

ENDL TEXAS

Date: 4 September 2001
 To: T10 Technical Committee
 From: Ralph O. Weber & Jim Hafner
 Subject: Access Controls for SPC-3 (the rewrite)

A – Introduction

The access controls proposal has been modified by several additional documents, producing the following list of proposals all related to access controls:

99-245r9 A Detailed Proposal For Access Controls
 00-261r0 Discussion of editorial changes to Access Controls in 99-245r9
 00-287r1 TransportIDs for Access Controls
 00-381r0 Three minor modifications to Access Controls in SPC-3
 01-026r1 SPC-3 Access Controls LUN conflicts due to transport IDs

In addition, past experience with complex proposals such as persistent reservations suggests that a rewrite of the original proposal by someone with T10 editing experience will occur sooner or later. *Why not sooner?*

This proposal intends to make no technical changes to the approved access controls proposals listed above. However, some omissions have been discovered during the rewrite process and statements have been added that may constitute requirements not previously noted explicitly. The author believes that the original intent has been maintained throughout.

Familiarity with the access controls concepts is assumed. This proposal contains almost none of the explanatory text found in the proposals listed above and reference is made to those proposals for the historical perspective.

It is anticipated that a few revisions will be needed before this proposal can be approved. While that work is in progress, it is recommended that incorporation of the proposals listed above be deferred in SPC-3. Once completed, this proposal should replace all of them.

A.1 – Changes from previous revisions

r1 All the words of the proposal are the same as in r0 with a few changes to increase readability (while decreasing exposition of changes). Text that r0 shows as being removed either by strikeout or by yellow text is not present in r1. Text that r0 shows in green because it has been moved is in blue in r1. Note: r1 contains what appear to be extraneous spaces caused by the r0 conditional text that is no longer being displayed. These will be cleaned up in r2 if the working group approves removal of the conditional text.

B – Notations Used

Editorial additions and sites where text has moved from one place to another are indicated with blue text. Red text that is double underlined indicates where new statements have been added that the author believes are statements of previously unstated requirements.

C – Issues to Work

C.1 – FCP-2 Glossary

The glossary entries as added in FCP-2 rev 7 for access controls are not exactly as given here. They are:

access controls: Mechanisms allowing a managing application client to control the set of initiators that have access to a target. The access control is enforced by the target. See SPC-3.

access controls data: Information sent to the target by the managing application client that is used by the target to control the set of initiators that have access to the target. See SPC-3.

access controls enrollment state: A state established in the target by the managing application client. This state governs the behavior of the target in controlling the set of initiators that have access to the target. See SPC-3.

D – Significant Changes to the Approved Access Controls Proposal

In the course of preparing this rewrite of the access controls proposal, a couple of issues have surfaced that I think should be considered as significant changes to the proposal:

- a) I LUN 0 access model described in the approved proposal should be removed in favor of accessing the access controls coordinator via a well known logical unit. The effects of this change are:
 - A) The access controls model, commands, and data go in clauses separate from the 'all device types' clauses
 - B) The access controls coordinator will need its own list of supported commands, probably only INQUIRY, ACCESS CONTROL IN, and ACCESS CONTROL OUT;
 - C) Discussion on LUN 0 usage is removed from the ACCESS CONTROL IN and ACCESS CONTROL OUT; and
 - D) The ACC bit in the standard INQUIRY data would be either left reserved or made vendor specific based on the status of existing implementations; also
- b) I believe that a new unit attention condition needs to be defined into which all logical units in a SCSI target device are placed after access controls are disabled. In the absence of such a unit attention condition, initiators may continue operating under obsolete understandings of LUN to logical unit relationships following the disabling of access controls.

E – Summary Information

The following information summarizes proposed code values. It is not directly part of this proposal.

E.1 – Access Control Operation Codes and Service Actions

Table 1 summarizes the service actions for the ACCESS CONTROL IN command (operation code 86h).

Table 1: ACCESS CONTROL IN Service Actions

Code	Name	Type	Clause
00h	REPORT ACL	M	7.1.2
01h	REPORT LU DESCRIPTORS	M	7.1.3
02h	REPORT ACCESS CONTROLS LOG	M	7.1.4
03h	REPORT OVERRIDE LOCKOUT TIMER	M	7.1.5
04h	REQUEST PROXY TOKEN	O	7.1.6
05h-17h	Reserved		
18h-1Fh	Vendor-specific	V	

Table 2 summarizes the service actions for the ACCESS CONTROL OUT command (operation code 87h).

Table 2: ACCESS CONTROL OUT Service Actions

Code	Name	Type	Clause
00h	MANAGE ACL	M	7.2.2
01h	DISABLE ACCESS CONTROLS	M	7.2.3
02h	ACCESS ID ENROLL	M	7.2.4
03h	CANCEL ENROLLMENT	M	7.2.5
04h	CLEAR ACCESS CONTROLS LOG	M	7.2.6
05h	MANAGE OVERRIDE LOCKOUT TIMER	M	7.2.7
06h	OVERRIDE MGMT ID KEY	M	7.2.8
07h	REVOKE PROXY TOKEN	O	7.2.9
08h	REVOKE ALL PROXY TOKENS	O	7.2.10
09h	ASSIGN PROXY LUN	O	7.2.11
0Ah	RELEASE PROXY LUN	O	7.2.12
0Bh-17h	Reserved		
18h-1Fh	Vendor-specific	V	

E.2 – Access Control Additional Sense Codes

Table 3 contains a list of the Additional Sense Code and Additional Sense Code Qualifiers relevant to access controls. Section F.5 formally proposes the addition of these codes.

Table 3: Access Control Additional Sense Codes and Qualifiers

ASC	ASCQ	Description	Description
20h	01h	ACCESS DENIED - INITIATOR PENDING-ENROLLED	An initiator in the pending-enrolled state sends a restricted command to a logical unit accessible under the enrolled AccessID.
20h	02h	ACCESS DENIED - NO ACCESS RIGHTS	An initiator in the not-enrolled state sends an ACCESS ID ENROLL service action and the given AccessID has no access rights in the ACL.
20h	03h	ACCESS DENIED - INVALID MGMT ID KEY	The Management Identifier Key value does not match the value maintained by the access controls coordinator.
20h	08h	ACCESS DENIED - ENROLLMENT CONFLICT	An initiator in the enrolled or pending-enrolled state issues an ACCESS ID ENROLL service action under a different AccessID.
20h	09h	ACCESS DENIED - INVALID LU IDENTIFIER	A LUN or default LUN value in a CDB field or parameter data is not valid.
20h	0Ah	ACCESS DENIED - INVALID PROXY TOKEN	The Proxy Token is not valid; it does not correspond to a logical unit.
20h	0Bh	ACCESS DENIED - ACL CONFLICT	The enrollment failed because an ACL conflict occurred.
55h	05h	INSUFFICIENT ACCESS CONTROL RESOURCES	The access controls coordinator has exhausted its resources for the requested access controls action.

F – Changes Proposed for SPC-3

F.1 – Glossary and Acronyms

The following additions to the glossary and acronyms clause of SPC-3 are proposed.

F.1.1 – Glossary

3.1.r access controls: An optional [SCSI target device](#) feature that restricts initiator access to specific logical units and modifies the information about logical units in the parameter data of INQUIRY and REPORT LUNS commands (see 5.99).

3.1.s access control list (ACL): The data used by a [SCSI target device](#) to configure access rights for initiators according to the access controls state of the [SCSI target device](#) (see 5.99.2).

3.1.t access control list entry (ACE): [One entry in the access control list](#) (see 3.1.s).

3.1.u access controls coordinator: The entity within a [SCSI target device](#) that coordinates the management and enforcement of access controls (see 5.99) for all logical units within the [SCSI target device](#). [The access controls coordinator](#) is always addressable through LUN 0.

3.1.v logical unit access control descriptor (LUACD): [The structure within an ACE](#) (see 3.1.t) that identifies a logical unit to which access is allowed and specifies the LUN by which the logical unit is to be accessed (see 5.99.2.3).

3.1.w proxy token: An identifier for a logical unit that may be used to gain temporary access to that logical unit in the presence of access controls (see 5.99.5.2).

F.1.2 – Acronyms

ACE	Access Control list Entry (see 3.1.t)
ACL	Access Control List (see 3.1.s)
LUACD	Logical Unit Access Control Descriptor (see 3.1.v)
SBC-2	SCSI Block Commands -2 (see clause 1)

F.2 – Access Controls & Reservations

Table 4 shows two lines to be added in SPC-3 for the new commands introduced by access controls. In SPC-3 revision 00, the affected table was table 10.

Table 4: SPC-3 Reservations Conflicts Table Changes for Access Controls

Command	Addressed LU is reserved by another initiator [A]	Addressed LU has this type of persistent reservation held by another initiator [B]				
		From any initiator		From registered initiator (RO all types)	From initiator not registered	
		Write Excl	Excl Access		Write Excl RO	Excl Access – RO
ACCESS CONTROL IN	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
ACCESS CONTROL OUT	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed

F.3 – Changes to the EXTENDED COPY command

In the target descriptor formats in SPC-Tables 17, 19, 20, 21, 22, and 23, change byte3, bits 0-1 to a new 2-bit field called LU ID TYPE. In SPC-Table 19, 20, 21, and 22, change the LOGICAL UNIT NUMBER field name to LU IDENTIFIER.

Add the following paragraphs to clause SPC-7.2.6.1 after the paragraph that begins “The copy manager may,...”:

The LU ID TYPE field (see table 1) specifies the interpretation of the LU IDENTIFIER field in target descriptors that contain a LU IDENTIFIER field .

Table t1 — LU ID type codes

Type Code	LU IDENTIFIER field contents	Reference
00b	Logical Unit Number	SAM-2
01b	Proxy Token	5.99.5.2
10b - 11b	Reserved	

Support for LU ID type codes other than 00b is optional. If a copy manager receives an unsupported LU ID type code , the command shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST.

If the LU ID TYPE field specifies that the LU IDENTIFIER field contains a logical unit number, then the LU IDENTIFIER field specifies the logical unit within the SCSI device specified by other fields in the target descriptor that shall be the source or destination for EXTENDED COPY operations.

If the LU ID TYPE field specifies that the LU IDENTIFIER field contains a proxy token (see 5.99.5.2), then the copy manager shall use the LU IDENTIFIER field contents to obtain proxy access rights to the logical unit associated with the proxy token. The logical unit number that represents the proxy access rights shall be the source or destination for EXTENDED COPY operations.

The copy manager should obtain a LUN value for addressing this logical unit by sending an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action (see 7.2.11) to the access controls coordinator of the SCSI device that is identified by other fields in the target descriptor. The copy manager shall use a LUN assigned

on the basis of a proxy token only for those commands that are necessary for the processing of the EXTENDED COPY command whose parameter data contains the proxy token . When the copy manager has completed EXTENDED COPY commands involving a proxy token, the copy manager should release the LUN value using an ACCESS CONTROL OUT command with RELEASE PROXY LUN service action (see 7.2.12) .

EXTENDED COPY access to proxy logical units is to be accomplished only via LU ID type 01b. If the copy manager receives a target descriptor containing LU ID type 00b and a logical unit number matching a LUN value that the copy manager has obtained using an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action, the EXTENDED COPY command shall be terminated with a CHECK CONDITION status, the sense key shall be set to COPY ABORTED and the additional sense code shall be set to COPY TARGET DEVICE NOT REACHABLE.

In each subclause SPC-7.2.6.2-7.2.6.5, remove the paragraph which starts “The LOGICAL UNIT NUMBER...” and replace it with the following paragraph:

The LU ID TYPE field and LU IDENTIFIER field are described in SPC-7.2.6.1.

In the subclause SPC-7.2.6.6, insert the following paragraph after the paragraph which starts “The contents of...”

The LU ID TYPE field is reserved for this target descriptor.

F.4 – Changes to the Standard INQUIRY Data

In the standard INQUIRY data format, SPC-Table 46, make the following change. Byte 5, bit 6 is changed from Reserved to ACC (for Access Controls Coordinator). The following additional text be added after the paragraph describing the sccs bit in clause SPC-7.3.2:

An Access Controls Coordinator (ACC) bit of one indicates that the device contains an access controls coordinator that may be addressed through this logical unit. An ACC bit of zero indicates that no access controls coordinator is present. If the device contains an access controls coordinator, the ACC bit shall be set to one for LUN 0.

F.5 – New additional sense codes

The following ASC/ASCQ codes should be added and marked as used by all device types:

20h/01h	ACCESS DENIED - INITIATOR PENDING-ENROLLED
20h/02h	ACCESS DENIED - NO ACCESS RIGHTS
20h/03h	ACCESS DENIED - INVALID MGMT ID KEY
20h/08h	ACCESS DENIED - ENROLLMENT CONFLICT
20h/09h	ACCESS DENIED - INVALID LU IDENTIFIER
20h/0Ah	ACCESS DENIED - INVALID PROXY TOKEN
20h/0Bh	ACCESS DENIED - ACL LUN CONFLICT
55h/05h	INSUFFICIENT ACCESS CONTROL RESOURCES

F.6 – Access Controls Model

This is the model clause for addition to SPC-3.

5.99 Access Controls

5.99.1 Access controls overview

Access controls are an optional [SCSI target device](#) feature that application clients may use to [restrict logical unit access to specified initiators or groups of initiators](#) .

Access controls are handled [in the SCSI target device](#) by an access controls coordinator. The access controls coordinator associates a specific LUN to a specific logical unit depending on which initiator accesses the [SCSI target device](#) and whether the initiator has rights to the logical unit.

Access rights to a logical unit affects whether the logical unit appears in the parameter data returned by a REPORT LUNS command and how the logical unit responds to INQUIRY commands.

The [access controls coordinator](#) maintains information about which initiators are allowed access to which logical units via which LUNs in the [access control list \(ACL\)](#), described in 5.99.2. The format of the ACL is vendor specific.

To support third party commands such as [EXTENDED COPY](#), the [access controls coordinator](#) may provide proxy tokens (see 5.99.5.2) to allow one initiator to pass its access capabilities to another initiator.

An application client [manages](#) the access controls state of the [SCSI target device](#) using [the following](#) commands:

- a) [ACCESS CONTROL IN](#) - [to request information or a proxy token from the access controls coordinator](#) ;
and
- b) [ACCESS CONTROL OUT](#)
 - A) [to allow](#) , change or revoke [logical unit](#) access ;
 - B) [to revoke a proxy token](#); and
 - C) otherwise [to manage](#) the access controls coordinator.

A [SCSI device](#) has access controls disabled when it is shipped from the factory and after successful completion of the [ACCESS CONTROL OUT](#) command with [DISABLE ACCESS CONTROLS](#) service action. In this state, the [ACL](#) contains no entries and the management identifier key (see 5.99.7) is zero.

The first successful [ACCESS CONTROL OUT](#) command with [MANAGE ACL](#) service action (see 7.2.2) shall enable access controls. When access controls are enabled, all logical units shall be inaccessible to all initiators unless the [ACL](#) (see 5.99.2) allows access .

The [ACL](#) allows an initiator [access](#) to a logical unit if the [ACL](#) contains an [ACE](#) (see 5.99.2) with an access identifier (see 5.99.2.2) associated with the initiator and that [ACE](#) contains a [LUACD](#) (see 5.99.2.3) that references the logical unit. When the [ACL](#) allows access to a logical unit, the [REPORT LUNS](#) command parameter data bytes representing that logical unit shall contain the LUN value found in the [LUACD](#) that references that logical unit and the initiator shall use the same LUN value when sending commands to the logical unit.

