ENDL
TEXAS

Date: 14 July 2004
To: T10 Technical Committee and SNIA OSD TWG
From: Ralph O. Weber
Subject: Rewrite of OSD Security and Policy/Storage Manager Models

Revision History

This document is being presented in a 'build up' fashion. That is r0 contains an initial amount of changes and each revision after that contains additional details and changes.

r0 Shows only the model split between Capabilities (aka Policy/Storage Management) and Credentials (aka Security) and provides a rudimentary description for fencing

r1 Contains the same normative text as r0, but the strikeouts are removed

r2 Example configuration figure cleaned up and used blue lines for connections that do not use the service delivery subsystem. Moves the communications security requirements to the security manager Trust Assumptions subclause. Updates the security threats table to cover non-secure channels. Adds prototype CDB definition with changes resulting from the model split between Capabilities (aka Policy/Storage Management) and Credentials (aka Security).

r3 Makes all agreed changes that the author could locate on the SNIA OSD TWG reflector and a few from other sources. It is believe that this revision addresses all the 04-108 comments that identify a revision of this document as detailing the response to a T10 OSD Letter Ballot comment.

r4 Contains the same normative text as r3, but with the most annoying strikeouts removed

r5
a) The Security methods and threats thwarted table was updated to more appropriately represent the secure channel requirements and features;
b) The requirements for maintaining lists of previously used request nonces was clarified;
c) The interactions of freezing audit values and/or working keys with request nonce list requirements was restored, and the definitions of related attributes updated;
d) The GLOBAL permission was added as a requirement for SET KEY commands that change the root key and for SET MASTER KEY commands;
e) The SET MASTER KEY command was updated to use the correct algorithms and verify that correct data is transferred during the CHANGE MASTER KEY step;
f) The restriction on seed LSB values being zero was removed and in support of that change the secret key algorithm was changed to flip the seed LSB between the authentication and generation key computations;
g) The need to protect capability keys assigned to all security model components;
h) The need for message integrity was added for communications between the security manager and policy/storage manager;
i) The fact that commands sent to the OSD by the security manager follow the same communications requirements as for any other application client was clarified;
j) Several aspects of clock coordination were polished slightly;
k) The requirement for MODP DH groups was clarified by adding some counter examples;
l) The notation used to describe the SET MASTER KEY steps was changed to better match T10 expectations;
m) A support requirements column was added to the table listing attributes pages defined by this standard; and
n) Several typographical errors were corrected.

Differences between r4 and r5 are marked with change bars.

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

Summary

The document shows all the changes to OSD r09 needed to:

- Separate Capability handling (aka Policy/Storage Management) from Credential handling (aka Security)
- Treat security manager communications requirements as a trust assumption
- Modify threats analysis to cover CAPKEY over a non-secure channel

Changes made by this document are shown as red text additions and ~~red text removals~~.

The author believes that this revision of this document addresses the following previously unresolved OSD Letter Ballot comments:

- ENDL 2, HP 62, IBM 42, IBM 141, Seagate 8, and Veritas 65 motivated the development of this document, meaning the all the changes it proposes are addressed to those comments more or less
- Agilent 7 and two-thirds of EMC 8 should be resolved by moving the Partition_ID to the capability (as described in the response to IBM 141)
- EMC 1 should be addressed by the changes in 4.9.2 (Trust assumptions)
- EMC 2 should be addressed by the paragraph added at the end of 4.9.6.2
- EMC 3 should be addressed by the content of 4.9.m
- EMC 4 should be addressed by the changes in the "Security methods and threats thwarted" table in 4.9.3.1 (Security methods … Introduction)
- EMC 5, EMC 6, HP 33, HP 35, and Lingua 19 should be resolved the completely new definition of a security token (see 4.9.3.3)
- EMC 7, EMC 9, and part of Panasas 2 should be addressed the addition of step 5 to 4.9.5.1. The remainder of Panasas 2 should be addressed by the changes in 4.x.2.2.
- EMC 10 should be addressed by removing discussion of far-in-the-future nonces and making 'oldest valid nonce' and 'newest valid nonce' settable attributes (see 4.9.6.2 and 7.1.2.21)
- EMC 13 should be addressed by the changes to the SET MASTER KEY command and subclauses that it references (see 6.20)
- END 2 and HP 62 should be addressed by the new 4.x.3 as well as by the changes in 7.1.2.21, 7.1.2.22, and 7.1.2.23
- HP 51 and Intel 21 should be addressed by the global change of 'drive key' to 'root key'
- IBM 147, Panasas 5, and Seagate 9 should be resolved by the addition of a SECURITY METHOD field to the Capability (see 4.x.2.2 and 4.9.m)
- Seagate 18 should be resolved by the changes in 4.9.7, table 16, table 17, table 22, table 42, and table 43.

This document also shows all approved changes for the clauses modified by this document, specifically: Agilent 3, Agilent 8, Agilent 9, Agilent 10, Brocade 17, EMC 12, HP 30, HP 31, HP 32, HP 34, HP 36, HP 40, HP 42, HP 43, HP 47, HP 48, HP 49, HP 50, HP 54, HP 55, HP 56, HP 57, HP 58, HP 59, HP 76, HP 77, HP 85, HB 115, HP 120, HP 122, IBM 39, IBM 40, IBM 41, IBM 43, IBM 44, IBM 46, IBM 47, IBM 48, IBM 49, IBM 50, IBM 52, IBM 53, IBM 55, IBM 56, IBM 57, IBM 58, IBM 59, IBM 91, IBM 128, IBM 129, IBM 130, IBM 131, IBM 132, IBM 133, IBM 134, IBM 136, IBM 137, IBM 138, IBM 142, IBM 153, Lingua 20, Lingua 22, Lingua 23, Lingua 24, Lingua 25, Lingua 26, Lingua 27, Lingua 28, Lingua 30, Lingua 31, Lingua 32, Lingua 36, Lingua 37, LSI 12, Seagate 7, Seagate 10, Seagate 11, Seagate 13, Seagate 14, Seagate 15, Seagate 18, Seagate 19, Seagate 20, Seagate 21, Seagate 50, Seagate 51, Veritas 45, Veritas 47, Veritas 49, Veritas 50, Veritas 51, Veritas 52, Veritas 53, Veritas 57, Veritas 58, Veritas 59, Veritas 61, Veritas 62, Veritas 63, Veritas 64, Veritas 66, Veritas 67, Veritas 68, Veritas 69, Veritas 70, Veritas 71, Veritas 72, Veritas 107, Veritas 108, Veritas 117, Veritas 118, Veritas 119, and Veritas 120.

These changes are shows as blue text additions and ~~blue text removals~~.

Suggested Changes:

2.4 Approved IETF References

Copies of the following approved IETF standards may be obtained through the Internet Engineering Task Force (IETF) at www.ietf.org.

RFC 1750, Randomness Recommendations for Security

RFC 2401, Security Architecture for the Internet Protocol

RFC 2409, The Internet Key Exchange

RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange

3.2 Acronyms

…

DH Diffie-Hellman (see 2.4, RFC 2409 and RFC 3526)

…

IANA Internet Assigned Numbers Authority (see www.iana.org)

…

MODP Modular Exponential (see 2.4, RFC 3526)

…

4.4 Elements of the example configuration

The example in this subclause (see figure 1) illustrates the three mandatory and two optional constituents of an OSD configuration:

a) Object-Based Storage Devices;
b) Service delivery subsystem;
c) Host systems (i.e., initiator devices);
d) Optionally, a security manager; and
e) Optionally, a policy/storage manager.

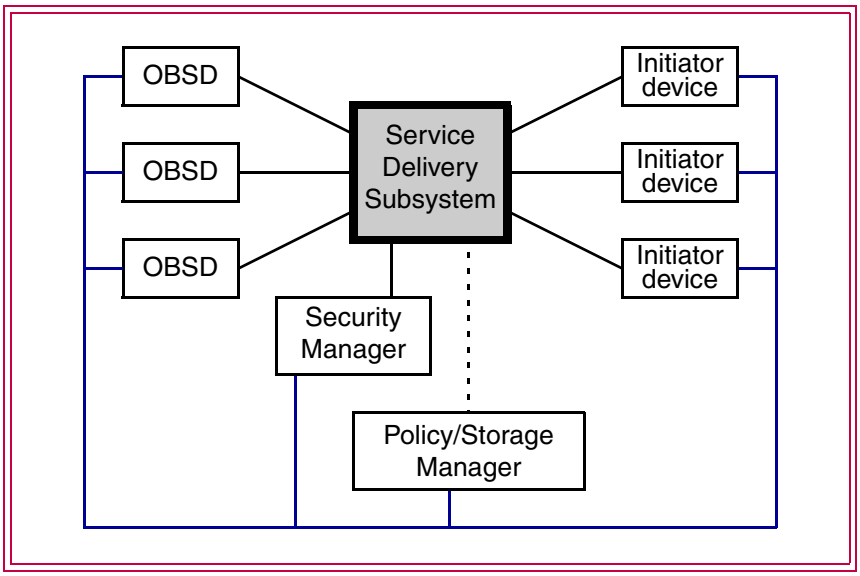

Figure 1 — Example OSD Configuration

The OBSDs are the storage components of the system to be shared (e.g., disc drives, RAID subsystems, tape drives, tape libraries, optical drives, jukeboxes, or other storage devices).

Application clients using multiple SCSI initiator ports share directly access an OBSD (see 3.1.26) via the service delivery subsystem. The service delivery subsystem is used by the components in the OSD model, except possibly the policy/storage manager and/or security manager, to intercommunicate. The OSD security model (see 4.9) does not require the service delivery subsystem to provide security-related services (i.e., authentication and confidentiality), but is designed to take advantage of whatever security-related services are provided.

The policy/storage manager (see 4.x), if present, coordinates access constraints between OSD device servers and application clients, preparing the capabilities application clients place in CDBs to gain access to OSD objects and command functions.

The security manager (see 4.9), if present, secures capabilities in cryptographically protected credentials for OSD device servers and application clients.

The policy/storage manager and security manager may reside in the OBSDs, in applications clients, or as a separate entities.

