ENDL
TEXAS

Date: 12 March 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: Capability-based Command Security (CbCS) [the rewrite]

Introduction

The rush to approve 07-454r5 concurrently with other security proposals such as IKEv2-SCSI and ESP-SCSI has lead to several nettlesome problems. Some prime examples are:

- The ability of the RECEIVE CREDENTIAL command to be used for a plaintext attack on the CbCS SA.
- There is too much dependence on a specific I_T Nexus for SA usage.

Rather than nickel-and-dime these changes, it is proposed to translate 07-454r5 into text that is at least 90% ready for incorporation in SPC-4 (i.e., the content of this proposal), review/revise that, and approve the result as a replacement for the already approved 07-454r5.

Related/Source Documents

This proposal incorporates material from the following T10 proposals:

07-454r5	Capability based Command Security {{not fully incorporated in this revision}}
08-101r1	SPC-4: CbCS field byte alignment changes {{not fully incorporated in this revision}}
08-128r0	SPC-4 RECEIVE CREDENTIAL command 'adjustments'
08-129r0	SPC-4 CbCS capability validation omissions
08-138r0	Constraints on SPC-4 SA creation based on Usage Type
08-141r0	CbCS SECURITY PROTOCOL IN/OUT tweaks in SPC-4

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

3.1.a CbCS extension descriptor: An XCDB descriptor (see 4.3.4.2) in which the EXTENSION TYPE field is set to 40h (i.e., CbCS) as described in 5.13.6.8.11.

18484 Preston Road, Suite 102 PMB 178, Dallas, TX 75252 214-912-1373 972-596-2775 Fx ENDL_TX@computer.org

4.3.4.2 The XCDB format

…

The EXTENSION TYPE field (see table 12) specifies the size and format of the extension parameters that follow in the XCDB descriptor.

Table 12 — EXTENSION TYPE field

Code	Descriptor Order [a]	Description	Extension size (bytes)	Reference
40h	first	CbCS extension descriptor	140	5.13.6.8.11
all others	Reserved			

[a] The order in which XCDB descriptors appear in an XCDB is arranged so that all the XCDB descriptors that follow an XCDB descriptor defined in a future version of this standard are also XCDB descriptors defined in a future version of this standard (i.e., after encountering one unrecognized XCDB descriptor, all subsequent XCDB descriptors are also going to be unrecognized).

{{The reference to the table footnote should have appeared in SPC-4 r12, but it was not present.}}

…

5.13.2.2 SA parameters

…

The USAGE_TYPE SA parameter shall be one of the values shown in table 49.

Table 49 — USAGE_TYPE SA parameter values

Value [a]	Description	Usage model	Usage data description	Reference
0000h - 0080h	Reserved			
0081h	Tape data encryption	ESP-SCSI [b]	None [c]	SSC-3
0082h - 8000h	Reserved			
8001h	CbCS authentication and credential encryption	ESP-SCSI [b]	None [b]	5.13.6.8
8002h - FFFFh	Reserved			
~~0082h - FFFFh~~	~~Reserved~~			

[a] USAGE_TYPE values between 8000h and CFFFh inclusive place additional constraints on how an SA is to be created as described in 7.6.3.5.13.

[b] ESP-SCSI usage is defined in 7.6.4.

[c] The usage data length field in the IKEv2-SCSI SAUT Cryptographic Algorithms payload (see 7.6.3.5.13) shall contain zero.

{{The 8001h value assignment in table 49 depends on the approval of 08-138.}}

…

5.13.6.8.7 Enforcement Manager class

…

5.13.6.8.8 CbCS Capability validation

{{All of 5.13.6.8.8 is new. Editing markups suspended.}}

The enforcement manager (see 5.13.6.8.7) shall validate the CbCS capability descriptor (see 6.r.2.3) included in the CbCS extension descriptor (see 3.1.a). If the validation fails, the enforcement manager shall interact with the secure CDB processor (see 5.13.6.8.6) in a way that causes the command containing the CbCS extension descriptor to be terminated with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

