

ENDL TEXAS

Date: 10 March 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: CbCS SECURITY PROTOCOL IN/OUT tweaks in SPC-4

Introduction

Because there was no prototype to clone, a potentially important requirement was omitted from 07-454r5.

Also, it might be useful to align the CbCS page codes between SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT.

Revision History

r0 Initial revision

Unless otherwise indicated additions are shown in **blue**, deletions in **red-strikethrough**, and comments in **green**.

Proposed Changes in SPC-4 r13

7.6.4 CbCS security protocol

7.6.4.1 Overview

If the SECURITY PROTOCOL field in a SECURITY PROTOCOL IN command (see 6.30) is set to 07h, then the command specifies one of the CbCS pages (see 7.6.4.2) to be returned by the device sever. The information returned by a CbCS SECURITY PROTOCOL IN command indicates the CbCS operating parameters of:

- a) The logical unit to which the CbCS SECURITY PROTOCOL IN command is addressed; or
- b) The SCSI target device that contains the well-known logical unit to which the CbCS SECURITY PROTOCOL IN command is addressed.

If the SECURITY PROTOCOL field in a SECURITY PROTOCOL OUT command (see 6.31) is set to 07h, then the command specifies one of the CbCS pages (see 7.6.4.4) to be sent to the device sever. The instructions sent in a CbCS SECURITY PROTOCOL OUT command specify the CbCS operating parameters of:

- a) The logical unit to which the CbCS SECURITY PROTOCOL IN command is addressed; or
- b) The SCSI target device that contains the well-known logical unit to which the CbCS SECURITY PROTOCOL IN command is addressed.

7.6.4.2 CbCS SECURITY PROTOCOL IN CDB description

The CbCS SECURITY PROTOCOL IN CDB has the format defined in 6.30 with the additional requirements described in this subclause.

When the SECURITY PROTOCOL field is set to CbCS (i.e., 07h) in a SECURITY PROTOCOL IN command, the SECURITY PROTOCOL SPECIFIC field (see table 419) specifies the CbCS page to be returned in the parameter data (see 7.6.4.3). If the CBCS bit is set to one in the Extended INQUIRY Data VPD page (see 7.7.4), the CbCS SECURITY PROTOCOL IN command support requirements are shown in table 419.

Table 419 — SECURITY PROTOCOL SPECIFIC field for the CbCS SECURITY PROTOCOL IN command

Code	CbCS page returned	Support	Reference
0000h	Supported CbCS SECURITY PROTOCOL IN pages	Mandatory	7.6.4.3.1
0001h	Supported CbCS SECURITY PROTOCOL OUT pages	Mandatory	7.6.4.3.2
0002h – 000Fh	Reserved		
0010h	Capabilities	Mandatory	7.6.4.3.3
0011h	Attributes	Mandatory	7.6.4.3.4
0012h	Reserved		
0012h 0013h	Set Master Key – Seed Exchange	Mandatory	7.6.4.3.5
0014h – FFFFh	Reserved		
0013h – FFFFh	Reserved		

If an CbCS SECURITY PROTOCOL IN command is received with the INC_512 bit set to one, the command shall be terminated with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

7.6.4.3 CbCS SECURITY PROTOCOL IN parameter data

...

7.6.4.4 CbCS SECURITY PROTOCOL OUT CDB description

The CbCS SECURITY PROTOCOL OUT CDB has the format defined in 6.31 with the additional requirements described in this subclause.

When the SECURITY PROTOCOL field is set to CbCS (i.e., 07h) in a SECURITY PROTOCOL OUT command, the SECURITY PROTOCOL SPECIFIC field (see table 420) specifies the CbCS page to be returned in the parameter data (see 7.6.4.5). If the CBCS bit is set to one in the Extended INQUIRY Data VPD page (see 7.7.4), the CbCS SECURITY PROTOCOL IN command support requirements are shown in table 420.

Table 420 — SECURITY PROTOCOL SPECIFIC field for the CbCS SECURITY PROTOCOL OUT command

Code	CbCS page sent	Support	Reference
0000h – 0010h	Reserved		
0011h	Set Attributes	Optional	7.6.4.5.1
0012h	Set Key	Mandatory	7.6.4.5.2
0013h	Set Master Key – Seed Exchange	Mandatory	7.6.4.5.3
0014h	Set Master Key – Change Master Key	Mandatory	7.6.4.5.4
0015h – FFFFh	Reserved		

If an CbCS SECURITY PROTOCOL OUT command is received with the INC_512 bit set to one, the command shall be terminated with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

7.6.4.5 CbCS SECURITY PROTOCOL OUT parameter data