The policy/storage manager and security manager may use the service delivery subsystem and be an application client, but they also may use another mechanism to communicate with the OSD device servers and application clients. Security-related requirements on the communications mechanisms used by the security manager are described in 4.9.2

4.x Policy/storage management

4.x.1 Overview

The policy/storage manager:

a) Provides access policy controls to application clients via preparation of policy-coordinated capabilities (see 4.x.2); and
b) In concert with the OSD logical unit, prevents unsafe or temporarily undesirable utilization of OBSD storage (see 4.x.3).

4.x.2 Capabilities

4.x.2.1 Introduction

Each CDB defined by this standard includes a capability (see 4.x.2.2) whose contents specify the command functions (see 3.1.10) that the device server is allowed to process in response to the command.

The device server validates that the requested command functions are allowed by the capability based on:

a) The type of functions (e.g., read, write, attributes setting, attributes retrieval); and
b) The OSD object on which the command functions are to be processed.

The policies that determine which capabilities are provided to which application clients are outside the scope of this standard.

The policy/storage manager shall coordinate the delivery of capabilities to application clients with the security manager (see 4.9) as follows:

a) If the security method for all partitions in the OSD logical unit is NOSEC (see 4.9.3.2), then the policy/storage manager may:
   A) Allow application clients to prepare their own capabilities;
   B) Coordinate the preparation of capabilities for multiple application clients in response to requests, the format and transport mechanisms for which are outside the scope of this standard; or
   C) Coordinate the preparation of capabilities with the security manager as described in item b);
   or
b) If a security method other than NOSEC is in use by any partition in the OSD logical unit, then the policy/storage manager shall coordinate the preparation of capabilities with the security manager by:
   A) Requiring application clients to request credentials and capabilities from the security manager; and
   B) Preparing capabilities only is response to requests from the security manager.

4.x.2.2 Capability format

4.x.2.2.1 Introduction

A capability (see table 1) is included in a CDB to enable the device server to verify that the sender is allowed to perform the command functions (see 3.1.10) specified by the CDB .

Table 1 — Capability format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved				CAPABILITY FORMAT (1h)			
1	KEY VERSION				INTEGRITY CHECK VALUE ALGORITHM			
2	SECURITY METHOD							
3	Reserved							
4	(MSB)	CAPABILITY EXPIRATION TIME						
9								(LSB)
10		AUDIT						
29								
30	(MSB)	CAPABILITY DISCRIMINATOR						
41								(LSB)
42	(MSB)	OBJECT CREATED TIME						
47								(LSB)
48	OBJECT TYPE							
49		PERMISSIONS BIT MASK						
53								
54	Reserved							
55	OBJECT DESCRIPTOR TYPE				Reserved			
56		OBJECT DESCRIPTOR						
79								

The CAPABILITY FORMAT field (see table 2) specifies the format of the capability. If capabilities are coordinated with the security manager, the capability format also is the credential format. The policy/storage manager shall set the CAPABILITY FORMAT field to 1h (i.e., the format defined by this standard).

Table 2 — Capability format values

Value	Description
0h	No capability
1h	The format defined by this standard
2h - Fh	Reserved

If the CAPABILITY FORMAT field contains 1h, the device server shall verify that the command functions requested by a CDB are permitted by the capability as described in this subclause. The device server may verify that a command function is permitted after other command functions are completed. The device server shall verify that a command

function is permitted before any part of the command function is performed. (E.g., the device server may delay verifying that the set attributes command functions specified by a set attributes list are allowed until the requested read command function is completed, but all the capability permissions concerning the setting attributes are to be verified before any attribute values are changed.)

The KEY VERSION field, INTEGRITY CHECK VALUE ALGORITHM field, and SECURITY METHOD field are used by the security manager. If capabilities are not coordinated with the security manager, the KEY VERSION field, INTEGRITY CHECK VALUE ALGORITHM field, and SECURITY METHOD field are reserved.

If CDB contains a non-zero value in the SECURITY METHOD field, the integrity of the CDB shall be validated (see 4.9.5.1) before any other command processing actions are undertaken (i.e., before verifying that command functions requested in the CDB are permitted by the capability).

The command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB, if the CDB SECURITY METHOD field or CAPABILITY FORMAT field contains zero and one of the following is true:

a) The command is SET KEY (see 6.23) or SET MASTER KEY (see 6.24); or
b) The security method attribute in the Partition Policy/Security attributes page (see 7.1.2.21) specifies a security method other than NOSEC for the partition identified as follows:
   A) For the CREATE PARTITION command (see 6.7), FLUSH OSD command (see 6.y), FORMAT OSD command (see 6.9), the identified partition is partition zero (see 3.1.31);
   B) For any command that is not one of those already listed, the partition is identified by the contents of the CDB PARTITION_ID field.

The CAPABILITY EXPIRATION TIME field specifies the value of the clock attribute in the Root Information attributes page (see 7.1.2.8) after which this capability is no longer valid. If a CDB CAPABILITY EXPIRATION TIME field contains a value other than zero and the value of the clock attribute in the Root Information attributes page is greater than the value in the CAPABILITY EXPIRATION TIME field, 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.

Successful use of the capability expiration time requires some degree of synchronization between the clocks of the device server, policy/storage manager, and security manager. The protocol for synchronizing the clocks is outside the scope of this standard.

The AUDIT field is a vendor specific value that the policy/storage manager and/or security manager may use to associate the capability with a specific application client.

The CAPABILITY DISCRIMINATOR field contains a nonce (see 3.1.23) that differentiates one capability from another.

The OBJECT CREATED TIME field specifies the contents of the created time attribute for the OSD object (see table 3) to which the capability applies. A value of zero specifies that any object created time is allowed.

Table 3 — Created time for OSD objects by type

Object Type (see table 4)	Attributes page containing created time attribute to which the capability OBJECT CREATED TIME field is applies
ROOT	Partition Timestamps attributes page (see 7.1.2.16) for partition zero (see 3.1.31)
PARTITION	Partition Timestamps attributes page (see 7.1.2.16)
COLLECTION	Collection Timestamps attributes page (see 7.1.2.17)
USER	User Object Timestamps attributes page (see 7.1.2.18)

If a CDB OBJECT CREATED TIME field contains a value other than zero and the value in the OBJECT CREATED TIME field is not identical to the value in the created time attribute from the associated timestamps attributes page (see table 3), 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 INVALID FIELD IN CDB.

The OBJECT TYPE field (see table 4) specifies the type of OSD object to which this capability allows access . If capabilities are coordinated with the security manager, the OBJECT TYPE field is used to select the secret key that is used in validating the credential.

Table 4 — Object type values

Value	Name	OSD object type to which access is allowed
01h	ROOT	Root object
02h	PARTITION	Partition
40h	COLLECTION	Collection
80h	USER	User objects
all other values	Reserved	

If the command functions specified by the CDB are not allowed for the OSD object type specified in the CDB OBJECT TYPE field (see 4.x.2.2), 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 PERMISSIONS BIT MASK field (see table 5) specifies which functions are allowed by this capability. More than one permissions bit may be set within the constraints specified in 4.x.2.3 resulting in a single capability that allows more than one command function.

Table 5 — Permissions bit mask format

Bit Byte	7	6	5	4	3	2	1	0
49	READ	WRITE	GET_ATTR	SET_ATTR	CREATE	REMOVE	OBJ_MGMT	APPEND
50	DEV_MGMT	GLOBAL	POL/SEC	Reserved				
51	Reserved							
52	Reserved							
53	Reserved							

A READ bit set to one allows read access to the data in an OSD object, but not to the attributes. For the root object, partitions, and collections the data in the OSD object is the list of other objects contained in the OSD object. A READ bit set to zero prohibits read access to the data in an OSD object.

A WRITE bit set to one allows processing of the WRITE command (see 6.21) , but not access to user object attributes. A WRITE bit set to zero prohibits processing of the WRITE command .

A GET_ATTR (get attributes) bit set to one allows retrieval of (i.e., read access to) the attributes associated with an OSD object. A GET_ATTR bit set to zero prohibits retrieval of attributes except for the attributes in the Current Command attributes page (see 7.1.2.24).

A SET_ATTR (set attributes) bit set to one allows the setting of (i.e., write access to) the attributes associated with an OSD object except for attributes located in the OSD object's policy/security attributes page (e.g., the User Object Policy/Security attributes page (see 7.1.2.23) if the OSD object is a user object). The setting of attributes located in the OSD object's policy/security attributes page is allowed only if both the SET_ATTR bit and the POL/SEC bit are set to one. A SET_ATTR bit set to zero prohibits the setting of the attributes associated with an OSD object.

A CREATE bit set to one allows the creation of OSD objects. A CREATE bit set to zero prohibits the creation of OSD objects.

A REMOVE bit set to one allows the removal of OSD objects. A REMOVE bit set to zero prohibits the removal of OSD objects.

An OBJ_MGMT (object management) bit set to one allows command functions that may change how the OSD logical unit handles an OSD object without affecting the stored data, stored attributes, commands in the task set, policies, or security for the OSD object. A OBJ_MGMT bit set to zero prohibits such command functions.

An APPEND bit set to one allows processing of the APPEND command (see 6.2), but not access to user object attributes. A APPEND bit set to zero prohibits processing of the APPEND command.

A DEV_MGMT (device management) bit set to one allows command functions that affect the OSD logical unit. A DEV_MGMT bit set to zero prohibits command functions that affect the OSD logical unit.

A GLOBAL bit set to one allows command functions that may affect all the OSD objects in the OSD logical unit. A GLOBAL bit set to zero prohibits command functions that may affect all the OSD objects in the OSD logical unit.

A POL/SEC bit set to one allows command functions that affect the policy/security functions performed for one or more OSD objects. A POL/SEC bit set to zero prohibits command functions that affect the policy/security functions performed for one or more OSD objects.

If the command functions specified by the CDB are not allowed by the CDB PERMISSIONS BIT MASK field (see 4.x.2.2), 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 OBJECT DESCRIPTOR TYPE field (see table 6) specifies the format of information that appears in the OBJECT DESCRIPTOR field.