The enforcement manager's validation of a CbCS capability descriptor shall fail if any of the following conditions occur:

a) The DESIGNATION TYPE field contains a value that table x10 defines as reserved (see 6.r.2.3);
b) The CBCS METHOD field contains a value that table x11 defines as reserved (see 6.r.2.3) or a vendor specific value that the enforcement manager does not support;
c) The INTEGRITY CHECK VALUE ALGORITHM field contains a value that is:
   A) Not one of those that table 71 (see 5.13.8) lists as being an integrity checking (i.e., AUTH) algorithm;
   B) Is AUTH_COMBINED; or
   C) Is a vendor specific value that the enforcement manager does not support;
d) The CAPABILITY EXPIRATION TIME field contains a non-zero value and the value in the CAPABILITY EXPIRATION TIME field is lower than the current time value (i.e., the current number of milliseconds passed since midnight, 1 January 1970 UT);
e) The enforcement manager is contained within the secure CDB processor, the DESIGNATION TYPE field value is set to 1h (i.e., logical unit designation descriptor), and the contents of the DESIGNATION DESCRIPTOR field in which a logical unit name (see SAM-4) is indicated does not match the addressed logical unit;
f) The enforcement manager is contained within the SCSI target device (i.e., addressed as a well-known logical unit), the DESIGNATION TYPE field value is set to 1h (i.e., logical unit designation descriptor), and the contents of the DESIGNATION DESCRIPTOR field in which a SCSI target device is indicated does not match the SCSI target device that contains the addressed well known logical unit;
g) The DESIGNATION TYPE field value is set to 2h (MAM attribute descriptor) and either of the following are true:
   A) The ATTRIBUTE IDENTIFIER field in the DESIGNATION DESCRIPTOR field contains any value other than 0401h (i.e., MEDIUM SERIAL NUMBER); or
   B) The DESIGNATION DESCRIPTOR field contents do not match the MAM attribute of the volume residing in the addressed logical unit;
h) The POLICY ACCESS TAG field contains a non-zero value that does not match the Policy Access Tag attribute (see 5.13.6.8.10) of the addressed logical unit; or
i) The command in the CDB field of the extended CDB (see 4.3.4) that contains the CbCS extension descriptor is not permitted by the PERMISSIONS BIT MASK field (see 5.13.6.8.9).

5.13.6.8.9 Association between commands and permission bits

{{All of 5.13.6.8.9 is new. Editing markups suspended.}}

Table x1 — Associations between commands and permissions (Sheet 1 of 2)

Command	PERMISSIONS BIT MASK bits [a]						
	DATA READ	DATA WRITE	PARM READ	PARM WRITE	SEC MGMT	RESRV	MGMT
ACCESS CONTROL IN	never allow [b]						
ACCESS CONTROL OUT	never allow [b]						
CHANGE ALIASES	always allow [c]						
EXTENDED COPY	never allow [b]						
INQUIRY	always allow [c]						
LOG SELECT				✓			
LOG SENSE			✓				
MANAGEMENT PROTOCOL IN							✓
MANAGEMENT PROTOCOL OUT							✓
MODE SELECT(6)				✓			
MODE SELECT(10)				✓			
MODE SENSE(6)			✓				
MODE SENSE(10)			✓				
PERSISTENT RESERVE IN			✓				
PERSISTENT RESERVE OUT						✓	
READ ATTRIBUTE			✓				
READ BUFFER					✓		
READ MEDIA SERIAL NUMBER			✓				
RECEIVE COPY RESULTS	never allow [b]						
RECEIVE CREDENTIAL	always allow [c]						
RECEIVE DIAGNOSTIC RESULTS			✓				
REPORT ALIASES			✓				
REPORT IDENTIFYING INFORMATION			✓				
REPORT LUNS	always allow [c]						

[a] The command in the CDB field of the extended CDB (see 4.3.4) that contains the CbCS extension descriptor shall be allowed only when all of the bits marked with a ✓ in the row for that command are set in the PERMISSIONS BIT MASK field of the CbCS capability in the CbCS extension descriptor.

[b] If the CBCS bit is set to one in the Extended INQUIRY Data VPD page (see 7.7.4), this command shall never be allowed.