An initiator also may [be allowed](#) access to a logical unit through the use of a proxy token (see 5.99.5.2).

Once access controls are enabled, they shall remain enabled until:

- a) successful completion of an ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action; or
- b) vendor specific physical intervention.

Successful downloading of firmware may result in access controls being disabled.

Once access controls are enabled, power cycles, logical unit resets, and target resets shall not disable them.

5.99.2 The access control list

5.99.2.1 ACL overview

The specific access controls for a SCSI target device are instantiated by the access controls coordinator using data in an access control list (ACL). The ACL contains zero or more access control list entries (ACEs), each ACE contains the following:

- a) one access identifier (see 5.99.2.2) that identifies the initiator(s) to which the ACE applies; and
- b) a list of logical unit access control descriptors (LUACDs) that identify the logical units to which the initiator(s) have access and the LUNs used to access those logical units by the initiator(s), each LUACD (see 5.99.2.3) contains the following:
 - A) a vendor specific reference for the logical unit; and
 - B) a LUN.

Figure f1 shows the structure of an ACL.

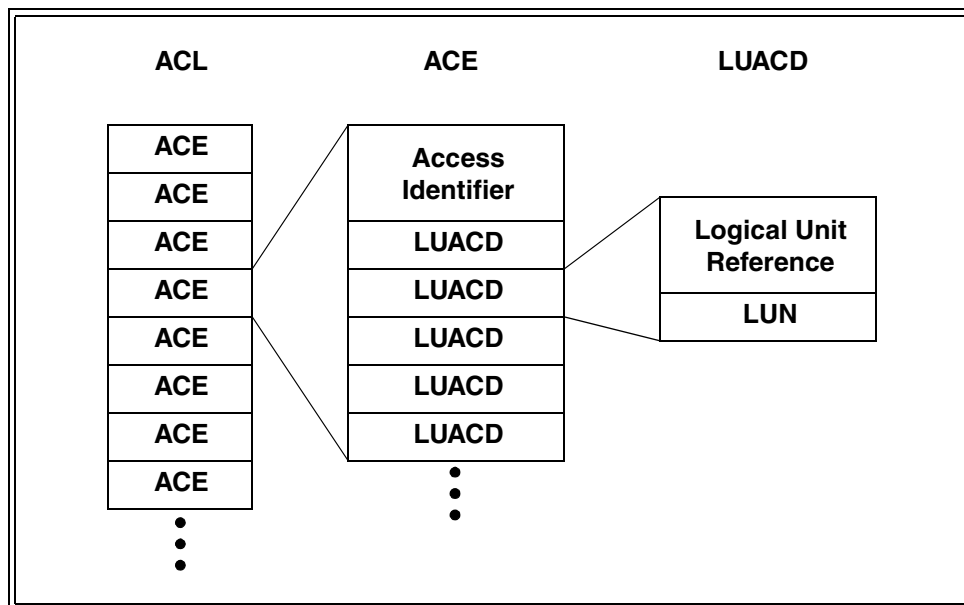


Figure f1 — ACL Structure

5.99.2.2 Access identifiers

5.99.2.2.1 Access identifiers overview

Initiators are identified in ACEs using one of the following types of access identifiers :

- a) AccessID - based on initiator enrollment as described in 5.99.2.2.2 ;
- b) TransportID - based on protocol and interconnect specific identification of initiators as described in 5.99.2.2.3; and
- c) vendor specific access identifiers.

5.99.2.2.2 AccessID access identifiers

All AccessID access identifiers shall have the format shown in table 2.

Table t2 — AccessID access identifier format

Bit Byte	7	6	5	4	3	2	1	0
0	ACCESSID							
15	ACCESSID							
16	Reserved							
23	Reserved							

The ACCESSID field contains a value that uniquely identifies the AccessID type ACE in which the AccessID access identifier appears.

An initiator is allowed access to the logical units in an ACE containing an AccessID type access identifier when that initiator is enrolled as described in 5.99.4. An initiator that has not previously enrolled uses the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action to enroll including the AccessID in parameter data as specified in 7.2.4.

An initiator is identified by or associated with an AccessID type access identifier if that initiator is in the enrolled or pending-enrolled state with respect to that AccessID (see 5.99.4). At any given time, an initiator may be identified or associated with at most one AccessID. All initiators enrolled using a given AccessID share the same ACE and access to all the logical units its LUACDs describe.

5.99.2.2.3 TransportID access type identifiers

Use of the TransportID is protocol and interconnect specific.

An initiator is identified by a TransportID if that initiator accessed the SCSI target device with that TransportID. At any given time, an initiator may be identified or associated with at most one TransportID .

Protocol standards should specify the description and use of the TransportID. A protocol specification for a TransportID shall only include initiator port identifiers or names (see SAM-2) that persist across common reset events in the service delivery subsystem. Additionally, a TransportID shall be no more than 24 bytes long and shall have in its first byte a value which uniquely identifies the transport protocol (see 8.99.99).

TransportIDs that for some protocols may be specified in clause 8.99.99 to support protocol standards that are unable to include a TransportID definition. When a protocol standard includes a TransportID definition, the definition in the protocol standard supersedes any definition appearing in this standard.

5.99.2.3 Logical unit access control descriptors

Each LUACD in an ACE identifies one logical unit to which the initiator(s) associated with the access identifier are allowed access and specifies the LUN value those initiators use when accessing the logical unit.

The identification of a logical unit in a LUACD is vendor specific. The LUN value shall conform to the requirements specified in SAM-2.

A logical unit shall be referenced in no more than one LUACD per ACE . A given LUN value shall appear in no more than one LUACD per ACE .

5.99.3 Managing the ACL

5.99.3.1 ACL management overview

The contents of the ACL are managed by an application client using the ACCESS CONTROL OUT command with MANAGE ACL and DISABLE ACCESS CONTROLS service actions. The ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2) is used to add, remove, or modify ACEs thus adding, revoking, or changing the allowed access of initiators to logical units. The ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action (see 7.2.3) disables access controls and discards the ACL.

5.99.3.2 Authorizing ACL management

To reduce the possibility of applications other than authorized ACL managers changing the ACL, successful completion of the ACCESS CONTROL OUT command with MANAGE ACL or DISABLE ACCESS CONTROLS service action requires delivery of the correct management identifier key value (see 5.99.7) in the ACCESS CONTROL OUT parameter data. For similar reasons other ACCESS CONTROL OUT and ACCESS CONTROL IN service actions require the correct management identifier key as summarized in table t3 and table t4.

Table t3 — ACCESS CONTROL OUT management identifier key requirements

Service Action	Name	Management Identifier Key Required	Reference
00h	MANAGE ACL	Yes	7.2.2
01h	DISABLE ACCESS CONTROLS	Yes	7.2.3
02h	ACCESS ID ENROLL	No	7.2.4
03h	CANCEL ENROLLMENT	No	7.2.5
04h	CLEAR ACCESS CONTROLS LOG	Yes	7.2.6
05h	MANAGE OVERRIDE LOCKOUT TIMER	Yes/ <u>No</u>	7.2.7
06h	OVERRIDE MGMT ID KEY	No	7.2.8
07h	REVOKE PROXY TOKEN	No	7.2.9
08h	REVOKE ALL PROXY TOKENS	No	7.2.10
09h	ASSIGN PROXY LUN	No	7.2.11
0Ah	RELEASE PROXY LUN	No	7.2.12
0Bh-17h	Reserved		
18h-1Fh	Vendor-specific		

Table t4 — ACCESS CONTROL IN management identifier key requirements

Service Action	Name	Management Identifier Key Required	Reference
00h	REPORT ACL	Yes	7.1.2
01h	REPORT LU DESCRIPTORS	Yes	7.1.3
02h	REPORT ACCESS CONTROLS LOG	Yes	7.1.4
03h	REPORT OVERRIDE LOCKOUT TIMER	Yes	7.1.5
04h	REQUEST PROXY TOKEN	No	7.1.6
05h-17h	Reserved		
18h-1Fh	Vendor-specific		

5.99.3.3 Identifying logical units during ACL management

Although the identification of logical units in the ACL is vendor specific (see 5.99.2.3), the ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2) needs a mechanism for identifying logical units that is independent of LUN value and suitable for exchanges between the access controls coordinator and application clients. To serve the needs of the ACCESS CONTROL OUT command with MANAGE ACL service action the access controls coordinator shall identify every logical unit of a SCSI target device with a unique default LUN value. The default LUN values used by the access controls coordinator shall be the LUN values that would be reported by the REPORTS LUNS command if access controls were disabled. An application client discovers the default LUN values using the ACCESS CONTROL IN command with REPORT LU DESCRIPTORS (see 7.1.3) or REPORT ACL (see 7.1.2) service action and subsequently supplies those default LUN values to the access controls coordinator using the ACCESS CONTROL OUT command with MANAGE ACL service action.

The association between default LUN values and logical units is managed by the access controls coordinator and may change in ways beyond the scope of this standard. To track changes in the association between default LUN values and logical units, the access controls coordinator shall maintain the DLgeneration (Default LUNs Generation) value as described in 5.99.3.4.

5.99.3.4 Tracking changes in logical unit identification

The access controls coordinator shall maintain the DLgeneration (Default LUNs Generation) value to track changes in the association between default LUN values and logical units.

When access controls are disabled DLgeneration shall be zero. When access controls are first enabled (see 5.99.1) DLgeneration shall be set to one. While access controls are enabled, the access controls coordinator shall increase DLgeneration by one every time the association between default LUN values and logical units changes for any reason, including but not limited to creation of a new logical unit, deletion of an existing logical unit or a change (delete and recreate) of an existing logical unit.

The access controls coordinator shall include the current DLgeneration in the parameter data returned by each ACCESS CONTROL IN command with REPORT LU DESCRIPTORS (see 7.1.3) or REPORT ACL (see 7.1.2) service action. The application client shall supply the DLgeneration for the default LUN values it is using in each ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2). Before processing the ACL change information in the parameter list provided by an ACCESS CONTROL OUT command with MANAGE ACL service action, the access controls coordinator shall verify that the DLgeneration in the parameter data matches the DLgeneration currently in use. If the DLgeneration verification finds a mismatch, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST.

5.99.4 Enrolling AccessIDs

5.99.4.1 Enrollment states

5.99.4.1.1 Summary of enrollment states

Initiators enroll an AccessID with an access controls coordinator in order to be allowed access to logical units listed in the ACE having the same AccessID type access identifier. Enrolling an AccessID is accomplished using the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action (see 7.2.4). An initiator shall be in one of three states with respect to such an enrollment:

- a) **not-enrolled:** The state for an initiator before it sends the first ACCESS CONTROL OUT command with ACCESS ID ENROLL service action to the access controls coordinator. Also the state for an initiator following successful completion of an ACCESS CONTROL OUT command with CANCEL ENROLLMENT service action (see 7.2.5);
- b) **enrolled:** The state for an initiator following successful completion of an ACCESS CONTROL OUT command with ACCESS ID ENROLL service action ; or
- c) **pending-enrolled:** The state for an enrolled initiator following:
 - A) Events in the service delivery subsystem described in 5.99.11; or
 - B) Successful completion of an ACCESS CONTROL OUT command with MANAGE ACL service action and FLUSH bit set to one (see 7.2.2).

5.99.4.1.2 Not-enrolled state

The access controls coordinator shall place an initiator in the not-enrolled state when it first detects the receipt of a SCSI command or task management function from that initiator . The initiator shall remain in the not-enrolled state until successful completion of an ACCESS CONTROL OUT command with ACCESS ID ENROLL service action (see 7.2.5).

When in the not-enrolled state, an initiator shall only have access to logical units on the basis of a TransportID or on the basis of proxy tokens.

The access controls coordinator shall change an initiator from the enrolled or pending-enrolled state to the not-enrolled state in response to the following events:

- a) Successful completion of the ACCESS CONTROL OUT command with CANCEL ENROLLMENT service action (see 7.2.5);
- b) Successful completion of an ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2) that replaces the ACL entry for the enrolled AccessID as follows:
 - A) If the NOCNCL bit (see 7.2.2.2) is set to zero in the ACCESS CONTROL OUT command with MANAGE ACL service action parameter data, the state shall change to not-enrolled; or
 - B) If the NOCNCL bit is set to one, the state may change to not-enrolled based on vendor specific criteria ; or
- c) Power cycles or target resets based on vendor specific criteria (see 5.99.11).

An enrolled initiator may find itself in the not-enrolled state as a result of actions taken by a third-party (e.g., an ACCESS CONTROL OUT command with MANAGE ACL service action performed by another initiator or a target reset). The purpose of placing an enrolled initiator in the not-enrolled state in response to these events is to give the initiator an indication that the ACE defining its logical unit access has changed. One consequence of changes in an ACE is that previous relationships between logical units and LUN values may no longer apply. If an initiator detects this loss of enrollment, it may take recovery actions. However, such actions may be disruptive for the initiator and may not always be required. Use of the not-enrolled state and the resulting disruptive recovery actions are avoidable if the application client that sends the ACCESS CONTROL OUT command with MANAGE ACL

service action is able to determine its requested changes to the ACL do not alter the existing relationships between logical units and LUN values in any existing ACEs with AccessID type access identifiers.

If the application client that sends the ACCESS CONTROL OUT command with MANAGE ACL service action is unable to determine whether the ACE logical unit relationships are altered as a result of processing the command, then it should set the NOCNCL bit to zero and it should coordinate the ACL change with the affected initiators to ensure proper data integrity. Such coordination is beyond the scope of this standard.

If the application client that sends the ACCESS CONTROL OUT command with MANAGE ACL service action is able to determine that ACE logical unit relationships are not be altered as a result of processing the command, then it should set the NOCNCL bit to one, recommending to the access controls coordinator that initiators be left in their current enrollment states.

The access controls coordinator has at least three vendor specific options for responding to a NOCNCL bit value of one :

- a) Honor the recommendation. This is least disruptive for the initiator and requires no extra actions on the part of the access controls coordinator;
- b) Ignore the recommendation and always place the initiator in the non-enrolled state. This may disrupt an initiator unnecessarily, but requires no extra resources on the part of the access controls coordinator; or
- c) Ignore the recommendation and instead examine the current and new ACEs to determine if the initiator should be placed in the non-enrolled state.

5.99.4.1.3 Enrolled state

The access controls coordinator shall place an initiator in the enrolled state (or enrolls the initiator) following successful completion of the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action (see 7.2.4). The ACCESS CONTROL OUT command with ACCESS ID ENROLL service action is successful only under the following conditions:

- a) If the initiator was in the not-enrolled state and the AccessID in the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action parameter data matches the access identifier in an ACE. The initiator thus enrolled is allowed access to the logical units specified in the LUACDs in the ACE (see 5.99.2) ; or
- b) If the initiator was in the enrolled or pending-enrolled state and the AccessID in the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action parameter data matches the current enrolled AccessID for the initiator.

If the initiator was in the enrolled or pending-enrolled state and the AccessID in the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action parameter data does not match the current enrolled AccessID for the initiator, the command shall be terminated with CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - ENROLLMENT CONFLICT, and the access controls coordinator shall transition an enrolled initiator to the pending-enrolled state.

- a) Transitions out of the enrolled state are described in:5.99.4.1.2 for changes to the not-enrolled state; and
- b) 5.99.4.1.4 for changes to the pending-enrolled state.

NOTE 1 - This standard does not preclude implicit enrollments through mechanisms in the service delivery subsystem. Such mechanisms should perform implicit enrollments after identification by TransportID and should fail in the case where there are ACL conflicts as described in 5.99.4.2.