Table 6 — Object descriptor types

Object Descriptor Type	Name	Description	Reference
0h	NONE	The OBJECT DESCRIPTOR field shall be ignored	
1h	U/C	A single collection or user object	4.x.2.2.2
2h	PAR	A single partition, including partition zero	4.x.2.2.3
3h - Fh		Reserved	

4.x.2.2.2 U/C capability object descriptor

If the object descriptor type is U/C (i.e., 1h), the OBJECT DESCRIPTOR field shall have the format shown in table 7, specifying a single collection or user object to which the capability allows access.

Table 7 — User object/collection object descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
56	(MSB)							
59				POLICY ACCESS TAG				(LSB)
60	(MSB)							
67				ALLOWED PARTITION_ID				(LSB)
68	(MSB)							
75				ALLOWED OBJECT_ID				(LSB)
76								
79				Reserved				

If the POLICY ACCESS TAG field contains a value other than zero, the policy access tag attribute identified by the command and object type field (see table 8) is compared to the POLICY ACCESS TAG field contents as part of verifying the capability. If the POLICY ACCESS TAG field contains zero, then no comparison is made to any policy access tag attribute. The policy/storage manager or OSD logical unit changes the policy access tag to prevent unsafe or temporarily undesirable accesses to an OSD object (see 4.x.3).

Table 8 — Policy access tag OSD objects

Command	Object Type (see table 4)	Attributes page containing policy access tag attribute to which credential POLICY ACCESS TAG field is compared
CREATE PARTITION	PARTITION	Partition Policy/Security attributes page (see 7.1.2.21) for partition zero (see 3.1.31)
CREATE COLLECTION	COLLECTION	Partition Policy/Security attributes page (see 7.1.2.21)
CREATE or CREATE AND WRITE	USER	Partition Policy/Security attributes page (see 7.1.2.21)
All other commands	ROOT	Partition Policy/Security attributes page (see 7.1.2.21) for partition zero
	PARTITION	Partition Policy/Security attributes page (see 7.1.2.21)
	COLLECTION	Collection Policy/Security attributes page (see 7.1.2.22)
	USER	User Object Policy/Security attributes page (see 7.1.2.23)

If the non-zero value in the CDB POLICY ACCESS TAG field is not identical to the value in the policy access tag attribute from the associated security attributes page (see table 8), 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 INVALID FIELD IN CDB.

The ALLOWED PARTITION_ID field specifies the partition to which access is allowed. The command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB, if:

a) The ALLOWED PARTITION_ID field contains zero in a CDB; or
b) The ALLOWED PARTITION_ID field contents do not match the contents of the PARTITION_ID field in the CDB.

The ALLOWED OBJECT_ID field specifies the Collection_Object_ID (see 4.6.6) or User_Object_ID (see 4.6.5) of the OSD object to which the capability allows access. The command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB, if:

a) The command is not CREATE, CREATE AND WRITE, or CREATE COLLECTION and the ALLOWED OBJECT_ID field contains zero;
b) The OBJECT TYPE field contains 40h (i.e., COLLECTION) and the ALLOWED OBJECT_ID field contents do not match the contents of the CDB COLLECTION_OBJECT_ID field or REQUESTED COLLECTION_OBJECT_ID field; or
c) The OBJECT TYPE field contains 80h (i.e., USER) and the ALLOWED OBJECT_ID field contents do not match the contents of the CDB USER_OBJECT_ID field or REQUESTED USER_OBJECT_ID field.

4.x.2.2.3 PAR capability object descriptor

If the object descriptor type is PAR (i.e., 2h), the OBJECT DESCRIPTOR field shall have the format shown in table 9, specifying a single partition, including partition zero (see 3.1.31), to which the capability allows access.

Table 9 — Partition descriptor format

Bit / Byte	7	6	5	4	3	2	1	0
56	(MSB)			POLICY ACCESS TAG				
59								(LSB)
60	(MSB)			ALLOWED PARTITION_ID				
67								(LSB)
68				Reserved				
79								

The POLICY ACCESS TAG field is described in 4.x.2.2.2.

The ALLOWED PARTITION_ID field specifies the partition to which access is allowed. The command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB, if:

a) The CDB USER_OBJECT_ID field, REQUESTED USER_OBJECT_ID field, COLLECTION_OBJECT_ID field or REQUESTED COLLECTION_OBJECT_ID field, if any, contains a value other than zero;
b) The OBJECT TYPE field contains 02h (i.e., PARTITION) and one of the following is true:
   A) The command is not CREATE PARTITION and the ALLOWED PARTITION_ID field contains zero;
   B) The ALLOWED PARTITION_ID field contents do not match the contents of the CDB PARTITION_ID field; or
c) The OBJECT TYPE field contains 01h (i.e., ROOT) and one of the following is true:
   A) The ALLOWED PARTITION_ID field contains a value other than zero; or
   B) The CDB PARTITION_ID field, if any, contains a value other than zero.

4.x.2.3 Capabilities and commands allowed

The validity of a specific command and some of the command function (see 3.1.10) related fields in that command is determined by the presence of specific combinations of values in capability fields as shown in table 10. A command function is allowed if at least one row in table 10 allows it, even if a different row that applies does not allow it.

Any command may retrieve or set attributes. The combinations of capability fields that allow those functions are shown in table 11. Retrieving or setting attributes is allowed if at least one row in table 11 allows it, even if a different row that applies does not allow it.

A single capability for a single object type may allow processing of multiple command functions (e.g., read and write) as well as retrieving and setting attributes by combining the permission bits values described in multiple rows of table 10 and table 11.

Table 10 — Commands allowed by specific capability field values (Sheet 1 of 2)

Commands allowed and CDB fields whose contents are restricted by capability field contents, if any	Capability Field values that allow a command		
	Object Type Name	Permission Bits That Are Set To One	Object Descriptor Name
An APPEND command	USER	APPEND	U/C
A CREATE command	USER	CREATE	U/C
A CREATE AND WRITE command	USER	CREATE and WRITE	U/C
A CREATE COLLECTION command	COLLECTION	CREATE	U/C
A CREATE PARTITION command	PARTITION	CREATE	PAR
A FLUSH command	USER	OBJ_MGMT	U/C
A FLUSH COLLECTION command	COLLECTION	OBJ_MGMT	U/C
A FLUSH PARTITION command	PARTITION	OBJ_MGMT	PAR
A FLUSH OSD command	ROOT	OBJ_MGMT	PAR
A FORMAT OSD command	ROOT	OBJ_MGMT and GLOBAL	PAR
A GET ATTRIBUTES command addressed to a user object	USER	see table 11	U/C
A GET ATTRIBUTES command addressed to a collection	COLLECTION	see table 11	U/C
A GET ATTRIBUTES command addressed to a partition	PARTITION	see table 11	PAR
A GET ATTRIBUTES command addressed to the root object	ROOT	see table 11	PAR
A LIST command addressed to a partition	PARTITION	READ	PAR
Combinations of OBJECT TYPE field, PERMISSION BITS field, and OBJECT DESCRIPTOR TYPE field values not shown in this table and table 11 are reserved. The capability fields not shown in this table may place additional limits on the objects that are allowed to be accessed.			

Table 10 — Commands allowed by specific capability field values (Sheet 2 of 2)

Commands allowed and CDB fields whose contents are restricted by capability field contents, if any	Capability Field values that allow a command		
	Object Type Name	Permission Bits That Are Set To One	Object Descriptor Name
A LIST command addressed to the root object	ROOT	READ	PAR
A LIST COLLECTION command addressed to a collection	COLLECTION	READ	U/C
A LIST COLLECTION command addressed to a partition	PARTITION	READ	PAR
A PERFORM TASK MANAGEMENT command with function code of ABORT TASK or QUERY TASK addressed to a user object	USER	DEV_MGMT	U/C
A PERFORM TASK MANAGEMENT command with function code of ABORT TASK or QUERY TASK addressed to a collection	COLLECTION	DEV_MGMT	U/C
A PERFORM TASK MANAGEMENT command with function code of ABORT TASK or QUERY TASK addressed to a partition	PARTITION	DEV_MGMT	PAR
A PERFORM TASK MANAGEMENT command with function code of ABORT TASK or QUERY TASK addressed to the root object	ROOT	DEV_MGMT	PAR
A PERFORM TASK MANAGEMENT command or a PERFORM SCSI COMMAND command	ROOT	DEV_MGMT and GLOBAL	PAR
A READ command	USER	READ	U/C
A REMOVE command	USER	REMOVE	U/C
A REMOVE COLLECTION command	COLLECTION	REMOVE	U/C
A REMOVE PARTITION	PARTITION	REMOVE	PAR
A SET ATTRIBUTES command addressed to a user object	USER	see table 11	U/C
A SET ATTRIBUTES command addressed to a collection	COLLECTION	see table 11	U/C
A SET ATTRIBUTES command addressed to a partition	PARTITION	see table 11	PAR
A SET ATTRIBUTES command addressed to the root object	ROOT	see table 11	PAR
A SET KEY command with KEY TO SET field equal to 10b or 11b	PARTITION	DEV_MGMT and POL/SEC	PAR
A SET KEY command with KEY TO SET field equal to 01b	ROOT	DEV_MGMT, POL/SEC, and GLOBAL	PAR
A SET MASTER KEY command	ROOT	DEV_MGMT, POL/SEC, and GLOBAL	PAR
A WRITE command	USER	WRITE	U/C

Combinations of OBJECT TYPE field, PERMISSION BITS field, and OBJECT DESCRIPTOR TYPE field values not shown in this table and table 11 are reserved.
The capability fields not shown in this table may place additional limits on the objects that are allowed to be accessed.