[c] This command shall always be allowed regardless of whether the CbCS extension descriptor is present and if the CbCS extension descriptor is present regardless of the value in the PERMISSIONS BIT MASK field.

Table x1 — Associations between commands and permissions (Sheet 2 of 2)

Command	PERMISSIONS BIT MASK bits [a]						
	DATA READ	DATA WRITE	PARM READ	PARM WRITE	SEC MGMT	RESRV	MGMT
REPORT PRIORITY			✓				
REPORT SUPPORTED OPERATION CODES	always allow [c]						
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	always allow [c]						
REPORT TARGET PORT GROUPS	always allow [c]						
REPORT TIMESTAMP			✓				
REQUEST SENSE			✓				
SECURITY PROTOCOL IN					✓		
SECURITY PROTOCOL OUT					✓		
SEND DIAGNOSTIC				✓			
SET IDENTIFYING INFORMATION				✓			
SET PRIORITY				✓			
SET TARGET PORT GROUPS				✓			
SET TIMESTAMP				✓	✓		
TEST UNIT READY	always allow [c]						
WRITE ATTRIBUTE				✓			
WRITE BUFFER					✓		

[a] The command in the CDB field of the extended CDB (see 4.3.4) that contains the CbCS extension descriptor shall be allowed only when all of the bits marked with a ✓ in the row for that command are set in the PERMISSIONS BIT MASK field of the CbCS capability in the CbCS extension descriptor.

[b] If the CBCS bit is set to one in the Extended INQUIRY Data VPD page (see 7.7.4), this command shall never be allowed.

[c] This command shall always be allowed regardless of whether the CbCS extension descriptor is present and if the CbCS extension descriptor is present regardless of the value in the PERMISSIONS BIT MASK field.

5.13.6.8.10 CbCS attributes

{{All of 5.13.6.8.10 is new. Editing markups suspended.}}

5.13.6.8.11 CbCS extension descriptor format

{{All of 5.13.6.8.11 is new. Editing markups suspended.}}

The CbCS extension descriptor (see table x2) allows the capability-based command security technique (see 5.13.6.8) to used with a SCSI command via the parameters specified in this subclause. Support for the CbCS extension descriptor is mandatory if CBCS bit to one in the Extended INQUIRY Data VPD page (see 7.7.4). When an extended CDB (see 4.3.4) includes a CbCS extension descriptor the CDB field may contain any CDB defined in this standard or any SCSI command standard (see 3.1.19).

Table x2 — CbCS extension descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	EXTENSION TYPE (40h)							
1	Reserved							
3								
4	CbCS capability descriptor							
75								
76	(MSB)							
139	INTEGRITY CHECK VALUE							(LSB)

The EXTENSION TYPE field contains 40h (i.e., CbCs extension descriptor).

The CbCS capability descriptor is defined in 8.2.1.

The INTEGRITY CHECK VALUE field contains an integrity check value (see 3.1.65).

The CbCS capability descriptor and the INTEGRITY CHECK VALUE field should be prepared by the secure CDB originator as described in 2.4.3.

The enforcement manager shall validate the CbCS capability descriptor and the INTEGRITY CHECK VALUE field as described in 2.4.4.

6.r RECEIVE CREDENTIAL command

{{All of 6.r is new. Editing markups suspended.}}

{{Numerous changes shown in 08-128r3 are replicated in 6.r without identifying annotations.}}

6.r.1 RECEIVE CREDENTIAL command description

6.r.1.1 Overview

The RECEIVE CREDENTIAL command (see table x3) allows a secure CDB originator (see 5.13.6.2) to receive a credential from a security manager device server (e.g., a CbCS management device server (see 5.13.6.8.3)) for use in a CDB (e.g., use in the CbCS extension descriptor (see 3.1.a)).

Table x3 — RECEIVE CREDENTIAL command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (7Fh)							
1	CONTROL							
2	Reserved							
6								
7	ADDITIONAL CDB LENGTH (n-7)							
8	(MSB)			SERVICE ACTION (1800h)				
9								(LSB)
10	(MSB)			ALLOCATION LENGTH				
11								(LSB)
12	Restricted (see RFC 4306)							
15								
16	(MSB)			AC_SAI				
19								(LSB)
20	Restricted (see RFC 4306)							
23								
24	(MSB)			DS_SAI				
27								(LSB)
28	(MSB)			CREDENTIAL REQUEST TYPE				
29								(LSB)
30	CREDENTIAL REQUEST DESCRIPTOR							
n								

The ALLOCATION LENGTH field is defined in 4.3.5.6.