5.99.4.1.4 Pending-enrolled state

The access controls coordinator shall place an initiator in the pending-enrolled state only if that initiator currently is in the enrolled state, and in response to the following:

- a) Any event in the service delivery subsystem that causes the access controls coordinator to question whether an initiator in the enrolled state has changed its AccessID (e.g., a process or port logout in Fibre Channel, or a hard bus reset for parallel SCSI);
- b) Successful completion of an ACCESS CONTROL OUT command with MANAGE ACL service action where the FLUSH bit is set to one in the parameter data; or
- c) Optionally after a TARGET RESET task management function, as described in 5.99.11.

While in the pending-enrolled state, the initiator's access to logical units is limited as described in 5.99.6.

5.99.4.2 ACL LUN conflict resolution

Three types of ACL LUN conflicts may occur at the time an initiator in the not-enrolled state attempts to enroll an AccessID using the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action:

- a) The TransportID ACE (see 5.99.2) and the AccessID ACE for the initiator each contain a LUACD with the same LUN value but with references to different logical units;
- b) The TransportID ACE and the AccessID ACE for the initiator each contain a LUACD with the different LUN values but with references to the same logical unit; or
- c) The initiator has proxy access rights to a logical unit addressed with a LUN value that equals a LUN value in a LUACD in the AccessID ACE for the initiator .

In any of these cases, the following actions shall be taken as part of the handling of the enrollment function :

- a) The ACCESS CONTROL OUT command with ACCESS ID ENROLL service action shall be terminated with CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - ACL LUN CONFLICT;
- b) The initiator shall remain in the not-enrolled state; and
- c) Except when the ACL LUN conflict is the result of proxy access rights , the access controls coordinator shall record the event in the access controls log as described in 5.99.9.

5.99.5 Granting and revoking access rights

5.99.5.1 Non-proxy access rights

The ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2) adds or replaces ACEs in the ACL (see 5.99.2). One ACE describes the logical unit access allowed to one access identifier (see 5.99.2.2) and the LUN values to be used in addressing the accessible logical units. The access identifier designates the initiator(s) that may be permitted the logical unit access described by the ACE.

With the exception of proxy access rights (see 5.99.5.2), logical unit access rights are granted by:

- a) Adding a new ACE to the ACL allowing logical unit access to a new access identifier ; or Replacing an existing ACE so that the revised ACE includes additional LUACDs .

With the exception of proxy access rights, access rights are revoked by:

- a) Removing an ACE from the ACL ; or
- b) Replacing an existing ACE so that the revised ACE removes one or more LUACDs .

When an ACE is added or replaced the requirements stated in 5.99.4.1.2 and 5.99.10 apply.

5.99.5.2 Proxy access

5.99.5.2.1 Proxy tokens

An initiator with access to a logical unit on the basis of an ACE in the ACL (see 5.99.5.1) may temporarily share that access with third parties using the proxy mechanism. The initiator uses the ACCESS CONTROL IN command with REQUEST PROXY TOKEN service action (see 7.1.6) to request that the access control coordinator generate a proxy token for the logical unit specified by the LUN value in the parameter data .

The access controls coordinator generates the proxy token in a vendor specific manner. For a given SCSI target device, all active proxy token values should be unique. Proxy token values should not be reused any more frequently than is necessary to prevent stale proxy tokens from being given unintended meaning.

Power cycles and target resets shall not affect the validity and proxy access rights of proxy tokens (see 5.99.11). A proxy token shall remain valid and retain the same proxy access rights until one of the following occurs:

- a) An initiator with access to the logical unit based on an ACE in the ACL revokes the proxy token using:
 - A) The ACCESS CONTROL OUT command with REVOKE PROXY TOKEN service action (see 7.2.9) supplying the specific proxy token in the parameter data; or
 - B) The ACCESS CONTROL OUT command with REVOKE ALL PROXY TOKENS service action (see 7.2.10) ;
- b) An application client issues the ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2) with parameter data containing the Revoke Proxy Token page (see 7.2.2.4) or Revoke All Proxy Tokens page (see 7.2.2.5).

5.99.5.2.2 Proxy LUNs

The initiator forwards the proxy token (see 5.99.5.2.2) to a third party (e.g., in a target descriptor in the parameter data of the EXTENDED COPY command).

The third party sends the access controls coordinator an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action (see 7.2.11) containing the proxy token to request creation of a proxy access right to the referenced logical unit . The access controls coordinator determines the referenced logical unit from the proxy token value; the third party is unaware of the exact logical unit to which it is requesting access. The parameter data for the ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action includes the LUN value that the third party intends to use when accessing the referenced logical unit. The LUN value thus assigned is called a proxy LUN.

A proxy LUN shall remain valid until one of the following occurs:

- a) The third party releases the proxy LUN value using the ACCESS CONTROL OUT command with RELEASE PROXY LUN service action (see 7.2.12);
- b) An event in the service delivery subsystem causes the access controls coordinator to question whether the third party initiator that created the proxy LUN value has changed and may no longer be in possession of the proxy token);
- c) The proxy token is made invalid as described in 5.99.5.2.1; or
- d) A power cycle or target reset occurs (see 5.99.11).

If the third party believes that the invalidation of a proxy LUN value is temporary, it may reissue the ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action in an attempt to re-establish its proxy access rights. The access controls coordinator shall process the request as described in 5.99.5.2.1 without reference to any previous assignment of the proxy LUN value.

5.99.6 Verifying access rights

When access controls are enabled (see 5.99.1), access rights for an initiator shall be validated as described in this subclause.

All commands shall be processed as if access controls were not present if the ACL (see 5.99.2) allows the initiator access to the addressed logical unit by virtue of one of the following conditions:

- a) The ACL contains an ACE containing a TransportID type access identifier for the initiator and that ACE includes a LUACD with LUN value matching the addressed LUN;
- b) The initiator is in the enrolled state (see 5.99.4.1.3) under an AccessID, the ACL contains an ACE containing that AccessID as an access identifier, and that ACE includes a LUACD with LUN value matching the addressed LUN; or
- c) The addressed LUN matches a proxy LUN value (see 5.99.5.2.2) assigned using the ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action (see 7.2.11) and the proxy token (see 5.99.5.2.1) used to assign the proxy LUN value is still valid.

If the initiator is in the pending-enrolled state (see 5.99.4.1.4) under an AccessID, the ACL contains an ACE containing that AccessID as an access identifier, and that ACE includes a LUACD with LUN value matching the addressed LUN, then commands shall be processed as follows:

- a) INQUIRY, REPORT LUNS, ACCESS CONTROL OUT and ACCESS CONTROL IN commands shall be processed as if access controls were not present;
- b) All other commands shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - INITIATOR PENDING-ENROLLED.

An initiator should respond to the ACCESS DENIED - INITIATOR PENDING-ENROLLED additional sense code by sending an ACCESS CONTROL OUT command with ACCESS ID ENROLL service action. If the command succeeds, the initiator may retry the failed command.

If an INQUIRY command is addressed to a LUN for which there is no matching LUN value in any LUACD in any ACE allowing the initiator logical unit access rights, the standard INQUIRY data (see 7.z.z) PERIPHERAL DEVICE TYPE field shall be set to 1Fh and the PERIPHERAL QUALIFIER field shall be set to 011b (the device server is not capable of supporting a device at this logical unit).

The parameter data returned in response to a REPORT LUNS command addressed to LUN 0 shall return only the list of LUN values that are associated to accessible logical units according to the following criteria:

- a) If the initiator is in the enrolled or pending-enrolled state, the REPORT LUNS parameter data shall include any LUN values found in LUACDs in the ACE containing the AccessID enrolled by the initiator;
- b) If the initiator (in any enrollment state) has a TransportID found in the access identifier of an ACE, the REPORT LUNS parameter data shall include any LUN values found in LUACDs in that ACE; and
- c) If the initiator (in any enrollment state) has access to any proxy LUNs (see 5.99.5.2.2), those LUN values shall be included in the REPORT LUNS parameter data.

If the initiator is in the not-enrolled state and is not allowed access to any logical unit as result of its TransportID or as a result of a proxy LUN assignment, then the REPORT LUNS parameter data shall include only LUN 0, as specified in 7.z.z.

Except when access controls are disabled, all cases not described previously in this subclause shall result in termination of the command with CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to LOGICAL UNIT NOT SUPPORTED.

5.99.7 The management identifier key

5.99.7.1 Management identifier key usage

The purpose of the management identifier key is to identify the application that is responsible for managing access controls for a SCSI target device. This identification is accomplished by allowing the application client to specify a new management identifier key value in the parameter data of each ACCESS CONTROL OUT command with the MANAGE ACL service action (see 7.2.2), and by requiring the most recently specified management identifier key value to appear in many ACCESS CONTROL IN and ACCESS CONTROL OUT service actions.

To allow for failure scenarios where the management identifier key value has been lost, an override procedure involving a timer is provided as described in 5.99.7.2.

- a) Use of the management identifier key has the following features: Management of access controls is associated with those application clients that are able to provide the correct management identifier key and not with a single initiator port identifier (see SAM-2);
- b) Only an application client that has knowledge of the management identifier key may (in most cases) change the ACL for the SCSI target device with the result that management of access controls may be limited to specific applications and application clients.

5.99.7.2 Overriding the management identifier key

5.99.7.2.1 The OVERRIDE MGMT ID KEY service action

Conditions may arise when the management identifier key needs to be replaced and the current key is not available. When this occurs, the ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action (see 7.2.8) may be used to force the management identifier key to a known value.

The ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action is intended only for failure scenarios. The ACCESS CONTROL OUT command with MANAGE ACL service action should be used in all other circumstances.

To protect the management identifier key from unauthorized overrides, the access controls coordinator shall restrict use of the ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action based on the value of the override lockout timer (see 5.99.7.2.2).

When the override lockout timer is not zero, an ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action shall be terminated with CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

When the override lockout timer is zero, an ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action shall be processed as described in 7.2.8.

The access controls coordinator shall log the receipt of all ACCESS CONTROL OUT commands with OVERRIDE MGMT ID KEY service action and their success or failure as described in 5.99.9.

5.99.7.2.2 The override lockout timer

The access controls coordinator shall maintain the override lockout timer as a 16 bit unsigned integer. When the override lockout timer is not zero it shall be decreased by one approximately once per second but no more frequently than once every 800 milliseconds until the value reaches zero. The ACCESS CONTROL OUT command with MANAGE OVERRIDE LOCKOUT TIMER service action manages the state of the override lockout timer (see

7.2.7), performing one of two functions depending on whether the correct management identifier key is supplied in the parameter data.

- a) If the incorrect management identifier key is supplied or if no parameter data is sent, the access controls coordinator shall reset the override lockout timer to the most recently received initial override lockout timer value; or
- b) If the correct management identifier key is supplied, then the access controls coordinator shall do the following:
 - 1) Save the initial override lockout timer value supplied in the parameter data; and
 - 2) Reset the override lockout timer to the new initial value.

NOTE 2 - Setting the initial override lockout timer value to zero disables the override lockout timer and allows the ACCESS CONTROL OUT command with OVERRIDE MGMT KEY service action to succeed at any time.

Overloading the management key identifier to have a function selection usage is an unusual operational specification, however, it offers significant advantages for the ACCESS CONTROL OUT command with MANAGE OVERRIDE LOCKOUT TIMER service action. Any application that knows the management identifier key may establish an initial override lockout timer value of sufficient duration (up to about 23 hours). Maintaining a non-zero override lockout timer value may be accomplished without knowing the management identifier key or transporting the management identifier key on the service delivery subsystem. Attempts to establish a zero initial override lockout timer value that are not accompanied by the correct management identifier key result in decreasing the probability that a subsequent ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action is able to succeed by resetting the override lockout timer to the most recently specified initial value that was accompanied by the correct management identifier key.

The ACCESS CONTROL IN command with REPORT OVERRIDE LOCKOUT TIMER may be used to discover the state of the override lockout timer.

5.99.8 Reporting access control information

Specific service actions of the ACCESS CONTROL IN command may be used by an application client to request a report from the access controls coordinator about its access controls data and state.

The ACCESS CONTROL IN command with REPORT ACL service action (see 7.1.2) returns the ACL (see 5.99.2). The information reported includes the following:

- a) the list of access identifiers (see 5.99.2.2) and the associated LUACDs (see 5.99.2.3) currently in effect; and
- b) the list of proxy tokens (see 5.99.5.2.1) currently in effect.

The ACCESS CONTROL IN command with REPORT ACCESS CONTROLS LOG service action (see 7.1.4) returns the contents of the access controls log (see 5.99.9).

The ACCESS CONTROL IN command with REPORT OVERRIDE LOCKOUT TIMER service action (see 7.1.5) reports on the state of the override lockout timer (see 5.99.7.2.2).

5.99.9 Access controls log

The access controls log is a record of events maintained by the access controls coordinator.

The access controls log has three portions, recording different classes of events:

- a) invalid key events: a mismatch between the management identifier key (see 5.99.7) in a CDB or parameter data and the current value maintained by the access controls coordinator;

- b) key override events: attempts to override the management identifier key (see 5.99.7.2.1), whether the attempt fails or succeeds;
- c) ACL LUN conflict events (see 5.99.4.2).

Each portion of the log is required to contain a counter of the events. When a device ships from the factory, the counters shall be zero. The counters shall be increased by one whenever the relevant event occurs

Optionally, each log portion may contain additional records with more specific information about each event. When the resources for additional log records are exhausted, the access controls coordinator shall preserve the most recently added log records in preference to the older log records.

Log records contain a TIME STAMP field whose contents are vendor specific. If the access controls coordinator has no time stamp resources the TIME STAMP field shall be set to zero. If time stamp values are provided, the same timing clock and time stamp format shall be used for all access controls log entries.

Invalid key events occur whenever an access controls command requires checking an initiator supplied management identifier key either in the CDB or in the parameter data against the current management identifier key saved by the access controls coordinator and the two values fail to match. When such an event occurs, the access controls coordinator shall increase the invalid keys counter by one. If the log has additional resources to record event details, the access controls coordinator shall add an invalid keys log record (containing the information defined in 7.1.4.2.3) describing the event.

Key override events occur when the access controls coordinator receives the ACCESS CONTROL OUT command with OVERRIDE MGMT KEY service action (see 7.2.8). When such an event occurs, the access controls coordinator shall increase the key overrides counter by one without regard for whether the command succeeds or fails. If the log has additional resources to record event details, the access controls coordinator shall add an key overrides log record (containing the information defined in 7.1.4.2.2) describing the event. ACL LUN conflict events occur as specified in 5.99.4.2. When such an event occurs, the access controls coordinator shall increase the ACL LUN conflicts counter by one. If the log has additional resources to record event details, the access controls coordinator shall add an ACL LUN conflicts log record (containing the information defined in 7.1.4.2.4) describing the event.

Selected portions of the access controls log may be requested by an application client using the ACCESS CONTROL IN command with REPORT ACCESS CONTROLS LOG service action (see 7.1.4). With the exception of the key overrides portion, selected portions of the log may be cleared and the counters reset to zero using the ACCESS CONTROL OUT command with CLEAR ACCESS CONTROLS LOG service action (see 7.2.6).