Table 11 — Attribute retrieval and setting functions allowed by specific capability field values (Sheet 1 of 3)

Attribute-Related Functions Allowed	Capability Field values that allow attribute-related functions		
	Object Type Name	Permission Bits That Are Set To One	Object Descriptor Name
Retrieval of attributes from the Current Command attributes page	USER or COLLECTION	none	U/C
Retrieval of attributes from the Current Command attributes page	PARTITION or ROOT	none	PAR
Retrieval of attributes from any attributes page associated with the addressed user object	USER	GET_ATTR	U/C
As part of a CREATE command or CREATE AND WRITE command, retrieval of attributes from any attributes page associated with any user object created by the command.	USER	GET_ATTR	U/C
Retrieval of attributes from any attributes page associated with the addressed collection	COLLECTION	GET_ATTR	U/C
As part of a CREATE COLLECTION command, retrieval of attributes from any attributes page associated with the collection created by the command	COLLECTION	GET_ATTR	U/C
Retrieval of attributes from any attributes page associated with the addressed partition	PARTITION	GET_ATTR	PAR
As part of a CREATE PARTITION command, the retrieval of attributes from any attributes page associated with the created partition	PARTITION	GET_ATTR	PAR
Retrieval of attributes from any attributes page associated with the root object or in any attributes page associated with partition zero (see 3.1.31)	ROOT	GET_ATTR	PAR
Setting attributes in any attributes page associated with the addressed user object, except attributes in a User Object Policy/Security attributes page	USER	SET_ATTR	U/C
As part of a CREATE command or CREATE AND WRITE command, the setting of attributes in any attributes page associated with any user object created by the command, except attributes in a User Object Policy/Security attributes page	USER	SET_ATTR	U/C
Combinations of OBJECT TYPE field, PERMISSION BITS field, and OBJECT DESCRIPTOR TYPE field values not shown in this table and table 10 are reserved. The capability fields not shown in this table may place additional limits on the objects that are allowed to be accessed.			

Table 11 — Attribute retrieval and setting functions allowed by specific capability field values (Sheet 2 of 3)

Attribute-Related Functions Allowed	Capability Field values that allow attribute-related functions		
	Object Type Name	Permission Bits That Are Set To One	Object Descriptor Name
Setting attributes in any attributes page associated with the addressed collection, except attributes in a Collection Policy/Security attributes page	COLLECTION	SET_ATTR	U/C
As part of a CREATE COLLECTION command, the setting of attributes in any attributes page associated with the collection created by the command, except attributes in the Collection Policy/Security attributes page	COLLECTION	SET_ATTR	U/C
Setting attributes in any attributes page associated with the addressed partition, except attributes in a Partition Policy/Security attributes page	PARTITION	SET_ATTR	PAR
As part of a CREATE PARTITION command, the setting of attributes in any attributes page associated with the partition created by the command, except attributes in the Partition Policy/Security attributes page	PARTITION	SET_ATTR	PAR
Setting attributes in any attributes page associated with the root object, except attributes in a Root Policy/Security attributes page Setting attributes in any attributes page associated with partition zero (see 3.1.31), except attributes in a Partition Policy/Security attributes page	ROOT	SET_ATTR	PAR
Setting attributes in any attributes page associated with the addressed user object	USER	SET_ATTR and POL/SEC	U/C
As part of a CREATE command or CREATE AND WRITE command, the setting of attributes in any attributes page associated with any user object created by the command	USER	SET_ATTR and POL/SEC	U/C
Setting attributes in any attributes page associated with the addressed collection	COLLECTION	SET_ATTR and POL/SEC	U/C
As part of a CREATE COLLECTION command, the setting of attributes in any attributes page associated with the collection created by the command	COLLECTION	SET_ATTR and POL/SEC	U/C

Combinations of OBJECT TYPE field, PERMISSION BITS field, and OBJECT DESCRIPTOR TYPE field values not shown in this table and table 10 are reserved.
The capability fields not shown in this table may place additional limits on the objects that are allowed to be accessed.

Table 11 — Attribute retrieval and setting functions allowed by specific capability field values (Sheet 3 of 3)

Attribute-Related Functions Allowed	Capability Field values that allow attribute-related functions		
	Object Type Name	Permission Bits That Are Set To One	Object Descriptor Name
Setting attributes in any attributes page associated with the addressed partition	PARTITION	SET_ATTR and POL/SEC	PAR
As part of a CREATE PARTITION command, the setting of attributes in any attributes page associated with the partition created by the command	PARTITION	SET_ATTR and POL/SEC	PAR
Setting attributes in any attributes page associated with the root object or in any attributes page associated with partition zero (see 3.1.31)	ROOT	SET_ATTR and POL/SEC	PAR
Combinations of OBJECT TYPE field, PERMISSION BITS field, and OBJECT DESCRIPTOR TYPE field values not shown in this table and table 10 are reserved. The capability fields not shown in this table may place additional limits on the objects that are allowed to be accessed.			

4.x.3 Policy access tags

The policy access tag (see table 12) allows the coordinated actions of both the OSD logical unit and policy/storage manager to prevent unsafe or temporarily undesirable utilization of OBSD storage that is assigned to the OSD logical unit.

Table 12 — Policy access tag format

Bit / Byte	7	6	5	4	3	2	1	0
0	FENCE	(MSB)						
1				VERSION				
2								
3								(LSB)

During normal operation the value of the FENCE bit is zero.

If the OSD logical unit detects a condition that would make further accesses to one or more OSD objects unsafe, it shall set the FENCE bit to one in the policy access tag attributes in the Policy/Security attributes pages associated with those objects (e.g., the User Object Policy/Security attributes page (see 7.1.2.23) if the OSD object is a user object) and notify the policy/storage manager of a condition needing attention. The OSD logical unit, policy/storage manager, or both act to correct whatever conditions are making accesses to the OSD objects unsafe. After the conditions making accesses to the OSD objects unsafe are corrected the policy/storage manager sets the FENCE bit to zero.

If a set attributes list (see 5.2.1.3) contains a request to set the FENCE bit to one, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field contains 4000 0001h (i.e., the security version policy access tag attribute) and the set attributes data specified by the SET ATTRIBUTES OFFSET field (see 5.2.1.2) specifies that the FENCE bit be set to one, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

To block capability-based access to one or more OSD objects, the policy/storage manager changes the VERSION field in the policy access tag attributes in the Policy/Security attributes pages associated with those objects. The conditions under which the policy/storage manager may be called on to do this include:

a) Recovery from errors other than those detected by the OSD logical unit that make accesses to one or more OSD object unsafe; and
b) Receipt of a request to change the policy access tag from the security manager (see 4.9.5.4).

If a set attributes list (see 5.2.1.3) contains a request to set the VERSION field to zero, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field contains 4000 0001h (i.e., the security version policy access tag attribute) and the set attributes data specified by the SET ATTRIBUTES OFFSET field (see 5.2.1.2) specifies that the VERSION field be set to zero, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The OSD logical unit shall not modify the contents of a policy access tag VERSION field.

The device server terminates any command received with a capability whose POLICY ACCESS TAG field contains a non-zero value that differs from the policy access tag attribute value in the Policy/Security attributes page associated with the objects (see 4.x.2.2).

4.9 Security

4.9.1 Basic security model

The OSD security model is composed of the following components:

a) An OBSD (see 3.1.26);
b) A policy/storage manager (see 4.x);
c) A security manager; and
d) Application clients.

The principal function of the security manager is preparing credentials in response to application client requests. A credential is a data structure containing a capability prepared by the policy/storage manager and protected by an integrity check value (see 3.1.18), having the following properties:

a) The capability in the credential grants defined access to an OSD logical unit for specific command functions (see 3.1.10); and
b) The integrity check value in the credential protects the capability and commands that include the capability from various attacks described in 4.9

Figure 2 shows the flow of transactions between the components of the OSD security model.

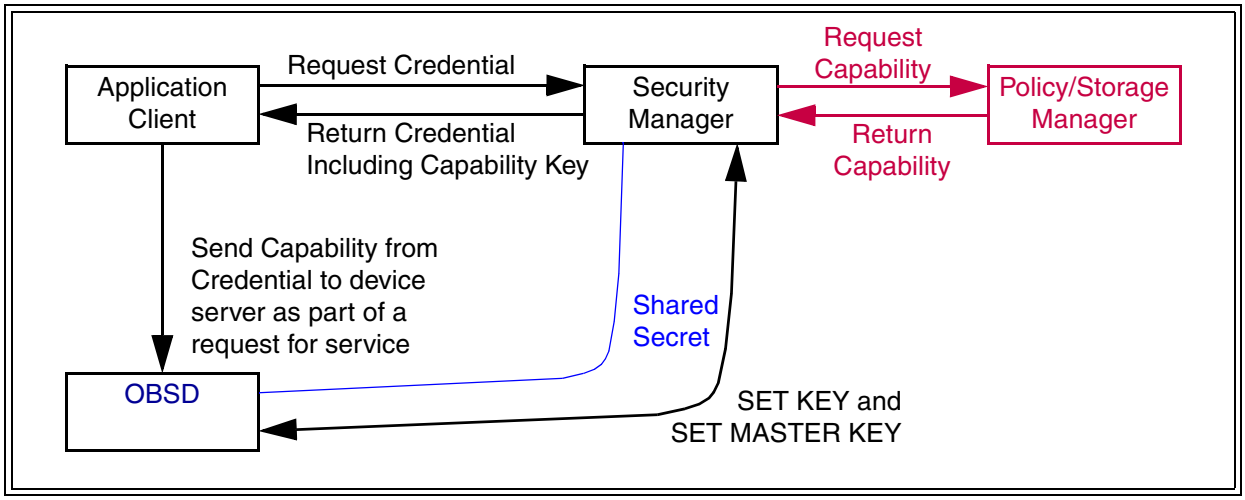

Figure 2 — OSD security model transactions

The security manager generates credentials, including capabilities prepared by the policy/storage manager, for authorized application clients at the request of an application client. The security manager returns a capability key with each credential. The credential gives the application client access to specific OSD components. The capability key allows the application client and device server to authenticate the commands and data they exchange with an integrity check value (see 4.9.7).

The protocol between the application client and the security manager is not defined by this standard. However, the structure of the credential returned from the security manager to the application client is.

If any security method except NOSEC is used, the device server validates each command received from an application client to confirm that:

a) The credential has not been tampered with (i.e., that the credential was generated by the security manager and includes an integrity check value using a secret key known only to the security manager and OSD device server); and
b) The credential was rightfully obtained by the application client from the security manager or through delegation by another application client (i.e., that the application client knows the capability key that is associated with the credential and has used the capability key to provide a proper integrity check value or values for the command).

The capability key allows the OSD device server to validate that an application client rightfully obtained a credential and that the capability has not been tampered with. An application client that has just the capability (e.g., obtained by monitoring CDBs sent to the OSD device server) but not the capability key is unable to generate commands with valid integrity check value, meaning that application client is denied access to the OSD logical unit. This protocol allows delegation of a credential if a application client delegates both the credential and the capability key.