The AC_SAI field contains the value of the AC_SAI SA parameter (see 5.13.2.2) for the SA to be used to encrypt the parameter data as described in 6.r.2.1.

The DS_SAI field contains the value of the DS_SAI SA parameter (see 5.13.2.2) for the SA to be used to encrypt the parameter data as described in 6.r.2.1.

If the device server is not maintaining an SA with an AC_SAI SA parameter that matches the AC_SAI field contents and a DS_SAI SA parameter that matches the DS_SAI field contents, then 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.

If the device server is maintaining the SA specified by the AC_SAI field and the DS_SAI field, then the SA shall be verified for use by this RECEIVE CREDENTIAL command as follows:

a) The USAGE_TYPE SA parameter (see 5.13.2.2) shall be verified to be equal to 82h (i.e., CbCS authentication and credential encryption; and
b) The USAGE_DATA SA parameter (see 5.13.2.2) shall be verified not to contain an ALGORITHM IDENTIFIER field (see 7.6.3.6) that is set to ENCR_NULL based on the contents the IKEv2-SCSI SAUT Cryptographic Algorithm descriptor (see 7.6.3.6) for the ENCR algorithm type during creation of the SA (see 5.13.2.3).

If any of these SA verifications fails, 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.

{{The current RECEIVE CREDENTIAL command structure has no mechanism for verifying that the source of the RECEIVE CREDENTIAL command has any knowledge of the shared keys in the specified SA. If source does not know the shared keys, it will not be able to decrypt the parameter data. However, there might be some type of guessing attack wherein knowledge of the shared keys is not required to obtain useful information from a RECEIVE CREDENTIAL command. If such an attack is possible, it will be necessary to have the source of the RECEIVE CREDENTIAL command compute some kind of integrity check value using the shared keys in the SA and place the computed ICV in the CDB.}}

The CREDENTIAL REQUEST TYPE field (see table x4) specifies type of credential being requested and the format of the CREDENTIAL REQUEST DESCRIPTOR field.

Table x4 — CREDENTIAL REQUEST TYPE field

Code	Description	Reference
0001h	CbCS logical unit	6.r.1.2
0002h	CbCS logical unit and volume	6.r.1.3
all other codes	Reserved	

{{A row in this table might define a range of codes as restricted to OSD, but first the interests of the SNIA OSD TWG must be assessed.}}

If return of the requested credential is not permitted, the command shall be terminated with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to ACCESS DENIED - NO ACCESS RIGHTS.

6.r.1.2 CbCS logical unit credential request descriptor

If the credential request type field is set to 0001h (i.e., CbCS logical unit), then the format of the CREDENTIAL REQUEST DESCRIPTOR field is as shown in table x5.

Table x5 — CbCS logical unit credential request descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	DESIGNATION DESCRIPTOR							
19								

The format of the DESIGNATION DESCRIPTOR field is defined in table 436 (see 7.7.3.1). 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 if any of the fields in the DESIGNATION DESCRIPTOR field are set as follows:

a) The DESIGNATOR TYPE field contains any value other than 3h (i.e., NAA);
b) The ASSOCIATION field contains any value other than 00b (i.e., logical unit) or 10b (i.e., SCSI target device); or
c) The DESIGNATOR LENGTH field is set to a value that is larger than 16.

6.r.1.3 CbCS logical unit and volume credential request descriptor

If the credential request type field is set to 0002h (i.e., CbCS logical unit and volume), then the format of the CREDENTIAL REQUEST DESCRIPTOR field is as shown in table x6.

