ENDL
TEXAS

Date: 10 March 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: SPC-4 RECEIVE CREDENTIAL command 'adjustments'

Introduction

I failed to study 07-454r5 closely enough during the CAP review process. Now, I must pay the price.

Many things need to be fixed:

- The usage of SAs is not at all as intended.
- There is too much dependence on a specific I_T Nexus for SA usage.
- Credentials can apply to target ports, which is count to the CbCS model.
- No additional sense code is specified for use when the requested credential is prohibited by the policy database.

Also, the RECEIVE CREDENTIAL command could be useful in OSD. So, the parameter data format and tiny bits of the description need to be restructured to accommodate this.

Revision History

r0 Initial revision
r1 Revised as requested by Sivan Tal in a message posted to the T10 reflector
r2 Revised as requested by Sivan Tal in additional messages posted to the T10 reflector

Differences between r0 and r2 are indicated by change bars.

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

Some text has been moved to a new subclause. Unmodified but moved text is shown in black. Removed/moved text is shown in ~~gray strikethrough~~.

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

Proposed Changes in SPC-4 r13

6.19 RECEIVE CREDENTIAL command

6.19.1 RECEIVE CREDENTIAL command description

6.19.1.1 Overview

The RECEIVE CREDENTIAL command (see table 178) allows a secure CDB originator (see 5.13.6.2) to receive a ~~CbCS~~ 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 3.1.19)).

Table 178 — 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 ~~18h or 3Dh~~)							
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								
~~12~~	~~DESIGNATION DESCRIPTOR~~							
~~31~~								
~~32~~	~~MAM ATTRIBUTE~~							
~~68~~								

~~A RECEIVE CREDENTIAL command shall be terminated with CHECK CONDITION status, the sense key set to NOT READY, and the additional sense code set to LOGICAL UNIT NOT READY, SECURITY INITIALIZATION REQUIRED if it is received before a SECURITY PROTOCOL IN command has completed successfully on the same I_T_L nexus as the RECEIVE CREDENTIAL command was received with the following field settings:~~

~~a) The SECURITY PROTOCOL field set to 41h (i.e., IKEv2-SCSI); and~~
~~b) The SECURITY PROTOCOL SPECIFIC field set to 0103h (i.e., Authentication step).~~

~~Editors Note 1 - ROW: LOGICAL UNIT NOT READY, SECURITY INITIALIZATION REQUIRED is an additional sense code for which no code value has been assigned. This is because document 08-128 eliminates its use.~~

~~If before a SECURITY PROTOCOL IN command has completed successfully on the same I_T_L nexus as the RECEIVE CREDENTIAL command was received with the following field settings:~~

~~a) The SECURITY PROTOCOL field set to 41h (i.e., IKEv2-SCSI);~~
~~b) The SECURITY PROTOCOL SPECIFIC field set to 0102h (i.e., Key Exchange step); and~~
~~c) The SCSI Cryptographic Algorithms payload contains a cryptographic algorithm descriptor of type Encryption Algorithm (ENCR) (i.e., ALGORITHM TYPE 01h) and an identifier other than ENCR_NULL (i.e., ALGORITHM IDENTIFIER other than 8001 000Bh),~~

~~then the command shall be terminated with a CHECK CONDITION status, the sense key set to NOT READY, and the additional sense code set to LOGICAL UNIT NOT READY, SECURITY INITIALIZATION REQUIRED.~~

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 6.19.2.1.

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 6.19.2.1.

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 x1) specifies type of credential being requested and the format of the CREDENTIAL REQUEST DESCRIPTOR field.

Table x1 — CREDENTIAL REQUEST TYPE field

Code	Description	Reference
0001h	CbCS logical unit	6.19.1.2
0002h	CbCS logical unit and volume	6.19.1.3
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.}}

~~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 following are true:~~

~~a) The DESIGNATOR TYPE field contains any value other than 3h (i.e., NAA); or~~
~~b) The DESIGNATOR LENGTH field is set to a value that is larger than 20.~~

~~The MAM ATTRIBUTE field is optional. The format of the MAM ATTRIBUTE field is specified in table 313 (see 7.3.1). If the MAM ATTRIBUTE field is present and 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.~~

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.

6.19.1.2 CbCS logical unit credential request descriptor

If the credential request type field is set to 0001h (i.e., CbCS logical unit), then the ~~The~~ format of the CREDENTIAL REQUEST DESCRIPTOR ~~DESIGNATION DESCRIPTOR~~ field is as shown in table x2.

Table x2 — 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 ~~following are true~~:

a) The DESIGNATOR TYPE field contains any value other than 3h (i.e., NAA); ~~or~~
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 ~~20~~ 16.

{{If the ASSOCIATION field requirement is not added CbCS could apply to target ports. This would necessitate numerous changes in the CbCS model (e.g., the capabilities overview subclause.}}

{{07-454r5 specified a total DESIGNATION DESCRIPTOR field length of 24 bytes. An editorial change was made to base the test on the DESIGNATOR LENGTH field in the designation descriptor. Since there is a 4-byte header in a designation descriptor, the length was editorially reduced to 20 bytes. However, neither of these match the 20 bytes defined for the designation descriptor field in table 178. Therefore, the additional length reduction to 16 bytes is necessary. No NAA designation descriptor has a length value larger than 16.}}

6.19.1.3 CbCS logical unit and volume credential request descriptor

~~The MAM ATTRIBUTE field is optional.~~ If the credential request type field is set to 0002h (i.e., CbCS logical unit and volume), then the ~~The~~ format of the CREDENTIAL REQUEST DESCRIPTOR ~~MAM ATTRIBUTE~~ field is as shown in table x3.

Table x3 — 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 ~~specified~~ in table 313 (see 7.3.1). If ~~the MAM ATTRIBUTE field is present and~~ 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.

6.19.2 RECEIVE CREDENTIAL parameter data

6.19.2.1 RECEIVE CREDENTIAL parameter data encryption

The RECEIVE CREDENTIAL parameter data shall be one of the ESP-SCSI data-in buffer descriptors shown in table 438 (see 7.6.4.5.1). 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. ~~that has been authenticated and~~

~~encrypted in accordance with an SA that has been created in the device server (see 5.13.2). The SA shall use an encryption algorithm other than ENCR_NULL and a usage type of CbCS Credential Authentication and Encryption (see table 45. See 5 in this document).~~

{{ENCR_NULL test moved to CDB definition.}}

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.

6.19.2.2 RECEIVE CREDENTIAL decrypted parameter data

Before encryption and after decryption, the UNENCRYPTED BYTES field (see 7.6.4.3) that are used to compute the ENCRYPTED OR AUTHENTICATED DATA field (see 7.6.4.5) contents shall contain a CbCS credential descriptor (see table 179).

Table 179 — CbCS credential descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
0	~~CR PRSNT~~	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								

~~If the credential present (CR PRSNT) bit is set to zero, no CbCS credential descriptor shall be returned. If the CR PRSNT bit is set to one, a CbCS credential is returned in the parameter data.~~

{{Since the credential descriptor is wrapped in an ESP-SCSI description that contains a length value, the CR PRSNT bit is redundant.}}

The CREDENTIAL FORMAT field (see table 180) indicates the format of the credential.

Table 180 — 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.

6.19.2.3 CbCS capability descriptor

…

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 190. 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 6.19.1.2) 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 6.19.1.3) in the CREDENTIAL REQUEST DESCRIPTOR field in the CDB.