5.99.10 Interactions of access controls and other features

5.99.10.1 Queuing relationships and access controls

Upon successful completion of an ACCESS CONTROL OUT command with MANAGE ACL service action (see 7.2.2), the ACL (see 5.99.2) defined by that command shall apply to all tasks that subsequently enter the task enabled state. Tasks that have modified the media, mode pages, or equivalent SCSI target device elements shall not be affected by an ACCESS CONTROL OUT command that subsequently enters the task enabled state. Tasks in the task enabled state that have not modified the media, mode pages or equivalent SCSI target device elements may or may not be affected by an ACCESS CONTROL OUT command that subsequently enters the task enabled state. The ACL in effect prior to when the ACCESS CONTROL OUT command with MANAGE ACL or DISABLE ACCESS CONTROLS service action entered the task enabled state shall apply to all tasks that are not affected by the ACCESS CONTROL OUT command.

A task shall complete all its media modifications etc. under the control of a single ACL, either the state in effect prior to processing of the ACCESS CONTROL OUT command or the state in effect following processing of the

ACCESS CONTROL OUT command. After a task has begun its media modifications etc., changing the access control state from disabled to enabled (see 5.99.1) shall have no effect on the task.

Multiple access control commands, both ACCESS CONTROL IN and ACCESS CONTROL OUT, may be queued concurrently. The order of processing of such commands is defined by the tagged queuing restrictions, if any, but each command shall be processed as a single indivisible command without any interleaving of actions that may be required by other access control commands.

5.99.10.2 Existing reservations and ACL changes

If a logical unit is reserved by one initiator and that logical unit becomes accessible to another initiator as a result of an access control command, there shall be no changes in the reservation state of that logical unit.

If a logical unit is reserved by an initiator and that logical unit becomes inaccessible to that initiator as a result of an access control command or other access control related event, there shall be no changes in the reservation. Existing mechanisms in RESERVE/RELEASE and Persistent Reservations allow for other initiators with access to that logical unit to clear the reservation.

5.99.11 Access controls information persistence and memory usage requirements

- a) If a SCSI target device supports the access controls, then the SCSI target device shall contain an access controls coordinator that shall maintain the following information in nonvolatile memory: Whether access controls are enabled or disabled;
- b) The access controls data described as persistent across power cycles and resets in table t5 and table t6.

If access controls are disabled the readiness of the access control coordinator's nonvolatile memory shall not affect the processing of commands. If access controls are enabled and the access control coordinator's nonvolatile memory is not ready, the device servers for all logical units shall terminate all commands except INQUIRY commands with a CHECK CONDITION status, the sense key shall be set to NOT READY and additional sense data shall be set as described in table 117 (see 7.z.z).

Following a power cycle or reset event, all previously enrolled initiators shall be placed in the same enrollment state and that state shall be one of the following:

- a) pending-enrolled (see 5.99.4.1.4); or
- b) not-enrolled (see 5.99.4.1.2).

The information shown in table t5 shall be maintained by the access controls coordinator.

Table t5 — Mandatory access controls resources

Information Description	Size (in bits)	Persistent Across Power Cycles and Resets
One ACL (see 5.99.2) containing at least one ACE containing one access identifier (see 5.99.2.2); and at least one LUACD (see 5.99.2.3)	VS	Yes
The Enrollment State for <u>each initiator</u> (see 5.99.4.1)	VS	Yes
Management Identifier Key (see 5.99.7)	64	Yes
Default LUNs Generation a.k.a. DLgeneration (see 5.99.3.4)	32	Yes
<u>Override Lockout Timer</u> (see 5.99.7.2.2)	<u>16</u>	<u>No</u>
Initial Override Lockout Timer value (see 5.99.7.2.2)	16	Yes
Access Controls Log Event Counters (see 5.99.9) containing at least the following:		Yes
Key Overrides Counter	16	Yes
Invalid Keys Counter	16	Yes
ACL LUN Conflicts Counter	16	Yes

Optionally, the access controls coordinator may maintain the information shown in table t6.

Table t6 — Optional access controls resources

Information Description	Size (in bits)	Persistent Across Power Cycles and Resets
One or more proxy tokens (see 5.99.5.2.1)	64	Yes
One or more proxy LUNs (see 5.99.5.2.2)	64	No
Access controls log event records (see 5.99.9) for		
Key Overrides events	(see 7.1.4.2.2)	<u>Yes</u>
Invalid Keys events	(see 7.1.4.2.3)	<u>Yes</u>
ACL LUN Conflicts events	(see 7.1.4.2.4)	<u>Yes</u>

When shipped from the factory, the ACL shall be empty, all values shown in table t5 shall be zero, additional access control log structures shall be empty and there shall be no valid proxy tokens.

F.7 – SPC-3 Command Definitions

Clause 7 of SPC-3 should have the following command definitions added.

7.1 ACCESS CONTROL IN command

7.1.1 ACCESS CONTROL IN [introduction](#)

The [service actions of the ACCESS CONTROL IN command](#) (see table t7) [are](#) used to obtain information about the access controls that are active within the access controls coordinator and to facilitate other [access control functions](#) (see 5.99). [If the ACCESS CONTROL IN command is implemented](#), the ACCESS CONTROL OUT command [also shall be implemented](#). [The ACCESS CONTROL IN command](#) shall not be affected by access controls.

Table t7 — ACCESS CONTROL IN service actions

Service Action	Command name	Type	Reference
00h	REPORT ACL	m	7.1.2
01h	REPORT LU DESCRIPTORS	m	7.1.3
02h	REPORT ACCESS CONTROLS LOG	m	7.1.4
03h	REPORT OVERRIDE LOCKOUT TIMER	m	7.1.5
04h	REQUEST PROXY TOKEN	o	7.1.6
05h - 17h	Reserved		
18h - 1Fh	Vendor specific		
Key: m = Service action implementation is mandatory if ACCESS CONTROL IN is implemented. o = Service action implementation is optional.			

If the device contains an access controls coordinator, [the ACCESS CONTROL IN command](#) shall be processed by the access controls coordinator if addressed to LUN 0. [The ACCESS CONTROL IN command also may be addressed](#) to any other LUN value whose standard INQUIRY data ([see 7.z.z](#)) has the ACC bit set to one, [in which case it shall be processed in the same manner as if the command had been addressed to LUN 0](#). [If an ACCESS CONTROL IN command is received by a device server whose standard INQUIRY data has the ACC bit set to zero](#), the command shall be [terminated with a CHECK CONDITION status](#), the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID COMMAND OPERATION CODE .

7.1.2 REPORT ACL service action

7.1.2.1 REPORT ACL introduction

The [ACCESS CONTROL IN command](#) with REPORT ACL service action (see [table t8](#)) is used to query the ACL (see [5.99.2](#)) maintained by the access controls coordinator. If the [ACCESS CONTROL IN command](#) is implemented, the REPORT ACL service action shall be implemented.

Table t8 — ACCESS CONTROL IN command with REPORT ACL service action

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (86h)							
1	Reserved			SERVICE ACTION (00h)				
2	(MSB)	MANAGEMENT IDENTIFIER KEY						(LSB)
9								
10	(MSB)	ALLOCATION LENGTH						(LSB)
13								
14	Reserved							
15	CONTROL							

If access controls are disabled, the device server shall ignore the MANAGEMENT IDENTIFIER KEY field and shall respond with GOOD status returning only the eight byte parameter list header specified in 7.1.2.2 subject to the ALLOCATION LENGTH limitation described in [4.3.4.6](#).

If access controls are enabled and the contents of the MANAGEMENT IDENTIFIER KEY field do not match the current management identifier key (see [5.99.3.2](#)) maintained by the access controls coordinator, parameter data shall not be returned, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see [5.99.9](#)).

The ALLOCATION LENGTH field is described in [4.3.4.6](#). The ALLOCATION LENGTH field value should be at least eight.

7.1.2.2 REPORT ACL parameter data format

7.1.2.2.1 REPORT ACL parameter data introduction

The format of the parameter data returned in response to an ACCESS CONTROL IN command with REPORT ACL service actions is shown in table t9.

Table t9 — ACCESS CONTROL IN with REPORT ACL parameter data format

Bit Byte	7	6	5	4	3	2	1	0
Parameter list header								
0	(MSB)	ACL DATA LENGTH (n-3)						(LSB)
3								
4	(MSB)	DLGENERATION						(LSB)
7								
ACL data pages								
8		ACL data page 0						
		⋮						
		ACL data page x						
n								

The ACL DATA LENGTH field shall contain a count of the number of bytes in the remaining parameter data. The value in the ACL DATA LENGTH field shall be the actual number of bytes available without consideration for insufficient allocation length in the CDB. If access controls are disabled, the ACL DATA LENGTH field shall be set to four .

The DLGENERATION field shall contain the current DLgeneration value (see 5.99.3.4).

The ACL data pages contain a description of the ACL (see 5.99.2) maintained by the access controls coordinator. Each ACL data page describes one ACE in the ACL or one proxy token (see 5.99.5.2). Every ACE and every proxy token managed by the access controls coordinator shall have an ACL data page in the parameter data. The content and format of an ACL data page is indicated by a page code (see table t10).

Table t10 — ACL data page codes

Page Code	Description	Reference
00h	Granted	7.1.2.2.2
01h	Granted All	7.1.2.2.3
02h	Proxy Tokens	7.1.2.2.4
03h-EFh	Reserved	
F0h-FFh	Vendor specific	

7.1.2.2.2 Granted ACL data page format

The Granted ACL data page (see table t11) describes an ACE that allows access to a specific set of logical units via a list of LUACDs (see 5.99.2.3).

Table t11 — Granted ACL data page format

Bit Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (00h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (n-3)						(LSB)
3								
4	Reserved							
5	ACCESS IDENTIFIER TYPE							
6	(MSB)	ACCESS IDENTIFIER LENGTH (m-7)						(LSB)
7								
8	ACCESS IDENTIFIER							
m								
LUACD Descriptors								
m+1	LUACD descriptor 0							
m+20								
	⋮							
n-19	LUACD descriptor x							
n								

The PAGE LENGTH field shall indicate the number of additional bytes required for this page and shall not be adjusted to reflect any truncation caused by insufficient allocation length.

The ACCESS IDENTIFIER TYPE field (see table t12) indicates the format and usage of the access identifier.

Table t12 — Access Identifier types

Access Identifier Type	Access Identifier Name	Access Identifier Format Reference
00h	AccessID	5.99.2.2.2
01h	TransportID	8.99.99.3
02h-7Fh	Reserved	
80h-FFh	Vendor specific	

The ACCESS IDENTIFIER LENGTH field indicates the number of bytes following taken up by the ACCESS IDENTIFIER field.

The ACCESS IDENTIFIER field contains the identifier that the access controls coordinator uses to select the initiator(s) that are allowed access to the logical units named by the LUACD descriptors in this ACL data page. The

format of the ACCESS IDENTIFIER field is specified in table t12. One and only one Granted or Granted All (see 7.1.2.2.3) page shall be returned for a given value in the ACCESS IDENTIFIER field.

Each LUACD descriptor (see table t13) describes the access allowed to one logical unit based on the access identifier. There shall be one LUACD descriptor for each logical unit to which the access identifier allows access.

Table t13 — Granted ACL page LUACD descriptor format

Bit Byte	7	6	5	4	3	2	1	0	
0	ACCESS MODE								
1	Reserved								
3	Reserved								
4	(MSB)	LUN VALUE						(LSB)	
11									
12	(MSB)	DEFAULT LUN						(LSB)	
19									

The ACCESS MODE field (see table t14) indicates the type of access allowed to the logical unit referenced by the DEFAULT LUN field and addressable at the specified LUN value.

Table t14 — Access mode values

Access Mode	Description
00h	Normal access
01h-EFh	Reserved
F0h-FFh	Vendor-specific

The LUN VALUE field indicates the LUN value an accessing initiator would use to access the logical unit to which the LUACD descriptor applies.

The DEFAULT LUN field identifies the logical unit to which access is allowed using the default LUN value described in 5.99.3.3. The value in the DEFAULT LUN field shall be consistent with the DLGENERATION field contents returned in the parameter list header (see 7.1.2.2).

NOTE 3 - It is acceptable for the LUN VALUE and DEFAULT LUN fields to contain the same value.

7.1.2.2.3 Granted All ACL data page format

The Granted All ACL data page (see table t15) describes an ACE that allows access to all the SCSI target device’s logical units with the default LUN value as the accessing LUN value. When an access identifier is present in a

Granted All ACL data page, initiators that access via that access identifier are allowed to access the SCSI target device as if access controls were disabled.

Table t15 — Granted All ACL data page format

Bit Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (01h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (m-3)						(LSB)
3								
4	Reserved							
5	ACCESS IDENTIFIER TYPE							
6	(MSB)	ACCESS IDENTIFIER LENGTH (m-7)						(LSB)
7								
8	ACCESS IDENTIFIER							
m								

The PAGE LENGTH, ACCESS IDENTIFIER TYPE, and ACCESS IDENTIFIER LENGTH, are described in 7.1.2.2.2.

The ACCESS IDENTIFIER field contains the identifier that the access controls coordinator uses to select the initiator(s) that are allowed access to all the SCSI target device's logical units with the default LUN value as the accessing LUN value. The format of the access identifier field is specified in table t12 (see 7.1.2.2.2). One and only one Granted (see 7.1.2.2.2) or Granted All page shall be returned for a given value in the ACCESS IDENTIFIER field.

7.1.2.2.4 Proxy tokens ACL data page format

The proxy tokens page (see table t16) describes the proxy tokens (see 5.99.5.2) maintained by the access controls coordinator.

Table t16 — Proxy tokens data page format

Bit Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (02h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (n-3)						(LSB)
3								
Proxy token Descriptors								
4	Proxy token descriptor 0							
23								
:								
:								
n-19	Proxy token descriptor x							
n								

The PAGE LENGTH field shall indicate the number of additional bytes required for this page and shall not be adjusted to reflect any truncation caused by insufficient allocation length.

If there are no active proxy tokens, the access controls coordinator may either not include the proxy tokens page in the parameter data or may include one such page containing no proxy token descriptors.

At most one proxy tokens page shall be included in the parameter data.

Each proxy token descriptor (see table t17) describes the access allowed to one logical unit based on one proxy token. There shall be one proxy token descriptor for each active proxy token maintained by the access controls coordinator.

Table t17 — Proxy token descriptor format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							
3								
4	(MSB)	PROXY TOKEN						(LSB)
11								
12	(MSB)	DEFAULT LUN						(LSB)
19								

The PROXY TOKEN field indicates the proxy token to which this proxy token descriptor applies.

The DEFAULT LUN field identifies the logical unit to which this proxy token allows access using the default LUN value described in 5.99.3.3. The value in the DEFAULT LUN field shall be consistent with the DLGENERATION value returned in the parameter list header (see 7.1.2.2).

NOTE 4 - The same default LUN value may appear in multiple proxy token descriptors, if multiple proxy tokens are valid for the same logical unit.

7.1.3 REPORT LU DESCRIPTORS service action

7.1.3.1 REPORT LU DESCRIPTORS introduction

The ACCESS CONTROL IN command with REPORT LU DESCRIPTORS service action (see table t18) is used to obtain the inventory of logical units for which access controls may be established. If the ACCESS CONTROL IN command is implemented, the REPORT LU DESCRIPTORS service action shall be implemented.

Table t18 — ACCESS CONTROL IN command with REPORT LU DESCRIPTORS service action

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (86h)							
1	Reserved			SERVICE ACTION (01h)				
2	(MSB)	MANAGEMENT IDENTIFIER KEY						(LSB)
9								
10	(MSB)	ALLOCATION LENGTH						(LSB)
13								
14	Reserved							
15	CONTROL							

If access controls are disabled, the device server shall ignore the MANAGEMENT IDENTIFIER KEY field and shall respond with GOOD status returning only the twenty byte parameter list header as specified in 7.1.3.2 subject to the ALLOCATION LENGTH limitation described in 4.3.4.6.