The application client requests credentials and capability keys from the security manager for the command functions it needs to perform and sends those capabilities in those credentials to the OSD device server as part of commands that include an integrity check value using the capability key. While the application client is not trusted to follow this protocol, an application client that does not follow the protocol is unlikely to receive service from the OSD device server.

The security manager may authenticate the application client, but the OSD device server does not authenticate the application client. It is sufficient for the OSD device server to verify the capabilities and integrity check values sent by the application client.

The security manager maintains security policy information the definition of which is outside the scope of this standard.

4.9.2 Trust assumptions

This subclause describes how each component of the OSD security model trusts the other components.

The OBSD is a trusted component, meaning that once an application client authenticates that it is communicating with a specific OSD logical unit using methods outside the scope of this standard, it trusts the OBSD to:

a) Provide integrity for stored data;
b) Perform the security protocol and functions defined for it by this standard; and
c) Not be controlled in a way that operates to the detriment of the application client's interests.

The security manager is a trusted component. After the security manager is authenticated by the application client and by the OBSD using methods outside the scope of this standard, the security manager is trusted to:

a) Safely store long-lived keys;
b) Apply access controls correctly according to requirements that are outside the scope of this standard;
c) Perform the security functions defined for it by this standard; and
d) Not be controlled in a way that operates to the detriment of the application client's or OSD logical unit's interests.

The application client is not a trusted component. However, the OSD security model is defined so that the application client receives service from the OSD device server only if it interacts with both the security manager and the OSD device server in ways that assure the propriety of the application client's actions.

The OSD security model components are trusted to protect capability keys from disclosure to unauthorized entities.

The OSD security model components are trusted to maintain some degree of synchronization between their clocks. The OSD security model includes features designed to manage the dependency on the degree of clock synchronization maintained by application clients (see 4.9.6).

Regardless of where the security manager resides (see 4.4), communications between the security manager and other components are trusted based on the requirements shown in table 13.

Table 13 — Security manager communications trust requirements

Component	Security Manager communications trust requirement
OSD device server	Same as for any application client
Application client	Confidential [a]
Policy/storage manager	Message Integrity [b]

[a] Confidential communications shall be protected from eavesdropping by physical or cryptographic means.
[b] Message integrity assures that the message received is the one was sent (i.e., no tampering occurred). Messages in which tampering is detected are discarded.

4.9.m Preparing credentials

In response to a request from an application client, the security manager shall prepare and return a credential as follows:

1) Forward the access requests from the application client to the policy/storage manager. If the policy/storage manager denies the forwarded request an error shall be returned to the requesting application client;
2) Insert the capability returned by the policy/storage manager in the credential;
3) Set the credential OSD SYSTEM ID field to the value in the OSD system ID attribute in the Root Information attributes page (see 7.1.2.8) of the OSD logical unit to which the credential applies;
4) Set the capability SECURITY METHOD field as follows:
   A) Select a security method other than the partition default:
      a) If the application client requested use of a specific security method, and use of the requested security method is allowed by both the addressed partition and the maintained security policy information, set the capability SECURITY METHOD field to the requested value;
      b) If the maintained security policy information requires use of a specific security method for the requesting application client, set the capability SECURITY METHOD field to that value;

      or
   B) Use the partition default:
      a) If the application client requested a credential to be used in a SET KEY command (see 6.23) or a SET MASTER KEY command (see 6.24), set the capability SECURITY METHOD field to the value in the default security method attribute in the Root Policy/Security attributes page (see 7.1.2.20);
      b) Otherwise, set the capability SECURITY METHOD field to the value in the default security method attribute in the Partition Policy/Security attributes page (see 7.1.2.21) for the partition whose Partition ID is contained in the capability ALLOWED PARTITION_ID field;
5) If the SECURITY METHOD field contains NOSEC, place zero in the CREDENTIAL INTEGRITY CHECK VALUE field and return the credential to the application client;

   Otherwise:
6) Set the capability KEY VERSION field to the number of the working key secret key used to compute the credential integrity check value. If a secret key other than a working key is used to compute the credential integrity check value (e.g. for a SET KEY command (see 6.23) or SET MASTER KEY command (see 6.24)), then set the capability KEY VERSION field to zero ;
7) Set the capability INTEGRITY CHECK VALUE ALGORITHM field to the value that specifies the algorithm used to compute all integrity check values related to this credential . The algorithm shall be one of those identified by the supported integrity check value algorithm attributes in the Root Policy/Security attributes page (see 7.1.2.20) and the INTEGRITY CHECK VALUE ALGORITHM field shall be set as described in 7.1.2.20;
8) As specified by the maintained security policy information, modify other capability fields, including but not limited to the following:
   A) Setting the CAPABILITY EXPIRATION TIME field to a value that is consistent with the policy;
   B) Ensuring that the capability AUDIT field and CAPABILITY DISCRIMINATOR field contain non-zero values;
   C) Setting the capability OBJECT CREATED TIME field to a non-zero value as described in 4.x.2.2.1; and
   D) Ensuring that the POL/SEC bit in the PERMISSIONS BIT MASK field is set to zero, if appropriate;
9) Compute the credential integrity check value as described in 4.9.5.3 and place the result in the CREDENTIAL INTEGRITY CHECK VALUE field in the credential;

   and
10) Return the credential thus constructed to the application client with the credential integrity check value serving as the capability key.

Successful use of the capability expiration time (see step A) in step 8)) requires some degree of synchronization between the clocks of the device server and security manager. The protocol for synchronizing the clocks is outside the scope of this standard, however, the protocol should be implemented in a secure manner (e.g., it should not be possible for an adversary to set the clock in the device server backwards to enable the reuse of expired credentials).

4.9.3 Security methods

4.9.3.1 Introduction

This standard defines several security methods (see table 14).

Table 14 — OSD security methods

Security Method	Description	Reference
NOSEC	No security	4.9.3.2
CAPKEY	Integrity of capabilities	4.9.3.3
CMDRSP	Integrity of CDB, status, and sense data	4.9.3.4
ALLDATA	Integrity of all data in transit	4.9.3.5

The OSD security methods are designed to address zero or more specific security threats (see table 15).

Table 15 — Security methods and threats thwarted

Threat	Threat thwarted by security method				
		CAPKEY			
		Over secure channel [a]			
	NOSEC	No	Yes	CMDRSP	ALLDATA
Forgery of credential	No	Yes	Yes	Yes	Yes
Alteration of capabilities	No	Yes	Yes	Yes	Yes
Use of credential by unauthorized application client	No	Yes [b]	Yes [c]	Yes	Yes
Replay of command or status	No	No	Yes [c]	Yes	Yes
Alteration of command or status	No	No	Yes [c]	Yes	Yes
Replay of data	No	No	Yes [c]	No	Yes
Alteration of data	No	No	Yes [c]	No	Yes
Inspection of command, status or data	No	No	Yes/No [d]	No	No

[a] This model assumes that one secure channel supports no more than one I_T nexus and that I_T nexus is not shared by multiple application clients. If a SCSI initiator device allows multiple application clients to share an I_T nexus, then the SCSI initiator device implementation and/or application clients shall provide security guarantees equivalent to those provided by a secure channel.

[b] If more than one application client has access to an I_T nexus, then credentials are not protected from use by unauthorized application clients.

[c] A secure channel provides the following security guarantees:

a) Cryptographic integrity: Any message received is the one was sent (i.e., no tampering occurred). Messages in which tampering is detected are discarded;

b) Data origin authentication: The message received originated from the authenticated originator within the limits of the secure channel authentication mechanism;

c) Replay protection: The same message is not delivered multiple times and that there is a limited number of out-of-order messages.

[d] Optionally, a secure channel may provide a Data Confidentiality guarantee that if a message is read, it cannot be understood other than by the unauthorized parties.

4.9.3.2 The NOSEC security method

In the NOSEC security method, no OSD security features or algorithms are used by the device server. If the root object and all partitions in the OSD logical unit use the NOSEC security method, then:

a) Specific SPC-3 commands (e.g., LOG SENSE) may be sent (see table 41 in 6.1) without encapsulating them in the PERFORM SCSI COMMAND command (see 6.16); and
b) Persistent reservations (see 4.15) are allowed for the logical unit.

4.9.3.3 The CAPKEY security method

The CAPKEY security method validates the integrity of the capability information in each CDB.

The application client computes the CDB REQUEST INTEGRITY CHECK VALUE field (see 5.2.6) contents using:

a) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field (see 4.x.2.2);
b) The security token returned in the Security Token VPD page (see 7.5.3) ; and
c) The credential capability key (see 4.9.4.2).

The device server validates the credential as described in 4.9.5.1.

The CAPKEY security method is useful when the service delivery subsystem between the OSD device server and application client is secured via methods specified in the applicable SCSI transport protocol, with both the CAPKEY security method and SCSI transport protocol secure channel contributing to securing communications as shown in table 15 (see 4.9.3).

4.9.3.4 The CMDRSP security method

The CMDRSP security method validates the integrity of the CDB, status, and sense data for each command.

The application client computes the CDB REQUEST INTEGRITY CHECK VALUE field (see 5.2.6) contents using:

a) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field (see 4.x.2.2);
b) All the bytes in the CDB with the bytes in the REQUEST INTEGRITY CHECK VALUE field set to zero; and
c) The credential capability key (see 4.9.4.2).

The device server validates the credential as described in 4.9.5.1.

If the credential validation process successfully validates the integrity check value associated with the command, the device server shall:

1) Compute an integrity check value for the response data using:
   A) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field (see 4.x.2.2);
   B) The following array of bytes:
      1) The request nonce from the CDB (see 5.2.6);
      2) The status byte; and
      3) If the status is CHECK CONDITION, the sense data with the RESPONSE INTEGRITY CHECK VALUE field in the OSD response integrity check value sense data descriptor (see 4.13.x.y) set to zero;

   and
   C) The capability key (see 4.9.4.2) for the reconstructed credential (see 4.9.5.2);

   and
2) Place the computed integrity check value in the following location:
   A) If the status is not CHECK CONDITION, the computed integrity check value shall be placed in the response integrity check value attribute in the Current Command attributes page (see 7.1.2.24); or

B) If the status is CHECK CONDITION, the computed integrity check value shall be placed in the RESPONSE INTEGRITY CHECK VALUE field in the OSD response integrity check value sense data descriptor (see 4.13.x.y) in the sense data.

