Date: November 1, 2000
To: T10 Committee (SCSI)
From: Jim Hafner (IBM) (hafner@almaden.ibm.com)

Subject: Three minor modifications to Access Controls in SPC-3

ABSTRACT:

This document proposes three changes to the Access Controls model/specification in SPC-3 (as defined in 99-245r9 and amended by 00-261r0 and 00-287r1 and approved in May, July and October 2000, respectively). None of the three affect the semantics of the protocol. The first two make room for some vendor-specific functions. The third clarifies some wording in the context of the EXTENDED COPY command. This proposal can be approved in whole or each part separately.

AUTHOR'S NOTE: *cross-references to specific clauses here are to 99-245r9 unless otherwise qualified. They are hard-coded and would need careful editing when incorporated into a complete document*.

1.0 Vendor-specific Page Code ranges

Table 6 and Table 26 define the one byte ACL Entry Page Codes for the REPORT ACL and MANAGE ACL service actions respectively. Currently, all undefined codes are reserved. This proposal requests that byte codes F0h-FFh be specified as Vendor-specific. The revised tables are:

TABLE 6: ACL Entry PAGE CODE definitions for REPORT ACL service action.

Page Code	Description	Clause
00h	Granted	5.2.2.2.2
01h	Granted All	5.2.2.2.2
02h	Proxy Tokens	5.2.2.2.3
03h-EFh	Reserved	
F0h-FFh	Vendor-specific	

TABLE 26: ACL Entry PAGE CODE definitions for MANAGE ACL service action.

Page Code	Description	Clause
00h	Grant/Revoke	6.2.2.2.2
01h	Grant All	6.2.2.2.2
02h	Revoke Proxy Token	6.2.2.2.3
03h	Revoke All Proxy Tokens	6.2.2.2.3
04h-EFh	Reserved	
F0h-FFh	Vendor-specific	

2.0 LUN/default LUN List in Granted ACL Entry Page (REPORT ACL) and Grant/ Revoke ACL Entry Page (MANAGE ACL)

In order to make additional room for vendor-specific functions, this proposal makes two changes to the format of the Granted ACL Entry Page of the REPORT ACL service action and parallel changes to the Grant/Revoke ACL Entry Page of the MANAGE ACL service action and the Proxy Tokens ACL Entry Page format of the REPORT ACL service action. In short, the proposal requests that the LUN/DEFAULT LUN List as defined in Table 8 be modified to include a four (4) byte prefix to each LUN/DEFAULT LUN pair. Adiitionally, the proposal requests that one byte (byte 0) be designated as the ACCESS MODE field. The value zero for this field would mean normal access. The values in the range F0h-FFh would be set apart as vendor-specific and all other values would be reserved. The PROXY TOKENS/DEFAULT LUN list should be changed to add a four byte reserved header on each proxy token/default LUN pair. Additionally, this proposal fixes some minor editorial issues and clarifies the existing wording. These proposed changes have no effect on the semantics of the defined commands and service actions. The only effect is in the implementation of the functions for construction and parsing of the parameter list.

The following subclauses provide the details for these changes.

2.1 Revisions to clause 5.2.2.2.2 “REPORT ACL parameter data Granted and Granted All page formats”

Table 8 should be replaced by the following table and additional text.

.

Table 8. LUN/DEFAULT LUN LIST format

	Bit							
Byte	7	6	5	4	3	2	1	0
0	ACCESS MODE							
1 3	RESERVED							
4 11	MSB	FIRST LUN						LSB
12 19	MSB	FIRST DEFAULT LUN						LSB
		. . .						
n-19	ACCESS MODE							
n-18 *n*-16	RESERVED							
n-15 *n*-8	MSB	LAST LUN						LSB
n-7 *n*	MSB	LAST DEFAULT LUN						LSB

In each block, the value in the ACCESS MODE field shall indicate the type of access that the specified initiator has to the logical unit referenced by the DEFAULT LUN value and addressible at the specified LUN value. The value 0h for ACCESS MODE shall mean normal access. The meaning of the values F0h-FFh are vendor-specific. The values 01h-EFh are reserved.

2.2 Revisions to clause 6.2.2.2.2 “MANAGE ACL parameter data Grant/Revoke and Grant All page formats”

The following proposed text is extracted from 99-245r9 and edited here with change bars. This is mostly editorial in nature, subject to the changes specified in the preceding clause. All other text in that clause should remain unchanged.

The Grant/Revoke and Grant All page formats for the MANAGE ACL service action is given in Table .