NOTE 5 - When access controls are disabled, the logical unit inventory may be obtained using commands such as REPORT LUNS (see 7.z.z). To facilitate access controls management the ACCESS CONTROL IN command with REPORT LU DESCRIPTORS service action returns more information than the REPORT LUNS command. When access controls are disabled additional commands such as INQUIRY (see 7.z.z) are require to obtain all the information provided by the ACCESS CONTROL IN command with REPORT LU DESCRIPTORS service action.

If access controls are enabled and the contents of the MANAGEMENT IDENTIFIER KEY field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, parameter data shall not be returned, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

The ALLOCATION LENGTH field is described in 4.3.4.6. The ALLOCATION LENGTH field value should be at least twenty.

7.1.3.2 REPORT LU DESCRIPTORS parameter data format

The format of the parameter data returned in response to an ACCESS CONTROL IN command with REPORT LU DESCRIPTORS service actions is shown in table t19.

Table t19 — ACCESS CONTROL IN with REPORT LU DESCRIPTORS parameter data format

Bit Byte	7	6	5	4	3	2	1	0
Parameter list header								
0	(MSB)	LU INVENTORY LENGTH (n-3)						(LSB)
3								
4	(MSB)	NUMBER OF LOGICAL UNITS						(LSB)
7								
8	(MSB)	SUPPORTED LUN-MASK FORMAT						(LSB)
15								
16	(MSB)	DLGENERATION						(LSB)
19								
Logical Unit descriptors								
20		Logical Unit descriptor 0						
		⋮						
		Logical Unit descriptor x						
n								

The LU INVENTORY LENGTH field shall contain a count of the number of bytes in the remaining parameter data. The value in the LU INVENTORY LENGTH field shall be the actual number of bytes available without consideration for insufficient allocation length in the CDB. If access controls are disabled, the LU INVENTORY LENGTH field shall be set to sixteen .

The NUMBER OF LOGICAL UNITS field shall contain a count of the number of logical units managed by the access controls coordinator. The value in NUMBER OF LOGICAL UNITS field shall be the same as the number of Logical Unit descriptors that follow in the parameter data.

The SUPPORTED LUN-MASK FORMAT field (see table t20) contains a summary of the LUN values (see 5.99.2.3) that the access controls coordinator supports. LUN values are exchanged between application clients and the access controls coordinator by several service actions (e.g., the REPORT ACL IN command with REPORT ACL service action described in 7.1.2 and the REPORT ACL OUT command with MANAGE ACL service action described in

7.x.y). The format of the SUPPORTED LUN-MASK FORMAT field follows the eight byte LUN structure defined for dependent logical units by SAM-2.

Table t20 — SUPPORTED LUN-MASK FORMAT field format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	FIRST LEVEL LUN MASK						(LSB)
1		SECOND LEVEL LUN MASK						(LSB)
2	(MSB)	THIRD LEVEL LUN MASK						(LSB)
3		FOURTH LEVEL LUN MASK						(LSB)
4	(MSB)							(LSB)
5								(LSB)
6	(MSB)							(LSB)
7								(LSB)

Table 5: SUPPORTED LUN-MASK FORMAT data format

Byte	Bit							
	7	6	5	4	3	2	1	0
0	MSB	lun-mask part one						LSB
1		lun-mask part two						LSB
2	MSB	lun-mask part three						LSB
3		lun-mask part four						LSB
4	MSB							LSB
5								LSB
6	MSB							LSB
7								LSB

The LUN MASK at each level indicates approximately the logical unit number values the access controls coordinator supports. A bit value of zero in a LUN MASK field indicates that the access controls coordinator prohibits setting that bit to one in a LUN value. A bit value of one in a LUN MASK field indicates that the access controls coordinator may allow setting that bit to one in a LUN value.

For example, if the access controls coordinator only supports level one LUN values and up to 256 LUN values, then the SUPPORTED LUN-MASK FORMAT field shall contain 00FF000000000000h . If only 200 LUN values were supported, the SUPPORTED LUN-MASK FORMAT field still would contain 00FF000000000000h.

The value in the SUPPORT LUN-MASK FORMAT field only summarizes the supported LUN values and is not a complete description. The value in the SUPPORT LUN-MASK FORMAT field should be used as a guideline for specifying LUN values in service actions such as the ACCESS CONTROL OUT command with MANAGE ACL service action, it should not be viewed as a guarantee against rejection of requested LUN values.

The DLGENERATION field shall contain the current DLgeneration value (see 5.99.3.4).

Each Logical Unit descriptor (see table t21) contains information about one logical unit managed by the access controls coordinator. There shall be one Logical Unit descriptor for every logical unit managed by the access controls coordinator.

Table t21 — Logical Unit descriptor format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved			PERIPHERAL DEVICE TYPE				
1	Reserved							
2	(MSB)	DESCRIPTOR LENGTH (n-3)						(LSB)
3								
4	(MSB)	DEFAULT LUN						(LSB)
11								
12	Reserved							
13	EVPD IDENTIFICATION DESCRIPTOR LENGTH							
14	Reserved							
15	DEVICE IDENTIFIER LENGTH							
16	(MSB)	EVPD IDENTIFICATION DESCRIPTOR						(LSB)
47								
48	(MSB)	DEVICE IDENTIFIER						(LSB)
79								
80	(MSB)	DEVICE-TYPE SPECIFIC DATA						(LSB)
n								

The PERIPHERAL DEVICE TYPE field is as defined in [7.z.z](#).

The DESCRIPTOR LENGTH field indicates the total number of bytes remaining in the descriptor and shall not reflect any truncation of the parameter data as a result of insufficient allocation length. If the PERIPHERAL DEVICE TYPE field contains 0h, 4h, or 7h, the DESCRIPTOR LENGTH field shall contain 92 if the descriptor includes the DEVICE-TYPE SPECIFIC DATA field and 80 if it does not. If the PERIPHERAL DEVICE TYPE field contains any value other than 0h, 4h, or 7h, the DESCRIPTOR LENGTH field shall contain 80.

The DEFAULT LUN field contains the default LUN value (see 5.99.3.3) for the logical unit described by this logical unit descriptor. The value in the DEFAULT LUN field shall be consistent with the DLGENERATION value returned in the parameter list header (see 7.1.3.2).

The EVPD IDENTIFICATION DESCRIPTOR LENGTH field indicates the number of non pad bytes in the EVPD IDENTIFICATION DESCRIPTOR field.

The DEVICE IDENTIFIER LENGTH field indicated the number of non pad bytes in the DEVICE IDENTIFIER field.

The EVPD IDENTIFICATION DESCRIPTOR field shall contain non zero bytes if:

- a) The logical unit supports the INQUIRY command (see 7.z.z) with EVPD bit set to one and the PAGE OR OPERATION CODE field set to 83h ; and
- b) At least one identification descriptor in the Device Identification VPD page (see 8.z.z) has 0h in the ASSOCIATION field .

Editors Note 1 - ROW: I believe that meeting both of the above requirements is now mandatory for all SPC-2 devices (and therefore for SPC-3 devices. So, I think the EVPD IDENTIFICATION DESCRIPTOR field must always contain non zero bytes.

When the above criteria are met , the EVPD IDENTIFICATION DESCRIPTOR field shall be derived from one of the identification descriptors having 0h in the ASSOCIATION field as follows:

- a) If the identification descriptor has a length less than or equal to 32 bytes, then the EVPD IDENTIFICATION DESCRIPTOR field shall be set to the value of the identification descriptor in the most significant bytes of the field and the remainder of the field shall be padded with zero in the least significant bytes. The EVPD IDENTIFICATION DESCRIPTOR LENGTH field shall be set to the length of the identification descriptor; or
- b) If the identification descriptor has a length greater than 32 bytes, then the EVPD IDENTIFICATION DESCRIPTOR field shall be set to the 32 most significant bytes of the identification descriptor. The EVPD IDENTIFICATION DESCRIPTOR LENGTH field shall be set to 32.

If there are several identification descriptors having 0h in the ASSOCIATION field, the choice of which descriptor to copy to the EVPD IDENTIFICATION DESCRIPTOR field is vendor specific, however, all ACCESS CONTROL IN commands with REPORT LU DESCRIPTORS service action shall return the same EVPD IDENTIFICATION DESCRIPTOR field contents for a given logical unit.

If no Device Identification VPD page identification descriptors with 0h in the ASSOCIATION field are available , then the EVPD IDENTIFICATION DESCRIPTOR LENGTH field shall be set to zero and the EVPD IDENTIFICATION DESCRIPTOR field shall have all bytes set to zero.

If a device identifier has been set for the logical unit using the SET DEVICE IDENTIFIER command (see 7.z.z), the DEVICE IDENTIFIER field shall contain that device identifier subject to the following considerations:

- a) If the device identifier has length less than or equal to 32 bytes, then the DEVICE IDENTIFIER field shall be set to the value of the device identifier in the most significant bytes of the field and the remainder of the field shall be padded with zero in the least significant bytes. The DEVICE IDENTIFIER LENGTH field shall be set to the length of the device identifier; or
- b) If the device identifier has length greater than 32 bytes, then the DEVICE IDENTIFIER field shall be set to the 32 most significant bytes of the identifier The DEVICE IDENTIFIER LENGTH field shall be set to 32.

If no device identifier has been established by a SET DEVICE IDENTIFIER command, then the DEVICE IDENTIFIER LENGTH field shall be set to zero and the DEVICE IDENTIFIER field shall have all bytes set to zero.

If the PERIPHERAL DEVICE TYPE field contains any value other than 0h, 4h, or 7h, the DEVICE-TYPE SPECIFIC DATA field shall not be present in the Logical Unit descriptor.

The Logical Unit descriptor shall include the DEVICE-TYPE SPECIFIC DATA field if:

- a) The PERIPHERAL DEVICE TYPE field contains 0h, 4h, or 7h;
- b) The logical unit supports the READ CAPACITY command (see SBC-2) with:
 - A) The RELADR bit set to zero; and

- B) The PMI bit set to zero; and
- c) The logical unit standard INQUIRY data (see 7.z.z) has the RMB bit set to zero.

If the Logical Unit descriptor includes the DEVICE-TYPE SPECIFIC DATA field, then the size of the DEVICE-TYPE SPECIFIC DATA field shall be 12 bytes and the field shall contain the same as the data that would be returned by a successful READ CAPACITY command with LONGLBA bit set to one, and the RELADR and PMI bits set to zero.

7.1.4 REPORT ACCESS CONTROLS LOG service action

7.1.4.1 REPORT ACCESS CONTROLS LOG introduction

The ACCESS CONTROL IN command with REPORT ACCESS CONTROLS LOG service action (see table t22) is used to obtain the access controls log (see 5.99.9). If the ACCESS CONTROL IN command is implemented, the REPORT ACCESS CONTROLS LOG service action shall be implemented.

Table t22 — ACCESS CONTROL IN command with REPORT ACCESS CONTROLS LOG service action

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (86h)							
1	Reserved			SERVICE ACTION (02h)				
2	(MSB) _____							
9	MANAGEMENT IDENTIFIER KEY							(LSB)
10	Reserved					LOG PORTION		
11	Reserved							
12	(MSB) _____							
13	ALLOCATION LENGTH							(LSB)
14	Reserved							
15	CONTROL							

If access controls are disabled, the device server shall ignore the MANAGEMENT IDENTIFIER KEY field and shall respond with GOOD status returning only the eight byte parameter list header as specified in 7.1.4.2.1 subject to the ALLOCATION LENGTH limitation described in 4.3.4.6. If access controls are enabled and table t23 specifies that the management identifier key is not required then the device server shall ignore the contents of the MANAGEMENT IDENTIFIER KEY field.

If access controls are enabled, table t23 specifies that the management key identifier is required and the contents of the MANAGEMENT IDENTIFIER KEY field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, parameter data shall not be returned, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

The LOG PORTION field (see table t23) specifies the access controls log portion being requested .

Table t23 — CDB LOG PORTION field values

Log Portion	Description	Management Identifier Key Required
00b	Key Overrides portion	No
01b	Invalid Keys portion	Yes
10b	ACL LUN Conflicts portion	Yes
11b	Reserved	

The ALLOCATION LENGTH field is described in 4.3.4.6. The ALLOCATION LENGTH field value should be at least eight.

7.1.4.2 REPORT ACCESS CONTROLS LOG parameter data format

7.1.4.2.1 REPORT ACCESS CONTROLS LOG parameter data introduction

The format of the parameter data returned in response to an ACCESS CONTROL IN command with REPORT ACCESS CONTROLS LOG service actions is shown in table t24.

Table t24 — ACCESS CONTROL IN with REPORT ACCESS CONTROLS LOG parameter data format

Bit Byte	7	6	5	4	3	2	1	0
	Parameter list header							
0	(MSB)	LOG LIST LENGTH (n-3)						(LSB)
3		Reserved						
4		Reserved				LOG PORTION		
5		COUNTER						
6	(MSB)	Access Controls Log pages						
7		Access Controls Log page 0						(LSB)
		:						
		:						
		Access Controls Log page x						
n		Access Controls Log page x						

The LOG LIST LENGTH field shall contain a count of the number of bytes in the remaining parameter data. The value in the LOG LIST LENGTH field shall be the actual number of bytes available without consideration for insufficient allocation length in the CDB. If access controls are disabled, the LOG LIST LENGTH field shall be set to eight.

The LOG PORTION field (see table t25) indicates the access controls log portion being returned, the contents of the COUNTER field, and the type of Access Controls Log pages being returned.

Table t25 — Parameter data LOG PORTION field values

Log Portion	Access Controls Log Portion Being Returned	COUNTER Field Contents	Access Controls Log Page Format Reference
00h	Key Overrides portion	Key Overrides counter	7.1.4.2.2
01h	Invalid Keys portion	Invalid Keys counter	7.1.4.2.3
02h	ACL LUN Conflicts portion	ACL LUN Conflicts counter	7.1.4.2.4
11b	Reserved		

The COUNTER field contains the events counter value (see 5.99.9) for the access controls log portion indicated by the LOG PORTION field (see table t25).

The format of the Access Controls Log pages is indicated by the value in the LOG PORTION field (see table t25). All the Access Controls Log pages returned in a single parameter list shall have the same format. If the access controls coordinator does not support Access Controls Log pages in the portion of the access controls log indicated by the LOG PORTION field, the parameter data shall only contain the parameter list header .

7.1.4.2.2 Key Overrides Access Controls Log page format

The Key Overrides Access Controls Log page (see table t26) contains details of recently recorded attempts to override the management identifier key (see 5.99.9) using the ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action (see 7.2.8), whether those attempts were successful or not.

Table t26 — Key Overrides Access Controls Log page format

Bit Byte	7	6	5	4	3	2	1	0	
0	Reserved								
2	Reserved								
3	Reserved							SUCCESS	
4	(MSB)	TIME STAMP							(LSB)
7								(LSB)	
8	(MSB)	TRANSPORTID							(LSB)
31								(LSB)	
32	(MSB)	INITIAL OVERRIDE LOCKOUT TIMER							(LSB)
33								(LSB)	
34	(MSB)	OVERRIDE LOCKOUT TIMER							(LSB)
35								(LSB)	

A SUCCESS bit of one indicates that the specific ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action event recorded in the access controls log successfully overrode the management identifier key . A value of zero indicates that the command did not succeed.

The TIME STAMP field shall contain zero or an indication of the time at which the ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action was processed as described in 5.99.9.