Table x6 — CbCS logical unit and volume credential request descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	DESIGNATION DESCRIPTOR							
19								
20	MAM ATTRIBUTE							
56								

The format of the DESIGNATION DESCRIPTOR field is defined in table 436 (see 7.7.3.1). 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 if any of the fields in the DESIGNATION DESCRIPTOR field are set as follows:

a) The DESIGNATOR TYPE field contains any value other than 3h (i.e., NAA);
b) The ASSOCIATION field contains any value other than 00b (i.e., logical unit) or 10b (i.e., SCSI target device); or
c) The DESIGNATOR LENGTH field is set to a value that is larger than 16.

The format of the MAM ATTRIBUTE field is defined in table 313 (see 7.3.1). If the ATTRIBUTE IDENTIFIER field in the MAM ATTRIBUTE field contains any value other than 0401h (i.e., MEDIUM SERIAL NUMBER), 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.

6.r.2 RECEIVE CREDENTIAL parameter data

6.r.2.1 RECEIVE CREDENTIAL parameter data encryption

The RECEIVE CREDENTIAL parameter data shall be one of the ESP-SCSI data-in buffer descriptors shown in table 66 (see 5.13.7.5.1). The SA specified by the AC_SAI field and the DS_SAI field in the CDB shall be used to construct the ESP-SCSI data-in buffer descriptor as described in 7.6.4.5.

Before processing the parameter data, the application client should validate and decrypt the ESP-SCSI data-in buffer descriptor as described in 7.6.4.5. If any errors are detected by the validation and decryption processing, the parameter data should be ignored.

6.r.2.2 RECEIVE CREDENTIAL decrypted parameter data

Before encryption and after decryption, the UNENCRYPTED BYTES field (see 5.13.7.3) that are used to compute the ENCRYPTED OR AUTHENTICATED DATA field (see 5.13.7.5) contents shall contain a CbCS credential descriptor (see table x7).

Table x7 — CbCS credential descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved				CREDENTIAL FORMAT (1h)			
1	Reserved							
2	(MSB)			CREDENTIAL LENGTH (n-3)				
3								(LSB)
4	(MSB)			CAPABILITY LENGTH (k-5)				
5								(LSB)
6				CbCS capability descriptor				
k								
k+1	(MSB)			CAPABILITY KEY LENGTH (n-(k+4))				
k+4								(LSB)
k+5				CAPABILITY KEY				
n								

{{The CR PRSNT bit defined in 07-454r5 has been removed in this proposal because it is redundant with the length information in the ESP-SCSI descriptor.}}

The CREDENTIAL FORMAT field (see table x8) indicates the format of the credential.

Table x8 — Credential format values

Value	Description
0h	Reserved
1h	The format defined by this standard
2h - Fh	Reserved

{{Because the capability format is not in the capability descriptor, the information it contains is not available in the CbCS extension descriptor. This requires the enforcement manager to use the XCDB extension descriptor EXTENSION TYPE field as the indicator of capability format.}}

The CREDENTIAL LENGTH field indicates the number of bytes that follow in the credential including the capability length, the CbCS capability descriptor, the capability key length, and the capability key.

The CAPABILITY LENGTH field indicates the number of bytes that follow in the capability.

The contents of the CbCS capability descriptor are defined in 6.19.2.3.

The CAPABILITY KEY LENGTH field indicates the number of bytes that follow in the capability key.

The CAPABILITY KEY field contains an integrity check value (see 3.1.65) that the device server computes as described in 5.13.6.8.? and the application client uses as described in 5.13.6.8.? to prepare CbCS extension descriptors.

6.r.2.3 CbCS capability descriptor

A CbCS capability descriptor (see table x9) specifies the commands that are allowed by the CbCS extension descriptor in which it appears.

Table x9 — CbCS capability descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	DESIGNATION TYPE				KEY VERSION			
1	CBCS METHOD							
2	(MSB)			INTEGRITY CHECK VALUE ALGORITHM				
5								(LSB)
6	(MSB)			CAPABILITY EXPIRATION TIME				
11								(LSB)
12				PERMISSIONS BIT MASK				
15								
16	(MSB)			POLICY ACCESS TAG				
19								(LSB)
20				DESIGNATION DESCRIPTOR				
55								
56				DISCRIMINATOR				
71								

{{The designation descriptor field is one byte too short. It is 36 bytes and it needs to be 37 to accomodate a MAM attribute.}}

The DESIGNATION TYPE field (see table x10) specifies the format of the Designation descriptor.