If the credential validation process fails to validate the integrity check value associated with the command, the device server shall place zero in the RESPONSE INTEGRITY CHECK VALUE field in the OSD response integrity check value sense data descriptor in the sense data.

If the status is not CHECK CONDITION, the application client validates the response integrity check value by recomputing it as described in this subclause and comparing the result to the value of the response integrity check value attribute in the Current Command attributes page.

If the status is CHECK CONDITION, the application client validates the response integrity check value by:

1) Saving the response integrity check value found in the RESPONSE INTEGRITY CHECK VALUE field in the OSD response integrity check value sense data descriptor in the sense data;
2) Placing zero in the response integrity check value found in the RESPONSE INTEGRITY CHECK VALUE field in the OSD response integrity check value sense data descriptor;
3) Recomputing the response integrity check value as described in this subclause; and
4) Comparing the result to the value saved in step 1).

If the application client fails in validating the response integrity check value as described in this subclause, it should take a recovery action not specified by this standard (e.g., one possible action is to request a new credential from the security manager and retry the command). If the error reoccurs, alternate recovery actions should be considered and the presence of malicious entities perpetrating a denial of service attack should be considered.

The CMDRSP security method may be used when the service delivery subsystem between the OSD device server and application client is not secured. The CMDRSP security method protects against corruption of the command, command parameter data, status, and sense data while avoiding the overhead that may be required to protect all transferred data. Use of the CMDRSP security method prevents an untrusted application client from forging, modifying or replaying a capability.

4.9.3.5 The ALLDATA security method

The ALLDATA security method validates the integrity of all data in transit between an application client and device server.

The application client computes the CDB REQUEST INTEGRITY CHECK VALUE field (see 5.2.6) contents using the same algorithm specified for the CMDRSP security method (see 4.9.3.4). The device server validates the credential as described in 4.9.5.1.

The application client also computes the data-out integrity check value using:

a) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field (see 4.x.2.2);
b) The used bytes in the following Data-Out Buffer segments (see 4.11.3):
    1) Command data or parameter data;
    2) Set attributes; and
    3) Get attributes;

    and
c) The credential capability key (see 4.9.4.2).

The application client places the data-out integrity information (see table 16) in the Data-Out Buffer starting at the byte specified by the CDB DATA-OUT INTEGRITY CHECK VALUE OFFSET field (see 5.2.6).

Table 16 — Data-out integrity information format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			NUMBER OF COMMAND OR PARAMETER BYTES				
7								(LSB)
8	(MSB)			NUMBER OF SET ATTRIBUTES BYTES				
15								(LSB)
16	(MSB)			NUMBER OF GET ATTRIBUTES BYTES				
23								(LSB)
24	(MSB)			DATA-OUT INTEGRITY CHECK VALUE				
43								(LSB)

The NUMBER OF COMMAND OR PARAMETER BYTES field specifies the number of bytes from the command data or parameter data segment that are included in the data-out integrity check value. If the value in the CDB LENGTH field, if any, or the value in the CDB PARAMETER LIST LENGTH field, if any, is larger than the value in the NUMBER OF COMMAND OR PARAMETER BYTES field, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The NUMBER OF SET ATTRIBUTES BYTES field specifies the number of bytes from the set attributes segment that are included in the data-out integrity check value. If the value in the CDB SET ATTRIBUTE LENGTH field, if any, or the value in the CDB SET ATTRIBUTES LIST LENGTH field, if any, is larger than the value in the NUMBER OF SET ATTRIBUTES BYTES field, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The NUMBER OF GET ATTRIBUTES BYTES field specifies the number of bytes from the get attributes segment that are included in the data-out integrity check value. If the value in the CDB GET ATTRIBUTES LIST LENGTH field, if any, is larger than the value in the NUMBER OF GET ATTRIBUTES BYTES field, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The DATA-OUT INTEGRITY CHECK VALUE field contains the data-out integrity check value computed by the application client.

The device server shall validate the data-out integrity check value by:

1) Computing an integrity check value using:
   A) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field;
   B) The following bytes from Data-Out Buffer:
      1) The number of bytes specified by the NUMBER OF COMMAND OR PARAMETER BYTES field starting at the Data-Out Buffer byte offset zero;
      2) The number of bytes specified by the NUMBER OF SET ATTRIBUTES BYTES field starting at the Data-Out Buffer byte offset specified by the CDB SET ATTRIBUTES LIST OFFSET field (see 5.2.1.3); and
      3) The number of bytes specified by the NUMBER OF GET ATTRIBUTES BYTES field starting at the Data-Out Buffer byte offset specified by the CDB GET ATTRIBUTES LIST OFFSET field (see 5.2.1.3); and

C) The capability key (see 4.9.4.2) for the reconstructed credential (see 4.9.5.2); and

2) Comparing the results to contents of the DATA-OUT INTEGRITY CHECK VALUE field.

If the validation fails, the state of the OSD objects and attributes shall not be altered in any detectable way, 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 DATA-OUT BUFFER INTEGRITY CHECK VALUE.

The device server shall compute the response integrity check value using the same algorithm specified for the CMDRSP security method (see 4.9.3.4) and the application client validates the response integrity check value using the same algorithm specified for the CMDRSP security method.

The device server shall compute the data-in integrity check value using:

a) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field;
b) The used bytes in the following Data-In Buffer segments (see 4.11.2):
   1) Command data or parameter data; and
   2) Retrieved attributes;
   and
c) The capability key (see 4.9.4.2) for the reconstructed credential (see 4.9.5.2).

The device server shall place the data-in integrity information (see table 17) in the Data-In Buffer starting at the byte specified by the CDB DATA-IN INTEGRITY CHECK VALUE OFFSET field (see 5.2.6).

Table 17 — Data-in integrity information format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			NUMBER OF COMMAND OR PARAMETER BYTES				
7								(LSB)
8	(MSB)			NUMBER OF RETRIEVED ATTRIBUTES BYTES				
15								(LSB)
16	(MSB)			DATA-IN INTEGRITY CHECK VALUE				
35								(LSB)

The NUMBER OF COMMAND OR PARAMETER BYTES field specifies the number of bytes from the command data or parameter data segment that are included in the data-in integrity check value.

The NUMBER OF RETRIEVED ATTRIBUTES BYTES field specifies the number of bytes from the retrieved attributes segment that are included in the data-in integrity check value.

The DATA-IN INTEGRITY CHECK VALUE field contains the data-in integrity check value computed by the device server.

After status has been received, the application client validates the data-in integrity check value by:

1) Computing an integrity check value using:
   A) The algorithm specified in the capability INTEGRITY CHECK VALUE ALGORITHM field;
   B) The following bytes from Data-In Buffer:
      1) The number of bytes specified by the NUMBER OF COMMAND OR PARAMETER BYTES field starting at the Data-In Buffer byte offset zero; and

2) The number of bytes specified by the NUMBER OF RETRIEVED ATTRIBUTES BYTES field starting at the Data-In Buffer byte offset specified by the CDB RETRIEVED ATTRIBUTES OFFSET field (see 5.2.1); and

C) The credential capability key (see 4.9.4.2); and

2) Comparing the results to contents of the DATA-IN INTEGRITY CHECK VALUE field.

If the application client fails in validating the data-in integrity check value, it should take a recovery action not specified by this standard (e.g., one possible action is to request a new credential from the security manager and retry the command). If the error reoccurs, alternate recovery actions should be considered and the presence of malicious entities perpetrating a denial of service attack should be considered.

The ALLDATA security method provides for applying integrity check values to every byte exchanged between the application client and OSD device server. Protection is provided against network attacks similar to those protected against by the security architecture for the internet protocol when confidentiality is not used (see RFC 2401), at the expense of computing and validating numerous integrity check values.

4.9.4 Credentials

4.9.4.1 Credential format

A credential (see table 18) is transferred from the security manager to an application client over a communications mechanism that meets the requirements specified in 4.9.2.

Table 18 — Credential format

Bit / Byte	7	6	5	4	3	2	1	0
0	Capability (see 4.x.2.2)							
79								
80	OSD SYSTEM ID							
99								
100	(MSB) CREDENTIAL INTEGRITY CHECK VALUE							
119								(LSB)

The capability is described in 4.x.2.2.

The OSD SYSTEM ID field specifies the value in the OSD system ID attribute in the Root Information attributes page (see 7.1.2.8) of the OSD logical unit to which the credential applies.

The CREDENTIAL INTEGRITY CHECK VALUE field contains an integrity check value (see 4.9.7) that is computed using the algorithm, inputs, and secret key specified in 4.9.5.3.

4.9.4.2 Capability key

All security methods except the NOSEC security method require the computation of one or more integrity check values using a capability key as the secret key (see 3.1.37).

For application clients, the capability key is the contents of the CREDENTIAL INTEGRITY CHECK VALUE field (see 4.9.4.1).

The device server processing of each command relies on only the capability portion of the credential (see 4.9.4.1) that the application client has copied into the CDB. Since the capability does not include the CREDENTIAL INTEGRITY CHECK VALUE field, the device server needs to compute the capability key for each processed command by:

1) Reconstructing the credential containing the CDB capability as described in 4.9.5.2; and
2) Computing the credential integrity check value for the reconstructed credential using the algorithm, inputs, and secret key specified in 4.9.5.3.

NOTE 1 The two steps used by the device server to compute capability key are the first two steps that the device server uses to validate the capability contained in the CDB (see 4.9.5.1). The device server may perform these two steps once for every command processed.

4.9.5 OSD device server security algorithms

4.9.5.1 Credential validation

The processes described in this subclause do not apply if the CDB SECURITY METHOD field specifies the NOSEC security method (i.e., if the CDB SECURITY METHOD field contains zero).