The **TRANSPORTID** field shall contain the TransportID of the initiator that issued the command.

The INITIAL OVERRIDE LOCKOUT TIMER field shall contain the access controls coordinator’s initial override lockout timer value (see 5.99.7.2.2) at time at which the ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action was processed. The OVERRIDE LOCKOUT TIMER field shall contain the access controls coordinator’s override lockout timer value (see 5.99.7.2.2) at time at which the ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action was processed.

7.1.4.2.3 Invalid Keys Access Controls Log page format

The Invalid Keys Access Controls Log page (see table t27) contains details of recently recorded receipts of ACCESS CONTROL IN or ACCESS CONTROL OUT commands specifying an incorrect management identifier key (see 5.99.9).

Table t27 — Invalid Keys Access Controls Log page format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	OPERATION CODE							
3	Reserved			SERVICE ACTION				
4	(MSB)	TIME STAMP						(LSB)
7								
8	(MSB)	TRANSPORTID						(LSB)
31								
32	(MSB)	INVALID MANAGEMENT IDENTIFIER KEY						(LSB)
39								

The OPERATION CODE and SERVICE ACTION fields shall be set to the respective values from the CDB of the access controls command that specified the invalid management identifier key whose value is found in the INVALID MANAGEMENT IDENTIFIER KEY field.

The TIME STAMP field shall contain zero or an indication of the time at which the ACCESS CONTROL IN or ACCESS CONTROL OUT command was processed as described in 5.99.9.

The **TRANSPORTID** field shall contain the TransportID of the initiator that issued the command.

The INVALID MANAGEMENT IDENTIFIER KEY field shall be set to the value of the invalid management identifier key detected by the access controls coordinator in the command or associated parameter data.

NOTE 6 - The management identifier key is typically in the CDB for ACCESS CONTROL IN commands and in the parameter data for ACCESS CONTROL OUT commands.

7.1.4.2.4 ACL LUN Conflicts Access Controls Log page format

The ACL LUN Conflicts Access Controls Log page (see table t28) contains details of recently recorded ACL LUN (see 5.99.9) encountered by the access controls coordinator when a previously not-enrolled initiator sends an ACCESS CONTROL OUT command with ACCESS ID ENROLL service action (see 7.2.4).

Table t28 — ACL LUN Conflicts Access Controls Log page format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							
3	Reserved							
4	(MSB)	TIME STAMP						(LSB)
7								
8	(MSB)	TRANSPORTID						(LSB)
31								
32	(MSB)	ACCESSID						(LSB)
55								

The TIME STAMP field shall contain zero or an indication of the time at which the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action was processed as described in 5.99.9.

The TRANSPORTID field shall contain the TransportID of the initiator that issued the command.

Editors Note 2 - ROW: I believe that the preceding paragraph is incorrect because some ACL LUN conflict events occur as the result of a proxy LUN. Therefore, making reference to an ACL entry (presumably an ACE) is incorrect because some ACL LUN conflict events do not involve an ACE. I have used the wording from other Access Control Log page formats because it seems to correctly cover all cases.

The ACCESSID field shall be set to the AccessID that the initiator attempted to enroll. This shall correspond to an access identifier in ACL entry at the time the ACL LUN conflict event occurred.

7.1.5 REPORT OVERRIDE LOCKOUT TIMER service action

The [ACCESS CONTROL IN](#) command with REPORT OVERRIDE LOCKOUT TIMER service action (see table t29) is used query the state of the override lockout timer (see 5.99.7.2.2). If the ACCESS CONTROL IN command is implemented, the REPORT OVERRIDE LOCKOUT TIMER service action shall be implemented.

Table t29 — ACCESS CONTROL IN command with REPORT OVERRIDE LOCKOUT TIMER service action

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (86h)							
1	Reserved			SERVICE ACTION (03h)				
2	(MSB)	MANAGEMENT IDENTIFIER KEY						(LSB)
9								
10	(MSB)	ALLOCATION LENGTH						(LSB)
13								
14	Reserved							
15	CONTROL							

Editors Note 3 - ROW: If access controls are disabled, the command shall be terminated with a CHECK CONDITION status, setting the sense key to ILLEGAL REQUEST My understanding of the principles of SCSI suggests that returning GOOD status on an ACCESS CONTROLS IN command without returning any parameter data violates the meaning of GOOD status.

If access controls are enabled and the contents of the MANAGEMENT IDENTIFIER KEY field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, parameter data shall not be returned, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

The ALLOCATION LENGTH field is described in [4.3.4.6](#). The ALLOCATION LENGTH field value should be at least eight.

If access controls are enabled, the parameter data returned by the [ACCESS CONTROL IN](#) command with REPORT OVERRIDE LOCKOUT TIMER service action shall have the format shown in table t30.

Table t30 — ACCESS CONTROL IN with REPORT OVERRIDE LOCKOUT TIMER parameter data

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB)	CURRENT OVERRIDE LOCKOUT TIMER						(LSB)
3								
4	(MSB)	INITIAL OVERRIDE LOCKOUT TIMER						(LSB)
5								
6	(MSB)	KEY OVERRIDES COUNTER						(LSB)
7								

The CURRENT OVERRIDE LOCKOUT TIMER field shall be set to the current value of the [override lockout timer](#) (see [5.99.7.2.2](#)).

The INITIAL OVERRIDE LOCKOUT TIMER field shall be set to the value of the [initial override lockout timer](#) (see [5.99.7.2.2](#)) as established by the last successful ACCESS CONTROL OUT command with MANAGE OVERRIDE LOCKOUT TIMER service action (see [7.2.7](#)).

The KEY OVERRIDES COUNTER field shall be set to the value of the [key overrides counter](#) in the access controls log (see [5.99.9](#)).

7.1.6 REQUEST PROXY TOKEN service action

The **ACCESS CONTROL IN command with REQUEST PROXY TOKEN service action** (see table t31) is used to obtain a proxy token (see 5.99.5.2) for a logical unit to which that initiator has non-proxy access rights. The proxy token thus obtained may be used to pass temporary access to the logical unit to a third party via other proxy related service actions of the ACCESS CONTROL IN and ACCESS CONTROL OUT commands. If the **ACCESS CONTROL IN command with REQUEST PROXY TOKEN** service action is not supported, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

Table t31 — ACCESS CONTROL IN command with REQUEST PROXY TOKEN service action

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (86h)							
1	Reserved			SERVICE ACTION (04h)				
2	(MSB)	LUN VALUE						(LSB)
9								
10	(MSB)	ALLOCATION LENGTH						(LSB)
13								
14	Reserved							
15	CONTROL							

Editors Note 4 - ROW: If access controls are disabled, the command shall be terminated with a CHECK CONDITION status, setting the sense key to ILLEGAL REQUEST My understanding of the principles of SCSI suggests that returning GOOD status on an ACCESS CONTROLS IN command without returning any parameter data violates the meaning of GOOD status.

NOTE 7 - If access controls are disabled, all logical units are accessible and all initiators share the same LUN values for addressing. A proxy token is not needed because sharing LUN values is sufficient.

The **LUN VALUE** field shall contain the LUN value the initiator uses to access the logical unit for which the proxy token is requested.

If the **LUN value** corresponds to a logical unit that is accessible to the requesting initiator either through a TransportID or through the AccessID under which the initiator is currently in the enrolled state (see 5.99.4.1), and the access controls coordinator has sufficient resources to create and manage a new proxy token, then the parameter data shown in table t32 shall be returned.

If the **LUN value** does not correspond to an accessible logical unit, parameter data shall not be returned and the command shall be terminated as follows:

- a) If the **LUN value**:
 - A) Does not correspond to an accessible logical unit; or
 - B) Corresponds to a logical unit accessible only through a proxy token;
 Then the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - INVALID LU IDENTIFIER; or

- b) If the LUN value corresponds to a logical unit accessible only through an enrolled AccessID and the initiator is in the pending-enrolled state, then the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - INITIATOR PENDING-ENROLLED.

If the access controls coordinator does not have enough resources to create and manage a new proxy token, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INSUFFICIENT ACCESS CONTROL RESOURCES.

The ALLOCATION LENGTH field is described in 4.3.4.6. The ALLOCATION LENGTH field value should be at least eight.

The format of the parameter data returned by the ACCESS CONTROL IN command with REQUEST PROXY TOKEN service action is shown in table t32.

Table t32 — ACCESS CONTROL IN with REQUEST PROXY TOKEN parameter data

Bit Byte	7	6	5	4	3	2	1	0	
0	(MSB)								
7	PROXY TOKEN								(LSB)

7.2 ACCESS CONTROL OUT Command

7.2.1 ACCESS CONTROL OUT introduction

The service actions of the ACCESS CONTROL OUT command (see Table 25) are used to request service actions by the access controls coordinator to limit or grant access to the logical units to initiators. If the ACCESS CONTROL OUT command is implemented, the ACCESS CONTROL IN command also shall be implemented. The ACCESS CONTROL OUT command shall not be affected access controls.

Table t33 — ACCESS CONTROL OUT service actions

Service Action	Command name	Type	Reference
00h	MANAGE ACL	m	7.2.2
01h	DISABLE ACCESS CONTROLS	m	7.2.3
02h	ACCESS ID ENROLL	m	7.2.4
03h	CANCEL ENROLLMENT	m	7.2.5
04h	CLEAR ACCESS CONTROLS LOG	m	7.2.6
05h	MANAGE OVERRIDE LOCKOUT TIMER	m	7.2.7
06h	OVERRIDE MGMT ID KEY	m	7.2.8
07h	REVOKE PROXY TOKEN	o	7.2.9
08h	REVOKE ALL PROXY TOKENS	o	7.2.10
09h	ASSIGN PROXY LUN	o	7.2.11
0Ah	RELEASE PROXY LUN	o	7.2.12
0Bh - 17h	Reserved		
18h - 1Fh	Vendor specific		
Key: m = Service action implementation is mandatory if ACCESS CONTROL OUT is implemented. o = Service action implementation is optional.			

The CDB format used by all ACCESS CONTROL OUT service actions is shown in table t34.

Table t34 — ACCESS CONTROL OUT command format

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (87h)							
1	Reserved			SERVICE ACTION (see table t33)				
2	Reserved							
9	Reserved							
10	(MSB)	PARAMETER LIST LENGTH						(LSB)
13	Reserved							
14	Reserved							
15	CONTROL							

If the device contains an access controls coordinator, the ACCESS CONTROL OUT command shall be processed by the access controls coordinator if addressed to LUN 0. The ACCESS CONTROL OUT command also may be addressed to any other LUN value whose standard INQUIRY data (see 7.z.z) has the ACC bit set to one, in which case it shall be processed in the same manner as if the command had been addressed to LUN 0. If an ACCESS CONTROL OUT command is received by a device server whose standard INQUIRY data has the ACC bit set to zero, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID COMMAND OPERATION CODE .

The PARAMETER LIST LENGTH field indicates the amount of data that the initiator shall send to the access controls coordinator in the Data-Out buffer. The format of the parameter list is specific to each service action.

7.2.2 MANAGE ACL service action

7.2.2.1 MANAGE ACL introduction

The ACCESS CONTROL OUT command with MANAGE ACL service action is used to authorize access or revoke access to a logical unit or logical units by initiators. The ACCESS CONTROL OUT command with MANAGE ACL service action adds, changes or removes an entry or multiple entries in the access controls coordinator's ACL (see 5.99.2). If the ACCESS CONTROL OUT command is implemented, the MANAGE ACL service action shall be implemented.

The format of the CDB for the ACCESS CONTROL OUT command with MANAGE ACL service action is shown in table t34 (see 7.2.1).

Editors Note 5 - ROW: The way the following paragraph is written (before editing), the ACCESS CONTROL OUT command with MANAGE ACL service action cannot be used enable access controls.

If ~~access controls are disabled or if~~ the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is less than 20 or results in truncation of any ACE page (see table t36) 6.2.2.2, then the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the access controls coordinator cannot complete the **ACCESS CONTROL OUT** command with **MANAGE ACL service action** because it has insufficient resources, the access controls coordinator shall take no action and not change any of its state and the command shall be terminated with a **CHECK CONDITION** status, the sense key shall be set to **ILLEGAL REQUEST** and the additional sense code shall be set to **INSUFFICIENT ACCESS CONTROL RESOURCES**.

The format of the parameter data for the **ACCESS CONTROL OUT** command with **MANAGE ACL service action** is shown in table t35.

Table t35 — ACCESS CONTROL OUT with MANAGE ACL parameter data format

Bit Byte	7	6	5	4	3	2	1	0
Parameter list header								
0	Reserved							
3	Reserved							
4	(MSB) MANAGEMENT IDENTIFIER KEY (LSB)							
11	(MSB) NEW MANAGEMENT IDENTIFIER KEY (LSB)							
12	(MSB) NEW MANAGEMENT IDENTIFIER KEY (LSB)							
19	(MSB) NEW MANAGEMENT IDENTIFIER KEY (LSB)							
20	Reserved							
21	FLUSH	Reserved						
22	Reserved							
23	Reserved							
24	(MSB) DLGENERATION (LSB)							
27	(MSB) DLGENERATION (LSB)							
ACE pages								
28	ACE page 0							
	⋮							
	ACE page x							
n	ACE page x							

If access controls are enabled and the contents of the **MANAGEMENT IDENTIFIER KEY** field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, the access controls coordinator's state shall not be altered, the command shall be terminated with a **CHECK CONDITION** status, the sense key shall be set to **ILLEGAL REQUEST**, the additional sense code shall be set to **ACCESS DENIED - INVALID MGMT ID KEY**, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

If the contents of the **MANAGEMENT IDENTIFIER KEY** field match the current management identifier key maintained by the access controls coordinator, the access controls coordinator shall set its management identifier key to the value specified in the **NEW MANAGEMENT IDENTIFIER KEY** field and if access controls are disabled it shall enable them .

The FLUSH bit of one instructs the access controls coordinator to **place** every initiator in the enrolled state into the pending-enrolled state (see 5.99.4.1.4).

The DLGENERATION field specifies the DLgeneration value associated with the default LUN values in the Grant/Revoke ACE pages in the parameter data.

The ACE pages that may follow in the parameter list provide additional changes to the ACL. Each ACE page describes one ACE in the ACL that is to be added, modified, or removed. The content and format of an ACE page is indicated by a page code (see table t36).

Table t36 — ACE page codes

Page Code	Description	Reference
00h	Grant/Revoke	7.2.2.2
01h	Grant All	7.2.2.3
02h	Revoke Proxy Token	7.2.2.4
03h	Revoke All Proxy Tokens	7.2.2.5
04h-EFh	Reserved	
F0h-FFh	Vendor-specific	

Editors Note 6 - ROW: MANAGE ACL Grant/Revoke ACE pages can cause ACL LUN conflicts (see 5.99.4.2) by adding LUN values that are already in use by some initiators via other ACEs or proxy LUNs. This condition is not covered in 5.99.4.2 or here. My understanding is that the authors' intention was for such ACL LUN conflicts to result in termination of the ACCESS CONTROL OUT command with MANAGE ACL service action.