Table x10 — DESIGNATION TYPE field

Code	Description	DESIGNATION DESCRIPTOR field format
0h	Reserved	
1h	Logical unit designation descriptor	See 7.7.3.2.1 and 7.7.3.2.2
2h	MAM attribute designation descriptor	See table 310 in 7.3.1
3h - Fh	Reserved	

The KEY VERSION field specifies which shared key, from the set of CbCS working keys, is being used to compute the capability key and other integrity check values for this CbCS capability.

The CBCS METHOD field (see table x10) specifies the CbCS method used by this CbCS capability.

Table x11 — CBCS METHOD field

Code	CbCS method	Reference
00h	BASIC	5.13.8...
01h	CAPKEY	5.13.8...
02h - EFh	Reserved	
F0h - FEh	Vendor specific	
FFh	Reserved	

The INTEGRITY CHECK VALUE ALGORITHM field specifies the algorithm used to compute the capkey and other integrity check values for this CbCS capability. The value in the INTEGRITY CHECK VALUE ALGORITHM field is selected from the codes that table 71 (see 5.13.8) lists as integrity checking (i.e., AUTH) algorithms, except for AUTH_COMBINED.

The CAPABILITY EXPIRATION TIME field specifies expiration time of this CbCS capability as the number of milliseconds that have elapsed since midnight, 1 January 1970 UT. If the CAPABILITY EXPIRATION TIME field is set to zero, this CbCS capability does not have an expiration time.

The PERMISSIONS BIT MASK field (see table x12) specifies the permissions allowed by this CbCS capability. More than one permissions bit may be set. The relationship between commands and bits in the PERMISSIONS BIT MASK field is defined in for the commands defined by this standard and in the command standard (see 3.1.19) that defines commands for a specific device type.

Table x12 — PERMISSIONS BIT MASK field format

Bit / Byte	7	6	5	4	3	2	1	0
0	DATA READ	DATA WRITE	PARM READ	PARM WRITE	SEC MGMT	RESRV	MGMT	PHY ACC
1	Reserved							
2								
3	Restricted (see applicable command standard)							

A DATA READ bit set to zero indicates a command has no read permission for user data and protection information. A DATA READ bit set to one indicates a command has permission to read user data and protection information.

A DATA WRITE bit set to zero indicates a command has no write permission for user data and protection information. A DATA WRITE bit set to one indicates a command has permission to write user data and protection information.

A parameter data read (PARM READ) bit set to zero indicates a command has no parameter data read permission. A PARM READ bit set to one indicates a command has permission to read parameter data.

A parameter data write (PARM WRITE) bit set to zero indicates a command has no parameter data write permission. A PARM WRITE bit set to one indicates a command has permission to write parameter data.

A security management (SEC MGMT) bit set to zero indicates a command has no security management permission. A SEC MGMT bit set to one indicates a command has security management permission.

A reservation (RESRV) bit set to zero indicates a command has no persistent reservation permission. A RESRV bit set to one indicates a has permission to make or modify persistent reservations.

A management (MGMT) bit set to zero indicates a command has no storage management permission. A MGMT bit set to one indicates a command has storage management permission. Storage management is outside the scope of this standard.

A physical access (PHY ACC) bit set to zero indicates a command has no permission to affect physical access to the logical unit or volume. A PHY ACC bit set to one indicates a command has permission to affect physical access to the logical unit or volume (see SSC-3).

If the POLICY ACCESS TAG field contains a value other than zero, the policy access tag attribute of the logical unit (see 5.13.6.8.10) is compared to the POLICY ACCESS TAG field contents as part of validating the CbCS capability (see 5.13.6.8.8). If the POLICY ACCESS TAG field contains zero, then no comparison is made.

The DESIGNATION DESCRIPTOR field is used during the validation of the CbCS capability (see 5.13.6.8.8) to ensure that the command is being addressed to the correct logical unit or volume (see SSC-3). The format of the DESIGNATION DESCRIPTOR field is defined by the value in the DESIGNATION TYPE field as described in table x10. The DESIGNATION DESCRIPTOR field is limited to 36 bytes in length.