The device server shall validate the credential associated with a CDB by:

1) Reconstructing the credential containing the capability as described in 4.9.5.2;
2) Computing the credential integrity check value for the reconstructed credential using the algorithm, inputs, and secret key specified in 4.9.5.3;
3) Computing the request integrity check value using:
   A) The algorithm specified by the INTEGRITY CHECK VALUE ALGORITHM field in the capability;
   B) Based on the contents of the CDB SECURITY METHOD field, one of the following arrays of bytes:
      a) For the CAPKEY security method, the security token (see 4.9.3.2); or
      b) For the CMDRSP security method and the ALLDATA security method, all the bytes in the CDB with the bytes in the REQUEST INTEGRITY CHECK VALUE field set to zero;

      and
   C) The credential integrity check value computed in step 2) as the secret key;
4) Verifying that the request integrity check value matches the contents of the CDB REQUEST INTEGRITY CHECK VALUE field (see 5.2.6). If the contents in the request integrity check value field in the CDB do not match the computed integrity check value, 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; and
5) If the CDB SECURITY METHOD field specifies the CMDRSP security method or the ALLDATA security method, validate the CDB REQUEST NONCE field as described in 4.9.6.2.

If the validation of a credential results in a CHECK CONDITION status being returned, the state of the OSD objects and attributes shall not be altered .

4.9.5.2 Reconstructing the credential

The device server reconstructs a credential from a CDB capability by:

1) Copying the value in the OSD system ID attribute in the Root Information attributes page (see 7.1.2.8) to the OSD SYSTEM ID field of the reconstructed credential; and
2) Copying the capability from the CDB to the reconstructed credential.

The CREDENTIAL INTEGRITY CHECK VALUE field is not used in a reconstructed credential.

4.9.5.3 Computing the credential integrity check value

The credential integrity check value shall be computed using:

a) The algorithm specified by the INTEGRITY CHECK VALUE ALGORITHM FIELD in the capability;
b) The following bytes:
   A) All of the bytes in all of the fields defined for the credential (see 4.9.4.1);
   B) Except the bytes in the CREDENTIAL INTEGRITY CHECK VALUE field;
   and
c) The secret key selected as follows;
   A) If the OBJECT TYPE field in the capability (see 4.x.2.2) contains COLLECTION or USER, the secret key is the authentication working key:
      a) Identified by the KEY VERSION field in the capability; and
      b) Associated with the partition identified by the PARTITION_ID field in the CDB;
   B) If the OBJECT TYPE field in the capability contains ROOT or PARTITION and the command is not SET KEY and not SET MASTER KEY, the secret key is the authentication working key for partition zero identified by the KEY VERSION field in the capability;
   C) If the command is SET KEY, the secret key is selected as follows:
      a) If the KEY TO SET field in the CDB (see 6.23) contains 01b (i.e., update root key), the authentication master key;
      b) If the KEY TO SET field in the CDB contains 10b (i.e., update partition key), the authentication root key; or
      c) If the KEY TO SET field in the CDB contains 11b (i.e., update working key), the authentication partition key for the partition identified by the PARTITION_ID field in the CDB;
      or
   D) For the SET MASTER KEY command:
      a) For the seed exchange step (see 6.20.2), the authentication master key; or
      b) For the change master key step (see 6.20.3), the next authentication master key computed after GOOD status has been returned by the set master key seed step.

4.9.5.4 Invalidating credentials

The security manager may invalidate the credentials for one OSD object by requesting that the policy/storage manager change the policy access tag attribute in the policy/security attributes page associated with that OSD object (see 4.x) to a value other than the policy access tag value that is contained in the credential's capability.

The security manager may invalidate credentials for an entire partition by using the SET KEY command (see 6.23) to update the working key version used to compute the credential integrity check value in those credentials.

4.9.6 Request nonces

4.9.6.1 Request nonce format

For some security methods (see 4.9.3), an application client generated request nonce (see table 19) is included in the input data for each integrity check value computation (see 4.9.7) to thwart attempts to capture OSD commands (e.g., FORMAT OSD) and replay them.

Table 19 — Request nonce format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			TIMESTAMP				
5								(LSB)
6	(MSB)			RANDOM NUMBER				
11								(LSB)

The TIMESTAMP field contains the number of milliseconds that have elapsed since midnight, 1 January 1970 UT (see 3.1.47). Timestamp values should be coordinated with the contents of the clock attribute in the Root Information attributes page (see 7.1.2.8) using techniques that are outside the scope of this standard.

The RANDOM NUMBER field contains a random number generated from a good source of entropy (e.g., as described in RFC 1750).

If the security method being used does not require generation of request nonce values, the nonce TIMESTAMP field should contain zero.

4.9.6.2 Device server validation of request nonces

If the inputs to an integrity check value computation include a request nonce that is listed (see 4.9.6.3) as having been used in any previous integrity check value computation, 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 NONCE NOT UNIQUE. The command shall be terminated regardless of the success or failure of the previous command in which the duplicate request nonce appeared (e.g., the request nonce appearing in a WRITE command that ultimately fails due to insufficient quota or the request nonce appearing in a CREATE command that ultimately fails because the computed credential integrity check value is wrong shall not be accepted a second time).

If the command is being processed using the CMDRSP security method or the ALLDATA security method (see 4.9.3) and a request nonce with zero in the TIMESTAMP field is received, 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 request nonce timestamp is less than the contents of the clock attribute in the Root Information attributes page (see 7.1.2.8) minus the value in the oldest valid nonce attribute in the Partition Policy/Security attributes page (see 7.1.2.21), then the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and with the additional sense code set to NONCE TIMESTAMP OUT OF RANGE. If a command is terminated in this way, the current contents of the clock attribute in the Root Information attributes page shall be returned left-aligned and zero-padded (see 3.7.2) in the COMMAND-SPECIFIC INFORMATION field of the command-specific information sense data descriptor.

If the request nonce timestamp is greater than the contents of the clock attribute in the Root Information attributes page plus the value in the newest valid nonce attribute in the Partition Policy/Security attributes page (see 7.1.2.21), 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 NONCE TIMESTAMP OUT OF RANGE. If a command is terminated in this way, the current contents of the clock attribute in the Root Information attributes page shall be returned left-aligned and zero-padded (see 3.7.2) in the COMMAND-SPECIFIC INFORMATION field of the command-specific information sense data descriptor.

Successful use of the capability request nonces requires some degree of synchronization between the clocks of the device server and security manager. The protocol for synchronizing the clocks is outside the scope of this standard, however, the protocol should be implemented in a secure manner (i.e., it should not be possible for an adversary to set the clock in the device server backwards to enable the replay of expired credentials).

4.9.6.3 Lists of previously used request nonces

4.9.6.3.1 Introduction

The device server shall maintain a list of all request nonces used in integrity check value computations. Failure of the integrity check value computation shall not result in exclusion from the list.

A request nonce shall appear in the list from the time it is received until:

a) The time in the request nonce timestamp field is less than the value in the clock attribute in the Root Information attributes page (see 7.1.2.8) minus the value in the oldest valid nonce limit attribute in the Root Policy/Security attributes page (see 7.1.2.20);
b) The working key used to compute the integrity check value in which the request nonce was used is invalidated by a SET KEY command (see 6.19);
c) Optionally, the capability audit field is frozen (see 4.9.6.3.2); or
d) Optionally, the working key is frozen (see 4.9.6.3.3).

For the SET KEY command and the SET MASTER KEY command, the request nonce shall appear in the list from the time it is received until the time in the request nonce timestamp field is less than the value in the clock attribute in the Root Information attributes page minus the value in the oldest valid nonce limit attribute in the Root Policy/Security attributes page (i.e., only item a) applies to these commands).

The request nonce list depth attribute in the Root Policy/Security attributes page shall indicate the minimum number of request nonce list entries available to one application client.

4.9.6.3.2 Freezing capability audit fields

The device server may refuse to accept any additional commands containing a specific combination of capability AUDIT field and capability KEY VERSION field (see 4.x.2.2) values. If the device server takes this action, it should terminate the selected command and all future commands containing the selected combination of capability AUDIT field and capability KEY VERSION field values with a CHECK CONDITION status, a sense key set to ILLEGAL REQUEST, and an additional sense code set to SECURITY AUDIT VALUE FROZEN.

The device server may repeat the process described in this subclause as often as necessary to reduce the amount of resources required to implement the nonce listing requirements (see 4.9.6.3.1).

4.9.6.3.3 Freezing working keys

The device server may refuse to accept any additional commands with a capability KEY VERSION field (see 4.x.2.2) specifying a certain working key version value. If the device server takes this action, it:

a) Should terminate the selected command and all future commands having the selected capability key version value with a CHECK CONDITION status, a sense key set to ILLEGAL REQUEST, and an additional sense code set to SECURITY WORKING KEY FROZEN; and
b) Shall set to one the bit in the frozen working key bit mask attribute in the Partition Policy/Security attributes page (see 7.1.2.21) that corresponds to the working key version thus selected.

The device server may repeat the process described in this subclause as often as necessary to reduce the amount of resources required to implement the nonce listing requirements (see 4.9.6.3.1).

4.9.7 Integrity check values

An integrity check value is a value produced by a cryptographic function (e.g., HMAC-SHA1) based on a secret key (see 4.9.8) that is able to be computed and verified by the entities knowing the secret key. Integrity check values are used to verify that:

a) A collection of data fields contain correct values; and
b) The values in those data fields were prepared by the entity that created the integrity check value.

4.9.8 Secret keys

4.9.8.1 Introduction

The hierarchy of secret keys and the mechanisms for updating them are described in:

a) This subclause;
b) The definition of the SET MASTER KEY command, 6.24; and
c) The definition of the SET KEY command, 6.23.

In the OSD security model, the security of transactions depends on a hierarchy of secret keys as shown in table 20, with the highest key in the hierarchy (i.e., the master key) shown at the top of the table and the lowest keys in the hierarchy (i.e., the capability keys) shown at the bottom of the table.

Table 20 — OSD secret key hierarchy

Key Name	Key Shared Using	Key Used To	Key Update Frequency
Keys shared between the security manager and the OSD device server			
Master	SET MASTER KEY command	Update Root key	Change of logical unit owner
Root	SET KEY command	Update Partition key	When Partition key may have been compromised (i.e., very infrequently)
Partition [a]	SET KEY command	Update Working keys	When Working key updates may have been compromised (i.e., infrequently)
Working [b]	SET KEY command	Create Capability keys	When normal key use affords too much chance that the working key might be reverse engineered (i.e., regularly)
Keys shared between the security manager and the application client [c]			
Capability [d]	Credentials and mechanisms not specified in this standard	Secure commands, responses, and data	New with each new Credential

[a] For the purposes of the secret key hierarchy, the root object is treated the same as any other partition OSD object using partition zero.