The following requirements apply to the processing of changes to the access control state :

- a) No change to the access control state shall occur if the ACCESS CONTROL OUT command with MANAGE ACL service action terminates with a status other than GOOD status; and
- b) If the ACCESS CONTROL OUT command with MANAGE ACL service action completes with a GOOD status, the following shall have been performed as a single indivisible event:
 - 1) Changes resulting from the contents of fields in the parameter list header shall be processed; and
 - 2) Changes resulting from the contents of ACE pages shall be processed;
 - a) Multiple ACE pages shall be processed sequentially;
 - b) If an ACE page contains conflicting instructions in LUACD descriptors, the instructions in the last LUACD descriptor within the page shall take precedence; and
 - c) If an ACE containing an AccessID type access identifier (see 5.99.2.2.2) is replaced and the ACE page that caused the change has the NOCNCL bit (see 7.2.2.2) set to zero, then any initiator in the enrolled or pending-enrolled state under the AccessID in that ACE shall be placed in the not-enrolled state (see 5.99.4.1.2).

An ACE page contains conflicting instructions if either of the following is true:

- a) Two LUACD descriptors are present with the same LUN value and different default LUN values; or
- b) Two LUACD descriptors are present with different LUN values and the same default LUN value.

7.2.2.2 The Grant/Revoke ACE page

The Grant/Revoke ACE page (see table t37) is used to add, modify, or remove an ACE from the ACL (see 5.99.2).

Table t37 — Grant/Revoke ACE page format

Bit Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (00h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (n-3)						(LSB)
3								
4	NOCNCL	Reserved						
5	ACCESS IDENTIFIER TYPE							
6	(MSB)	ACCESS IDENTIFIER LENGTH (m-7)						(LSB)
7								
8	ACCESS IDENTIFIER							
m								
LUACD Descriptors								
m+1	LUACD descriptor 0							
m+20								
	⋮							
n-19	LUACD descriptor x							
n								

The PAGE LENGTH field specifies the number of additional bytes present in this page.

A NOCNCL (no changes to current logical unit access) bit of one specifies that the application client believes that this ACE page makes no changes to the existing logical unit access conditions in the ACL. A NOCNCL bit of zero specifies that the ACE page may or may not change existing logical unit access conditions. If the ACCESS IDENTIFIER TYPE specifies a TransportID (see 7.1.2.2.2), the NOCNCL bit shall be ignored.

The ACCESS IDENTIFIER TYPE and ACCESS IDENTIFIER length fields are described in 7.1.2.2.2.

The ACCESS IDENTIFIER field contains the identifier that the access controls coordinator uses to select the ACE that is to be added, modified, or removed. The format of the ACCESS IDENTIFIER field is specified in table t12 (see 7.1.2.2.2).

Any of the following conditions in the parameter header or any Grant/Revoke ACE page or Grant All ACE page shall cause the access coordinator to not change its state and shall cause the command to be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST :

- a) The contents of the DLGENERATION field in the parameter list header (see 7.2.2.1) do not match the current DLgeneration value (see 5.99.3.4) maintained by the access controls coordinator;
- b) An ACCESS IDENTIFIER TYPE field that specifies an unsupported value;

- c) An ACCESS IDENTIFIER TYPE that contains 01h (see 5.99.2.2) with an ACCESS IDENTIFIER field that contains an invalid TransportID (see 5.99.2.2.3) as defined for the applicable protocol standard; or
- d) Two ACE pages that have the same values in the ACCESS IDENTIFIER TYPE and ACCESS IDENTIFIER fields.

NOTE 8 - The application client is responsible for obtaining the current association of default LUN values to logical units (and the DLgeneration value for that association) prior to issuing this service action. The ACCESS CONTROL IN command with REPORT LU DESCRIPTORS service action (see 7.1.3) returns the necessary information.

Each LUACD descriptor (see table t38) describes the access to be allowed to one logical unit based on the access identifier in the ACE page. An ACE page may contain zero or more LUACD descriptors.

Table t38 — ACE page LUACD descriptor format

Bit Byte	7	6	5	4	3	2	1	0	
0	ACCESS MODE								
1	Reserved								
3	Reserved								
4	(MSB)	LUN VALUE							
11							(LSB)		
12	(MSB)	DEFAULT LUN							
19							(LSB)		

The ACCESS MODE field is described in 7.1.2.2.2.

The LUN VALUE field specifies the LUN value an accessing initiator uses to access the logical unit to which the LUACD descriptor applies.

The DEFAULT LUN field specifies the logical unit to which the value in the LUN VALUE allows access. The DEFAULT LUN field shall contain a default LUN value (see 5.99.3.3). The value in the DEFAULT LUN field shall be consistent with the DLGENERATION field contents specified in the parameter list header (see 7.2.2.1).

If the specified access mode is not supported or if the DEFAULT LUN field contains value that is not valid or the LUN VALUE field contains a value that the access controls coordinator does not support as a valid LUN, the access controls coordinator's state shall not be modified and the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID LU IDENTIFIER, and the SENSE-KEY SPECIFIC field shall be set as described for the ILLEGAL REQUEST sense key in 7.2.2. If the error is an unsupported value in the LUN VALUE field, the first eight bytes of the additional sense bytes should contain a suggested LUN value that the access controls coordinator supports.

Based on the access identifier and the presence or absence of LUACD descriptors, the access controls coordinator shall add, modify, or remove an ACE in the ACL as shown in table t39.

Table t39 — Access Coordinator Grant/Revoke ACE page actions

		ACL already contains an ACE with the access identifier matching the one in the ACE page?	
		Yes	No
ACE page includes LUCAD descriptors?	Yes	Modify the existing ACE in the ACL.	Add a new ACE to the ACL.
	No	Remove the existing ACE from the ACL.	Take no action, this shall not be considered a error.

If the ACCESS IDENTIFIER TYPE indicates type AccessID, the enrollment state (see 5.99.4.1) of any initiator that is enrolled under the specified AccessID, shall be affected as follows:

- a) If the ACE containing the AccessID is removed, the initiator shall be placed in the not-enrolled state; or
- b) If the ACE containing the AccessID is modified by a Grant/Revoke ACE page or a Grant All ACE page, then;
 - A) If the NOCNCL bit is zero in that ACE page, the initiator shall be placed in the not-enrolled state; or
 - B) If the NOCNCL bit is one in that ACE page, the enrollment state of the initiator may be left unchanged or the initiator may be placed in the not-enrolled state (see 5.99.4.1.2).

7.2.2.3 The Grant All ACE page

The Grant All ACE page (see table t40) is used to add or modify an ACE from the ACL (see 5.99.2). An ACE added or modified using the Grant All ACE page allows initiators with the specified access identifier to access the SCSI target device as if access controls were disabled.

Table t40 — Grant All ACE page format

Bit Byte	7	6	5	4	3	2	1	0
0	PAGE CODE (01h)							
1	Reserved							
2	(MSB)	PAGE LENGTH (n-3)						(LSB)
3								
4	NOCNCL	Reserved						
5	ACCESS IDENTIFIER TYPE							
6	(MSB)	ACCESS IDENTIFIER LENGTH (m-7)						(LSB)
7								
8	ACCESS IDENTIFIER							
n								

The PAGE LENGTH, ACCESS IDENTIFIER TYPE, ACCESS IDENTIFIER LENGTH, and ACCESS IDENTIFIER fields are defined in 7.2.2.3.

When an existing ACE that was created or modified using the Grant/Revoke ACE page is modified by a Grant All ACE page or when an existing ACE that was created or modified using the Grant All ACE page is modified by a Grant/Revoke ACE page, the modification shall be processed as if the Grant All ACE page is or was a Grant/Revoke ACE page with one LUACD descriptor for every logical unit managed by the access controls coordinator with the fields in each LUACD containing:

- a) An access mode of 00h (see 7.1.2.2.2);
- b) A LUN VALUE field whose contents match the contents of the DEFAULT LUN field; and
- c) A DEFAULT LUN field whose contents reference the logical unit appropriate to the DLgeneration value (see 5.99.3.3).

7.2.2.4 The Revoke Proxy Token ACE page

The Revoke Proxy Token ACE page (see table t41) is used to revoke one or more proxy tokens (see 5.99.5.2).

Table t41 — Revoke Proxy Token ACE page format

Bit Byte	7	6	5	4	3	2	1	0	
0	PAGE CODE (02h)								
1	Reserved								
2	(MSB)	PAGE LENGTH (n-3)							
3								(LSB)	
4	PROXY TOKEN 0								
11	:								
n-7	PROXY TOKEN x								
n									

The PAGE LENGTH field specifies the number of additional bytes present in this page.

The one or more PROXY TOKEN field(s) specify the proxy tokens to be revoked. The access controls coordinator shall revoke each proxy token listed in a PROXY TOKEN field. If the contents of a PROXY TOKEN field do not identify a valid proxy token the field shall be ignored, this shall not be considered an error.

Multiple Revoke Proxy Token ACE pages may be included in the parameter data.

7.2.2.5 The Revoke All Proxy Tokens ACE page

The Revoke All Proxy Tokens ACE page (see table t41) is used to revoke all currently valid proxy tokens (see 5.99.5.2).

Table t42 — Revoke All Proxy Tokens ACE page format

Bit Byte	7	6	5	4	3	2	1	0	
0	PAGE CODE (03h)								
1	Reserved								
2	(MSB)	PAGE LENGTH (0000h)							
3								(LSB)	

Multiple Revoke ALL Proxy Tokens ACE pages may be included in the parameter data.

7.2.3 DISABLE ACCESS CONTROLS service action

The ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action is used to place the access controls coordinator in access controls disabled state. If the ACCESS CONTROL OUT command is implemented, the DISABLE ACCESS CONTROLS service action shall be implemented.

The format of the CDB for the ACCESS CONTROL OUT command with DISABLE ACCESS CONTROLS service action is shown in table t34 (see 7.2.1).

If access controls are disabled or if the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor 12, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is 12, the parameter list shall have the format shown in table t43.

Table t43 — ACCESS CONTROL OUT with DISABLE ACCESS CONTROLS parameter data format

Bit Byte	7	6	5	4	3	2	1	0	
0	Reserved								
3	Reserved								
4	(MSB)	MANAGEMENT IDENTIFIER KEY							
11								(LSB)	

If access controls are enabled and the contents of the MANAGEMENT IDENTIFIER KEY field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, the access controls coordinator's states shall not be altered, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

...

In response to a **ACCESS CONTROL OUT** command with **DISABLE ACCESS CONTROLS** service action with correct management identifier key value the access controls coordinator shall:

- a) Disable access controls;
- b) Clear the ACL (see 5.99.2);
- c) Place all initiators into the not-enrolled state (see 5.99.4.1);
- d) Set the management identifier key to zero (see 5.99.7);
- e) Set the override lockout timer to zero (see 5.99.7.2.2);
- f) Set the initial override lockout timer value to zero (see 5.99.7.2.2);
- g) Clear the access controls log (including resetting counters to zero) with the exception of the key overrides portion of the access controls log (see 5.99.9);
- h) Allow all initiator's access to all logical units at their default LUN value; and
- i) Optionally, reset the DLgeneration value to zero (see 5.99.3.4).

7.2.4 ACCESS ID ENROLL service action

The ACCESS ID ENROLL service action of the ACCESS CONTROL OUT command is used by an initiator to enroll an AccessID with the access controls coordinator. If the ACCESS CONTROL OUT command is implemented, the ACCESS ID ENROLL service action shall be implemented.

The format of the CDB for the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action is shown in table t34 (see 7.2.1).

If access controls are disabled or if the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor 24, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is 24, the parameter list shall have the format shown in table t44.

Table t44 — ACCESS CONTROL OUT with ACCESS ID ENROLL parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	ACCESSID							
15	ACCESSID							
16 (MSB)	Reserved							
23	Reserved (LSB)							

The AccessID field is described in 5.99.2.2.2.

If the initiator is in the enrolled or pending-enrolled state (see 5.99.4.1) under a given AccessID and the ACCESSID field contains a different AccessID, the access controls coordinator shall place the initiator in the pending-enrolled state, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - ENROLLMENT CONFLICT.

If the initiator is in the enrolled or pending-enrolled state under a given AccessID and the ACCESSID field contains a matching AccessID, the access controls coordinator shall place the initiator in the enrolled state and make no other changes .

If the initiator is in the not-enrolled state and the ACCESSID field contents do not match the AccessID in any ACE in the ACL (see 5.99.2) , the initiator shall remain in the not-enrolled state and the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - NO ACCESS RIGHTS.

If the initiator is in the not-enrolled state and the ACCESSID field contents matches the AccessID in any ACE in the ACL the actions taken depend on whether enrolling the initiator would create an ACL LUN conflict (see 5.99.4.2). If there is no ACL LUN conflict, the initiator shall be placed in the enrolled state (see 5.99.4.1.3). If there is an ACL LUN conflict, the initiator shall remain in the not-enrolled state and the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - ACL LUN CONFLICT and the event shall be recorded in the ACL LUN conflicts portion of the access controls log (see 5.99.9).

NOTE 9 - An initiator that receives the ACCESS DENIED - ACL LUN CONFLICT additional sense code should remove any proxy access rights it has acquired using the ACCESS CONTROL OUT command with RELEASE PROXY LUN service action and retry the enrollment request. If the ACL LUN conflict resulted from proxy access, the retried enrollment succeeds. Otherwise, the mechanisms for resolving ACL LUN conflicts are outside the scope of this standard.

7.2.5 CANCEL ENROLLMENT service action

The ACCESS CONTROL OUT command with CANCEL ENROLLMENT service action is used to remove an initiator's enrollment with the access controls coordinator (see 5.99.4). Successful completion of this command changes the state of the initiator to the not-enrolled state. If the ACCESS CONTROL OUT command is implemented, the CANCEL ENROLLMENT service action shall be implemented.

The ACCESS CONTROL OUT command with CANCEL ENROLLMENT service action should be used by an initiator prior to any period where use of its accessible logical units may be suspended for a lengthy period of time (e.g., when a host is preparing to shutdown). This allows the access controls coordinator to free any resources allocated to manage the enrollment for that initiator.

The format of the CDB for the ACCESS CONTROL OUT command with ACCESS ID ENROLL service action is shown in table t34 (see 7.2.1).

If access controls are disabled, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

There is no parameter data for the ACCESS CONTROL OUT command with CANCEL ENROLLMENT service action. If the PARAMETER LIST LENGTH field in the CDB is not set to zero, the initiator's enrollment shall not be changed and the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the PARAMETER LIST LENGTH field in the CDB is set to zero, the initiator shall be placed in the not-enrolled state (see 5.99.4.1.2) Any subsequent commands addressed to the logical units no longer accessible are handled according to the rules stated in 5.99.6.

7.2.6 CLEAR ACCESS CONTROLS LOG service action

The ACCESS CONTROL OUT command with CLEAR ACCESS CONTROLS LOG service action is used to instruct the access controls coordinator to reset a specific access control log counter to zero and to clear a portion

of the access controls log (see 5.99.9). If the ACCESS CONTROL OUT command is implemented, the CLEAR ACCESS CONTROLS LOG service action shall be implemented.

The format of the CDB for the ACCESS CONTROL OUT command with CLEAR ACCESS CONTROLS LOG service action is shown in table t34 (see 7.2.1).

If access controls are disabled or if the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor 12, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is 12, the parameter list shall have the format shown in table t45.

Table t45 — ACCESS CONTROL OUT with CLEAR ACCESS CONTROLS LOG parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							
2	Reserved							
3	Reserved						LOG PORTION	
4	(MSB)							
11	MANAGEMENT IDENTIFIER KEY (LSB)							

the shall be the shall be The LOG PORTION field (see table t46) specifies the access controls log portion to be cleared.