If the CREDENTIAL REQUEST TYPE field in a RECEIVE CREDENTIAL command is set to 0001h (i.e., CbCS logical unit), then the DESIGNATION DESCRIPTOR field shall contain a logical unit designation descriptor that matches the DESIGNATION DESCRIPTOR field (see 6.r.1.2) in the CREDENTIAL REQUEST DESCRIPTOR field in the CDB. If the CREDENTIAL REQUEST TYPE field in a RECEIVE CREDENTIAL command is set to 0002h (i.e., CbCS logical unit and volume), then the DESIGNATION DESCRIPTOR field shall contain a MAM attribute designation descriptor that matches the MAM ATTRIBUTE field (see 6.r.1.3) in the CREDENTIAL REQUEST DESCRIPTOR field in the CDB.

The DISCRIMINATOR field provides uniqueness to the CbCS capability (see 5.13.6.8.?).

The enforcement manager (see 5.13.6.8.7) shall validate each CbCS capability it receives as described in 5.13.6.8.8.

…

7.6.c CbCS security protocol

{{All of 7.6.c is new. Editing markups suspended.}}

{{Changes related to the INC_512 bit are shown in 08-141r0 are replicated in 7.6.c without identifying annotations.}}

7.6.c.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.c.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.c.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.c.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 x13) specifies the CbCS page to be returned in the parameter data (see 7.6.c.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 x13.

Table x13 — 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.c.3.1
0001h	Supported CbCS SECURITY PROTOCOL OUT pages	Mandatory	7.6.c.3.2
0002h – 000Fh	Reserved		
0010h	Capabilities	Mandatory	7.6.c.3.3
0011h	Attributes	Mandatory	7.6.c.3.4
0012h	Reserved		
0013h	Set Master Key – Seed Exchange	Mandatory	7.6.c.3.5
0014h – FFFFh	Reserved		

{{Code assignments in table x13 have been modified to align them with code assignments in table x14.}}

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.c.3 CbCS SECURITY PROTOCOL IN parameter data

7.6.c.3.1 Supported CbCS SECURITY PROTOCOL IN pages CbCS page

7.6.c.3.2 Supported CbCS SECURITY PROTOCOL OUT pages CbCS page

7.6.c.3.3 Capabilities CbCS page

7.6.c.3.4 Attributes CbCS page

7.6.c.3.5 Set Master Key – Seed Exchange CbCS page

7.6.c.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 x14) specifies the CbCS page to be returned in the parameter data (see 7.6.c.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 x14.

Table x14 — 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.c.5.1
0012h	Set Key	Mandatory	7.6.c.5.2
0013h	Set Master Key – Seed Exchange	Mandatory	7.6.c.5.3
0014h	Set Master Key – Change Master Key	Mandatory	7.6.c.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.c.5 CbCS SECURITY PROTOCOL OUT parameter data

7.6.c.5.1 Set Attributes CbCS page

7.6.c.5.2 Set Key CbCS page

7.6.c.5.3 Set Master Key – Seed Exchange CbCS page

7.6.c.5.4 Set Master Key – Change Master Key CbCS page

…

7.7.4 Extended INQUIRY Data VPD page

The Extended INQUIRY Data VPD page (see table 446) provides the application client with a means to obtain information about the logical unit.

Table 446 — Extended INQUIRY Data VPD page

Bit / Byte	7	6	5	4	3	2	1	0
0	PERIPHERAL QUALIFIER			PERIPHERAL DEVICE TYPE				
1	PAGE CODE (86h)							
2	Reserved							
3	PAGE LENGTH (3Ch)							
4	Reserved		SPT			GRD_CHK	APP_CHK	REF_CHK
5	Reserved		UASK_SUP	GROUP_SUP	PRIOR_SUP	HEADSUP	ORDSUP	SIMPSUP
6	Reserved				WU_SUP	CRD_SUP	NV_SUP	V_SUP
7	Reserved							LUICLR
8	Reserved							CBCS
9 ~~8~~ – 63	Reserved							

…

A capability-based command security (CBCS) bit set to one indicates that the logical unit supports the capability-based command security technique (see 5.13.6.8). A CBCS bit set to zero indicates that the logical unit does not support the capability-based command security technique.