Table 27 Grant/Revoke and Grant All page formats

Byte	Bit							
	7	6	5	4	3	2	1	0
0	PAGE CODE (`00h-01h`)							
1	RESERVED							
2								
3	PAGE LENGTH (*m*-3)							
4	NOCNCL	RESERVED						
5	IDENTIFIER TYPE							
6								
7	IDENTIFIER LENGTH (*n*-7)							
8	MSB							
n	ACCESS IDENTIFIER							LSB
n+1								
m	LUN/DEFAULT LUN LIST							

The IDENTIFIER TYPE and ACCESS IDENTIFIER fields are described in 7.1. The IDENTIFIER LENGTH field indicates the number of bytes following taken up by the ACCESS IDENTIFIER field.

NOTE All currently defined Identifier Types require the IDENTIFIER LENGTH field be set to 24 (see Table 33).

The PAGE LENGTH field shall indicate the number of additional bytes required for this page.

For the Grant/Revoke page, the LUN/DEFAULT LUN LIST field shall contain a (possibly empty) set of LUN/default LUN pairs as specified in Table 8. If an ACCESS MODE value occurs that is not supported or if any default LUN value is not valid at the access controls coordinator or any LUN value cannot be supported as a valid LUN address, the device server shall fail the command with CHECK CONDITION status, sense key set to ILLEGAL REQUEST and additional sense code set to ACCESS DENIED - INVALID LU IDENTIFIER. The sense data shall be modified as follows. The SENSE-KEY SPECIFIC bit shall be set as described in 7.22.1 (of SPC-2, revision 16) with the FIELD POINTER field indicating the first byte of the invalid field (as counted within the full parameter data). If the error is caused by an unsupported LUN value, the next eight bytes (if available) beyond the last byte of the FIELD POINTER may include a LUN value that the access controls coordinator would support for the logical unit referenced by the paired default LUN.

A Grant/Revoke page with a non-empty LUN/DEFAULT LUN LIST instructs the access controls coordinator to add a new or to replace an existing ACL entry for the specified access identifier. The accessible logical unit pairs of this ACL entry shall be derived from the LUN/DEFAULT LUN LIST as follows. Each accessible logical unit pair shall take its LUN value from a LUN/default LUN pair and its logical unit reference shall refer to the logical unit corresponding to the default LUN value. The access rights to that logical unit shall be as specified by the Access Mode value as described in 5.2.2.2.2.

A Grant/Revoke page with an empty LUN/DEFAULT LUN LIST instructs the access controls coordinator to remove an existing ACL entry for the specified access identifier. It is not an error condition if no such entry exists.

The Grant All page shall contain an empty LUN/DEFAULT LUN LIST field. That is, there shall be no data in this page after the last byte of the ACCESS IDENTIFIER field.

The Grant All page instructs the access controls coordinator to add a new or replace an existing ACL entry for the specified access identifier. The Grant All page shall be processed to have the same effect as a Grant/Revoke page containing the same access identifier and a complete list of LUN/default LUN pairs (with LUN equal to the default LUN in each pair and with ACCESS MODE set to 0h, normal access) for all logical units.

2.3 Revisions to clause 5.2.2.2.3 “REPORT ACL parameter data Proxy Tokens page format”

Table 10 should be replaced by the following table.

Table 10. PROXY TOKEN/DEFAULT LUN LIST format

	Bit							
Byte	7	6	5	4	3	2	1	0
0 3	RESERVED							
4 11	MSB	FIRST PROXY TOKEN						LSB
12 19	MSB	FIRST DEFAULT LUN						LSB
		. . .						
n-19 *n*-16	RESERVED							
n-15 *n*-8	MSB	LAST PROXY TOKEN						LSB
n-7 *n*	MSB	LAST DEFAULT LUN						LSB

3.0 Additional clarify text in Appendix D2 for EXTENDED COPY command

The paragraph that begins “If the LU ID Type” field indicates Proxy Token...” contains the following additional text:

> “The copy manager shall send to the LUN assigned on the basis of this Proxy Token only those commands that are necessary for the completion of those EXTENDED COPY commands that contain this Proxy Token value in their target descriptors.”

This text does not specify conditions when the copy manager might be requested to perform these “forbidden” commands, nor does it specify the error response. To clarify and complete, this proposal requests the following additional paragraph be added immedidately after the aforementoined paragraph

> If the copy manager receives a target descriptor that specifies a logical unit either by LUN or by logical unit identifier and the copy manager has access to that logical only under the rights of one or more Proxy Tokens, it shall reject the command with CHECK CONDITION status, sense key set to COPY ABORTED and the additional sense code set to COPY TARGET DEVICE NOT REACHABLE.