Table t46 — CLEAR ACCESS CONTROLS LOG LOG PORTION field values

Log Portion	Description
00b	Reserved
01b	Invalid Keys portion
10b	ACL LUN Conflicts portion
11b	Reserved

If access controls are enabled and the contents of the MANAGEMENT IDENTIFIER KEY field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, the access controls coordinator's states shall not be altered, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

In response to a ACCESS CONTROL OUT command with CLEAR ACCESS CONTROLS LOG service action with correct management identifier key value the access controls coordinator shall perform the following to clear the portion of the access controls log identified by the LOG PORTION field (see table t46) in the parameter data:

- a) Set the counter for the specified log portion to zero; and
- b) If the specified log portion contains details records, remove the detail records from the specified log portion.

7.2.7 MANAGE OVERRIDE LOCKOUT TIMER service action

The **ACCESS CONTROL OUT** command with MANAGE OVERRIDE LOCKOUT TIMER service action is used to manage the override lockout timer (see 5.99.7.2.2). If the **ACCESS CONTROL OUT** command is implemented, the **MANAGE OVERRIDE LOCKOUT TIMER** service action shall be implemented.

If access controls are disabled, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

The format of the CDB for the **ACCESS CONTROL OUT** command with **MANAGE OVERRIDE LOCKOUT TIMER** service action is shown in table t34 (see 7.2.1).

If the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall reset the override lockout timer to the current initial override lockout timer value maintained by the access controls coordinator .

If the value in the PARAMETER LIST LENGTH field is neither zero nor 12, the device server shall respond with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is 12, the parameter list shall have the format shown in table t47.

Table t47 — ACCESS CONTROL OUT with MANAGE OVERRIDE LOCKOUT TIMER parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB)	NEW INITIAL OVERRIDE LOCKOUT TIMER						(LSB)
3								
4	(MSB)	MANAGEMENT IDENTIFIER KEY						(LSB)
11								

The **NEW INITIAL OVERRIDE LOCKOUT TIMER** field specifies the value that access controls coordinator maintains for initial override lockout timer if the specified management identifier key is correct.

If access controls are enabled and the contents of the **MANAGEMENT IDENTIFIER KEY** field do not match the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator, the access controls coordinator shall not change the initial override lockout timer value but shall set the override lockout timer to the unaltered current initial override lockout timer value. The command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST, the additional sense code shall be set to ACCESS DENIED - INVALID MGMT ID KEY, and the event shall be recorded in the invalid keys portion of the access controls log (see 5.99.9).

In response to a **ACCESS CONTROL OUT** command with **MANAGE OVERRIDE LOCKOUT TIMER** service action with correct management identifier key value the access controls coordinator shall:

- a) Replace the currently saved initial override lockout timer with the value in the **NEW INITIAL OVERRIDE LOCKOUT TIMER** field ; and
- b) Set the override lockout timer to the new initial value.

7.2.8 OVERRIDE MGMT ID KEY service action

The **ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action** is used to override the current management identifier key (see 5.99.3.2) maintained by the access controls coordinator. The **ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action** is intended to be used in a failure situation where the application client no longer has access to its copy of this key. Successful use of the **ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action** is restricted by the override lockout timer (see 5.99.7.2.2). If the **ACCESS CONTROL OUT command** is implemented, the **OVERRIDE MGMT ID KEY service action** shall be implemented.

The format of the CDB for the **ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action** is shown in table t34 (see 7.2.1).

If access controls are disabled or if the **PARAMETER LIST LENGTH** field in the CDB is zero, the access controls coordinator shall take no action and **the command shall be completed** with a **GOOD** status.

If access controls are enabled, the access controls coordinator shall log every **ACCESS CONTROL OUT command with OVERRIDE MGMT ID KEY service action** processed whether successful or not in the access controls log as specified in 5.99.9.

If the value in the **PARAMETER LIST LENGTH** field is neither zero nor 12, the **command shall be terminated** with a **CHECK CONDITION** status, the sense key shall be set to **ILLEGAL REQUEST** and the additional sense code shall be set to **PARAMETER LIST LENGTH ERROR**.

If the value in the **PARAMETER LIST LENGTH** field is 12, the parameter data shall have the format shown in table t48.

Table t48 — ACCESS CONTROL OUT with OVERRIDE MGMT ID KEY parameter data format

Bit Byte	7	6	5	4	3	2	1	0	
0	Reserved								
3	Reserved								
4	(MSB)	NEW MANAGEMENT IDENTIFIER KEY							
11								(LSB)	

The **NEW MANAGEMENT IDENTIFIER KEY** field specifies a new management identifier key.

If the **override lockout timer** managed by the access controls coordinator is **not zero**, the access controls coordinator's states shall not be altered, the **command shall be terminated** with a **CHECK CONDITION** status, the sense key shall be set to **ILLEGAL REQUEST** and the additional sense code shall be set to **INVALID FIELD IN CDB**.

If the **override lockout timer** managed by the access controls coordinator is zero, then the access controls coordinator shall **replace** the current management identifier key with the value in the **NEW MANAGEMENT IDENTIFIER KEY** field.

7.2.9 REVOKE PROXY TOKEN service action

The **ACCESS CONTROL OUT command with REVOKE PROXY TOKEN service action** is used to cancel all proxy access rights to a logical unit that were granted to third parties under the specified proxy token (see 5.99.5.2). If this service action is not supported, the **command shall be terminated with a CHECK CONDITION** status, the sense key shall be set to **ILLEGAL REQUEST** and the additional sense code shall be set to **INVALID FIELD IN CDB**.

The format of the CDB for the ACCESS CONTROL OUT command with REVOKE PROXY TOKEN service action is shown in table t34 (see 7.2.1).

If access controls are disabled or if the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor eight, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is eight, the parameter data shall have the format shown in table t49.

Table t49 — ACCESS CONTROL OUT with REVOKE PROXY TOKEN parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)							
7	PROXY TOKEN						(LSB)	

If the PROXY TOKEN field does not contain a valid proxy token associated with any logical unit at the access controls coordinator, no further action is taken by the access controls coordinator. This shall not be considered an error.

If the proxy token is valid, the access controls coordinator shall take the following actions:

- a) Invalidate the proxy token; and
- b) Deny access to the associated logical unit by any initiator whose rights were granted under that proxy token via an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action (see 7.2.11) according to the rules stated in 5.99.6.

7.2.10 REVOKE ALL PROXY TOKENS service action

The ACCESS CONTROL OUT command with REVOKE ALL PROXY TOKENS service action is used to cancel all proxy access rights to a specified logical unit that were granted to third parties under any applicable proxy tokens (see 5.99.5.2). If this service action is not supported, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

The format of the CDB for the ACCESS CONTROL OUT command with REVOKE ALL PROXY TOKENS service action is shown in table t34 (see 7.2.1).

If access controls are disabled or if the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor eight, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is eight , the parameter data shall have the format shown in table t50.

Table t50 — ACCESS CONTROL OUT with REVOKE ALL PROXY TOKENS parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)							
7	LUN VALUE							(LSB)

If the LUN in the LUN VALUE field is not associated to a logical unit to which the requesting initiator has non-proxy access rights based on the contents of an ACE (see 5.99.2) or if the LUN value is based on a proxy token (see 5.99.5.2), no further action is taken by the access controls coordinator. This shall not be considered an error.

If the LUN value is associated to a logical unit to which the requesting initiator has non-proxy access rights, , the access controls coordinator shall take the following additional actions:

- a) Invalidate all proxy tokens associated to the logical unit specified by the LUN VALUE field ;
- b) Deny access to that logical unit by any initiator whose rights were granted under any of the invalidated proxy tokens via an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action (see 7.2.11) according to the rules stated in 5.99.6.

7.2.11 ASSIGN PROXY LUN service action

The ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action is used to request access to a logical unit under the rights of a proxy token (see 5.99.5.2) and to assign that logical unit a particular LUN value for addressing by the requesting initiator. If this service action is not supported , the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

The format of the CDB for the ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action is shown in table t34 (see 7.2.1).

If the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor 16, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is 16, the parameter data shall have the format shown in table t51.

Table t51 — ACCESS CONTROL OUT with ASSIGN PROXY LUN parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)							
7	PROXY TOKEN							(LSB)
8	(MSB)							
15	LUN VALUE							(LSB)

If the contents of the PROXY TOKEN field are not valid, then the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - INVALID PROXY TOKEN.

NOTE 10 - If access controls are disabled, there no valid proxy tokens and the device server always responds with the specified error information . This differs from the behavior of many other ACCESS CONTROL OUT service actions where the response is GOOD status when access controls are disabled. The difference in behavior is intended to inform the application client that its request for the new LUN assignment failed.

The LUN VALUE field specifies the LUN value the application client intends to use when accessing the logical unit described by the proxy token.

If the proxy token is valid but the access controls coordinator cannot assign the requested LUN value to the associated logical unit (e.g., because the LUN value already is associated with a logical unit for the initiator, or because the LUN value is not a supported logical unit address), access rights shall not be granted, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to ACCESS DENIED - INVALID LU IDENTIFIER, and the SENSE-KEY SPECIFIC field shall be set as described for the ILLEGAL REQUEST sense key in 7.2.2. The first eight bytes of the additional sense bytes should contain a suggested LUN value that the access controls coordinator supports

If the proxy token is valid but the access controls coordinator has insufficient resources to manage proxy logical unit access , the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INSUFFICIENT ACCESS CONTROL RESOURCES.

If the proxy token is valid and the access controls coordinator has sufficient resources, the initiator shall be allowed proxy access to the referenced logical unit at the specified LUN value .

7.2.12 RELEASE PROXY LUN service action (Optional)

The ACCESS CONTROL OUT command with RELEASE PROXY LUN service action is used to release proxy access to a logical unit created with a proxy token (see 5.99.5.2) and the ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action (see 7.2.11). If this service action is not supported , the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

The ACCESS CONTROL OUT command with RELEASE PROXY LUN service action should be used when an initiator no longer requires the logical unit access rights granted under a proxy token (e.g., when a copy manager has completed a specific third party copy operation under a proxy token). This allows the access controls coordinator to free any resources allocated to manage the proxy access .

The format of the CDB for the ACCESS CONTROL OUT command with RELEASE PROXY LUN service action is shown in table t34 (see 7.2.1).

If the PARAMETER LIST LENGTH field in the CDB is zero, the access controls coordinator shall take no action and the command shall be completed with a GOOD status.

If the value in the PARAMETER LIST LENGTH field is neither zero nor eight , the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to PARAMETER LIST LENGTH ERROR.

If the value in the PARAMETER LIST LENGTH field is eight , the parameter data shall have the format shown in table t52.

Table t52 — ACCESS CONTROL OUT with RELEASE PROXY LUN parameter data format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)							
7	LUN VALUE							(LSB)

The LUN VALUE field specifies a LUN value that was associated with a logical unit based on a proxy token using a ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action. If the LUN value was not assigned to a logical unit by an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action, the command shall be terminated with a CHECK CONDITION status, the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN PARAMETER LIST.

NOTE 11 - If access controls are disabled, there are no valid proxy tokens and therefore no LUN value could be assigned to a logical unit by an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action so the device server always responds with the specified error information . This differs from the behavior of many other ACCESS CONTROL OUT service actions where the response is GOOD status when access controls are disabled. The difference in behavior is intended to inform the application client that the LUN value remains as a valid address for the logical unit.

If the LUN value was assigned to a logical unit by an ACCESS CONTROL OUT command with ASSIGN PROXY LUN service action, the access controls coordinator shall disallow access to the logical unit at the specified LUN value .

F.8 – Protocol Specific Data

There is a proliferation of protocol specific command and parameter data that is being piled in SPC. Access controls is only the latest contributor to this onslaught.

The proposal here is to collect this data in a separate subclause in clause 8 by taking the following steps:

- a) Create a subclause 8.x titled "Protocol specific parameters";
- b) Create a subclause 8.x.a titled "EXTENDED COPY target descriptors" and move all the protocol specific target descriptors from their current location to 8.x.y;
- c) Create a subclause 8.x.b titled "Mode pages" and move the Disconnect-Reconnect mode page plus the two protocol specific mode pages to 8.x.b; and
- d) Create a subclause 8.x.c titled "Access controls TransportIDs" containing the subclauses shown here as 8.99.99...

8.99 Protocol specific parameters

8.99.1 Protocol specific parameters introduction

Some commands use protocol specific information in their CDBs or parameter lists. This subclause describes those protocol specific parameters. The descriptions in this subclause may be general, giving an overview to the protocol specific parameters as applied to all protocols or the descriptions may be specific to usage in a specific protocol. Each description includes a discussion of its scope.

In all cases, protocol specific parameter descriptions in a protocol standard [\(see 3.x.y\)](#) supersede descriptions for the same parameters in this standard.

8.99.99 Access controls TransportID access identifiers

8.99.99.1 TransportID introduction

TransportIDs (see table 53) are a type of access identifier (see 5.99.2.2) used in ACL ACEs to allow logical unit access to an initiator based on a protocol specific initiator device name, initiator port identifier, or initiator port name belonging to that initiator.

Table t53 — TransportID format

Bit Byte	7	6	5	4	3	2	1	0
0	PROTOCOL CODE							
1	Protocol Specific Data							
23								

The **PROTOCOL CODE** field (see table 54) identifies the protocol to which the TransportID applies.

Table t54 — Protocol codes

Protocol Code	Protocol	Protocol Standard	Reference
<u>00h</u>	SCSI over Fibre Channel	FCP-2	8.99.99.2
<u>01h</u>	Parallel SCSI	SPI-4	8.99.99.3
02h-FFh	Reserved		

8.99.99.2 TransportIDs for initiators using SCSI over Fibre Channel

A Fibre Channel TransportIDs (see table 55) is a type of access identifier (see 5.99.2.2) used in ACL ACEs to allow logical unit access to a FCP-2 initiator based on the world wide unique initiator port name belonging to that initiator.

Table t55 — Fibre Channel TransportID format

Bit Byte	7	6	5	4	3	2	1	0
0	PROTOCOL CODE (01h)							
1	(MSB)	Reserved						(LSB)
7								
8	(MSB)	WORLD WIDE NAME						(LSB)
15								
16	(MSB)	Reserved						(LSB)
23								

The **WORLD WIDE NAME** field shall contain the port World Wide Name defined by the Physical Log In (PLOGI) extended link service, defined in FC-FS.

A Fibre Channel TransportID allows the initiator specified by the world wide name access to the logical units described in an ACE (see 5.99.2).

8.99.99.3 TransportIDs for initiators using a parallel SCSI bus

A parallel SCSI bus TransportIDs (see table 56) is a type of access identifier (see 5.99.2.2) used in ACL ACEs to allow logical unit access to a SPI-4 initiator based on the SCSI address of an initiator and the SCSI target device relative port through which the initiator accesses the SCSI target device.

Table t56 — Parallel SCSI bus TransportID format

Bit Byte	7	6	5	4	3	2	1	0
0	PROTOCOL CODE (00h)							
1	Reserved							
2	(MSB)	SCSI ADDRESS						(LSB)
3								
4	(MSB)	RELATIVE PORT IDENTIFIER						(LSB)
7								
8	(MSB)	Reserved						(LSB)
23								

The SCSI ADDRESS field specifies the SCSI address (see SPI-4) of the initiator.

The RELATIVE PORT IDENTIFIER field specifies the four-byte binary number identifying a specific port in the SCSI target device relative to other ports. The relative port identifier value shall be one of the values returned in the Device Identifier VPD page (see 8.z.z). If the RELATIVE PORT IDENTIFIER does not reference a port in the device, the TransportID is invalid.

In order for a parallel SCSI bus TransportID to allow access to the logical units described in an ACE (see 5.99.2), an initiator having the specified SCSI address shall access the SCSI target device via the port specified by the relative port identifier.