7.7.5 Management Network Addresses VPD page

{{Several *pro forma* changes follow this note. The subclause and table numbering is reset at this point.}}

5.6.1 Persistent Reservations overview

…

For each command, this standard or a command standard (see 3.1.19) defines the conditions that result in RESERVATION CONFLICT. Command standards define the conditions either in the device model or in the descriptions each of specific command.

Table 35 — SPC commands that are allowed in the presence of various reservations

Command	Addressed logical unit has this type of persistent reservation held by another I_T nexus				
	From any I_T nexus		From registered I_T nexus (RR all types)	From not registered I_T nexus	
	Write Excl	Excl Access		Write Excl RR	Excl Access – RR
…	…	…	…	…	…
RECEIVE COPY RESULTS	Conflict	Conflict	Allowed	Conflict	Conflict
RECEIVE CREDENTIAL	Conflict	Conflict	Allowed	Conflict	Conflict
…					

…

6.1 Summary of commands for all device types

The operation codes for commands that apply to all device types when the MCHNGR bit is set to zero, the SCCS bit is set to zero, and the ENCSERV bit is set to zero in the standard INQUIRY data (see 6.4.2) are listed in table 77.

Table 77 — Commands for all device types

Command name	Operation code	Type	Reference
…	…	…	…
RECEIVE COPY RESULTS	84h	O	6.18
RECEIVE CREDENTIAL	7Fh/1800h [a]	O	6.r

Type Key: C = Command implementation is defined in the applicable command standard (see 3.1.19).
M = Command implementation is mandatory.
O = Command implementation is optional.
Z = Command implementation is defined in a previous standard.

[a] This command is defined by a combination of operation code and service action. The operation code value is shown preceding the slash and the service action value is shown after the slash.

…

6.30 SECURITY PROTOCOL IN command

…

The SECURITY PROTOCOL field (see table 229) specifies which security protocol is being used.

Table 229 — SECURITY PROTOCOL field in SECURITY PROTOCOL IN command

Code	Description	Reference
00h	Security protocol information	7.6.1
01h - 06h	Defined by the TCG	3.1.169
07h	CbCS	7.6.c
~~07h~~ 08h - 1Fh	Reserved	
20h	Tape Data Encryption	SSC-3
21h	Data Encryption Configuration	TBD
22h - 3Fh	Reserved	
40h	SA Creation Capabilities	7.6.2
41h	IKEv2-SCSI	7.6.3
42h - ECh	Reserved	
EDh	SD Card TrustedFlash specification	3.1.137
EEh	Authentication in Host Attachments of Transient Storage Devices	IEEE 1667
EFh	ATA Device Server Password Security	SAT-2
F0h - FFh	Vendor Specific	

…

6.31 SECURITY PROTOCOL OUT command

…

The SECURITY PROTOCOL field (see table 230) specifies which security protocol is being used.

Table 230 — SECURITY PROTOCOL field in SECURITY PROTOCOL OUT command

Code	Description	Reference
00h	Reserved	
01h - 06h	Defined by the TCG	3.1.169
07h	CbCS	7.6.c
~~07h~~ 08h - 1Fh	Reserved	
20h	Tape Data Encryption	SSC-3
21h	Data Encryption Configuration	TBD
22h - 40h	Reserved	
41h	IKEv2-SCSI	7.6.3
42h - ECh	Reserved	
EDh	SD Card TrustedFlash specification	3.1.137
EEh	Authentication in Host Attachments of Transient Storage Devices	IEEE 1667
EFh	ATA Device Server Password Security	SAT-2
F0h - FFh	Vendor Specific	

…

D.3.5 Variable length CDB service action codes

The variable length CDB service action codes assigned by this standard are shown in table D.8.

Table D.8 — Variable Length CDB Service Action Codes Used by All Device Types

Service Action Code	Description
1800h	RECEIVE CREDENTIAL command
1801h - 1FFFh	Reserved
~~1800h - 1FFFh~~	~~Reserved~~