion of the 07-454 proposal (based on Security call discussion of 12/18/07):

Requested command	Permissions		
	PHY ACC	ACC MCHGR	ACC MEDIUM
EXCHANGE MEDIUM		v	v
INITIALIZE ELEMENT STATUS		v	
INITIALIZE ELEMENT STATUS WITH RANGE		v	
MOVE MEDIUM		v	v
OPEN/CLOSE IMPORT/EXPORT ELEMENT	v		
POSITION TO ELEMENT		v	
PREVENT ALLOW MEDIUM REMOVAL	v		
READ ELEMENT STATUS		v	
REQUEST VOLUME ELEMENT ADDRESS		v	
SEND VOLUME TAG		v	

Plus the following new text:

The following commands shall, if implemented, be processed by the secure CDB processor without requiring CbCS extension (see SPC-4):
a) REPORT VOLUME TYPES SUPPORTED command; and
b) REQUEST DATA TRANSFER ELEMENT INQUIRY command.

Notes:
- Media changers do not read or write customer data, so DATA READ or DATA WRITE permissions are not used.
- SCSI commands that direct movement of media (i.e., not including commands that may cause incidental movement of media, e.g., INITIALIZE ELEMENT STATUS) are permitted via ACC MEDIUM.
- Some of the SMC-3 commands do not appear to involve 'parameter data' but rather have element status data instead (e.g., READ ELEMENT STATUS). Other commands involve robotic motion, but do not move media (e.g. POSITION TO ELEMENT). And still other commands are matched pairs, such that a single permission should govern both commands (i.e., SEND VOLUME TAG/REQUEST VOLUME ELEMENT ADDRESS). These commands are all permitted via a proposed ACC MCHGR (new name). This name was chosen to avoid overloading the meaning of other possible terms (e.g., 'ROBOTICS', 'ELEMENT') and facilitate a minimal number of permission bits (stands for 'media changer'; could spell it out if preferred).
- ACC MGMT was changed to PHY ACC to match previous changes to 07-454.
- Two commands don't appear suitable for requiring permissions, so new text is proposed to address that.
- Should SEND VOLUME TAG require an additional permission since it can be used to modify volume identifiers in the library? If so, would PARM WRITE be sufficient (which would separate it from REQUEST VOLUME ELEMENT ADDRESS), or would a new permission bit be justified for only that pair of commands? Should there be a new permission bit defined in SPC-4 that could be used (then SEND DIAGNOSTICS/RECEIVE DIAGNOSTICS RESULTS could be covered better perhaps).