[b] For each partition, up to sixteen working keys may be active at any time, uniquely identified by the capability KEY VERSION field (see 4.x.2.2).

[c] The device server is capable of computing the capability key (see 4.9.5.3) using the reconstructed credential (see 4.9.5.2).

[d] As a dual purpose number, the capability key is different from other keys in the hierarchy. The capability key is the credential integrity check value. Even though the security manager computes it, the computation is based on values beyond the security manager's control (e.g., the user object to which the credential allows access). While changing the working key used to construct the credential integrity check value invalidates the capability key, the credential may expire before that, making the capability key invalid.

Each master, root, and partition key represents two secret key values as follows:

a) An authentication key that is used to compute the credential integrity check values; and
b) A generation key that is used by future SET KEY commands and SET MASTER KEY commands to compute the updated generation key and new authentication key values.

When an OBSD is manufactured, both the master authentication key and master generation key values shall be provided for each logical unit. The values may be identical. The initial master keys should be generated as specified by FIPS 198 and the length of initial master keys should comply with FIPS 198.

The secret keys shared between the security manager and OSD device server are very secret information. They should be protected from being discovered by an adversary. They should be stored in a tamper resistant non-volatile manner and may be protected by a tamper resistant software shield. The master key shall be stored in a tamper resistant manner.

The seeds that have been used to create all secret keys other than the master key may be saved in nonvolatile memory for later use in recomputing the secret key values. The OSD logical unit should not store the commands sent to set the master key in a manner that has the potential for being externally accessible.

4.9.8.2 Computing updated generation keys and new authentication keys

The SET KEY command and SET MASTER KEY command shall perform the steps described in this subclause to compute new generation and authentication keys.

The inputs to the process are:

a) The input key value is one of the following:
   A) For a SET KEY command, the generation key from the next higher level in the key hierarchy shall be used (e.g., the root key generation key is used to create the first partition keys for a newly created partition), as selected by the KEY TO SET field in the CDB of that command; or
   B) For a SET MASTER KEY command, the previous master key generation key shall be used;
b) The seed value is one of the following:
   A) For a SET KEY command, the contents of the SEED field of the CDB for the command; or
   B) For a SET MASTER command key, the result of the seed exchange step (see 6.20.2);
   and
c) The integrity check value algorithm, as specified in the INTEGRITY CHECK VALUE ALGORITHM field in the capability in the CDB for the command.

The updated generation key shall be computed by performing the specified integrity check algorithm with the following inputs:

a) Input key value; and
b) Seed value.

The new authentication key shall be computed by performing the specified integrity check algorithm with the following inputs:

a) Input key value; and
b) Seed value with the least significant bit changed as follows:
   A) If the seed value least significant bit is zero, then it is changed to one; or
   B) If the seed value least significant bit is one, then it is changed to zero.

4.9.9 OSD security interactions with SPC-3 commands and SAM-3 task management functions

Persistent reservations (see 4.15) are incompatible with an OSD logical unit in which the root object or any partition is using any security method other than NOSEC (see 4.9.3).

Except for the INQUIRY command, the REPORT LUNS command, the REQUEST SENSE command, and the TEST UNIT READY command, all SPC-3 commands are invalid if addressed to an OSD logical unit in which any partition is using any security method other than NOSEC (see table 41 in 6.1). The PERFORM SCSI COMMAND command (see 6.16) allows SPC-3 commands other than persistent reservations commands to be performed under the protection of the current security method.

If the root object or any partition in the OSD logical unit is using any security method other than NOSEC, all SAM-3 task management functions except QUERY TASK shall be ignored and responded to as if they have been successfully processed . The PERFORM TASK MANAGEMENT FUNCTION command (see 6.17) allows SAM-3 task management functions to be processed under the protection of the current security method.

5.2 Fields commonly used in OSD commands

OSD commands employ the basic structure shown in table 21 for the service action specific fields (see table 19) so that the same field is in the same location in all OSD CDBs. Fields that are unique to one or two CDBs are not shown in table 21.

Table 21 — OSD service action specific fields

Bit / Byte	7	6	5	4	3	2	1	0
10	OPTIONS BYTE							
11	Reserved		GET/SET CDBFMT		Command specific options			
12	TIMESTAMPS CONTROL							
13	Reserved							
15								
16	(MSB)							
23	PARTITION_ID							(LSB)
24	(MSB)							
31	USER_OBJECT_ID							(LSB)
32	Reserved							
35								
36	(MSB)							
43	LENGTH							(LSB)
44	(MSB)							
51	STARTING BYTE ADDRESS							(LSB)
52	Get and set attributes parameters (see 5.2.1)							
79								
80	Capability (see 4.x.2.2)							
159								
160	Security parameters (see 5.2.6)							
199								

5.2.6 Security parameters

The CDB security parameters (see table 22) contain the security information needed for each command.

Table 22 — Security parameters format

Bit / Byte	7	6	5	4	3	2	1	0
				⋮ Other CDB fields				
159								
160	(MSB)			REQUEST INTEGRITY CHECK VALUE				
179								(LSB)
180				REQUEST NONCE				
191								
192				DATA-IN INTEGRITY CHECK VALUE OFFSET				
195								
196				DATA-OUT INTEGRITY CHECK VALUE OFFSET				
199								
				~~Capability (see 4.x.2.2)~~				

…

~~The capability is part of the credential (see 4.9.4) that the application client obtains from the security manager. The device server uses the capabilities along with other information to validate the command as described in 4.9.5.2. The format of a capability is defined in 4.x.2.2.~~

6.19 SET KEY

The SET KEY command (see table 23) causes the OSD device server to update the specified secret key.

Table 23 — SET KEY command

Bit / Byte	7	6	5	4	3	2	1	0
8	(MSB)							
9				SERVICE ACTION (8818h)				(LSB)
10	Reserved							
11	Reserved		GET/SET CDBFMT		Reserved		KEY TO SET	
12	TIMESTAMPS CONTROL							
13								
15				Reserved				
16	(MSB)							
23				PARTITION_ID				(LSB)
24	Reserved				KEY VERSION			
25	(MSB)							
31				KEY IDENTIFIER				(LSB)
32	(MSB)							
51				SEED				(LSB)
52								
79				Get and set attributes parameters (see 5.2.1)				
80								
159				Capability (see 4.x.2.2)				
160								
199				Security parameters (see 5.2.6)				

The GET/SET CDBFMT field specifies the format of the get and set attributes parameters as described in 5.2.1.

The contents of the TIMESTAMPS CONTROL field are defined in 5.2.8.

The KEY TO SET field (see table 24) specifies which key shall be updated, which key identifier shall be stored, and which keys shall be invalid following the SET KEY command.

Table 24 — Key to set code values

Value	Key to update	Key identifier attribute to store	Keys to invalidate
00b	Reserved		
01b	~~Drive~~ Root	The ~~drive~~ root key identifier attribute in the Root Policy/Security attributes page (see 7.1.2.20)	Previous ~~drive~~ root key, and all partition and working keys
10b	Partition	The partition key identifier attribute in the Partition Policy/Security attributes page (see 7.1.2.21)	Previous partition key, and all working keys
11b	Working	The working key identifier attribute in the Partition Policy/Security attributes page selected by the KEY VERSION field in the CDB	None

For every key that is invalidated by a SET KEY command, the associated key identifier attribute shall have its attribute length set to zero.

The contents of the PARTITION_ID field are defined in 5.2.4. If the KEY TO SET field contains 01b and the PARTITION_ID field contains a value other than 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 FIELD IN CDB.

The KEY VERSION field specifies the working key version to be updated. If the KEY TO SET field contains 01b or 10b, the KEY VERSION field shall be ignored.

The KEY IDENTIFIER field specifies a unique identifier to be associated with the new key. Successful processing of the SET KEY command shall include storing the key identifier value in the attribute specified in table 24.

The SEED field contains a random number generated from a good source of entropy (e.g., as described in RFC 1750). The updated key values shall be computed as described in 4.9.8.2.

~~If the least significant bit in the SEED field is set to one, the key values shall not be updated, 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 get and set attributes parameters are defined in 5.2.1. The format of the Data-In Buffer and Data-Out Buffer when attributes are being retrieved or set is described in 4.11.

The security parameters are defined in 5.2.6. The secret key whose authentication key shall be used to compute the capability key for this SET KEY command is specified in ~~4.9.8.2~~ 4.9.5.3.

6.20 SET MASTER KEY

6.20.1 Introduction

The SET MASTER KEY command (see table 25) causes the OSD device server to update the master key secret key.

Table 25 — SET MASTER KEY command

Bit / Byte	7	6	5	4	3	2	1	0
8	(MSB)							
9				SERVICE ACTION (8819h)				(LSB)
10				Reserved				
11	Reserved			GET/SET CDBFMT		Reserved		DH_STEP
12				TIMESTAMPS CONTROL				
13								
23				Reserved				
24				DH_GROUP				
25	(MSB)							
31				KEY IDENTIFIER				(LSB)
32	(MSB)							
35				PARAMETER LIST LENGTH				(LSB)
36	(MSB)							
39				ALLOCATION LENGTH				(LSB)
40								
51				Reserved				
52								
79				Get and set attributes parameters (see 5.2.1)				
80								
159				Capability (see 4.x.2.2)				
160								
199				Security parameters (see 5.2.6)				

The DH_STEP (Diffie-Hellman step) field (see table 26) specifies which step in the Diffie-Hellman exchange to process.

Table 26 — Diffie-Hellman exchange step values

Code	Name	Reference
00b	SEED EXCHANGE	6.20.2
01b	CHANGE MASTER KEY	6.20.3
10b to 11b	Reserved	

If a SET MASTER KEY command is received with the DH_STEP field set to CHANGE MASTER KEY and no SET MASTER KEY command has been received with the DH_STEP field set to SEED EXCHANGE on the same I_T_L nexus during the past ten seconds, 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.

A device server that receives a SET MASTER KEY command on one I_T_L nexus while the processing the DH_ steps on a different I_T_L nexus is incomplete may terminate the second SET MASTER KEY command with a CHECK CONDITION status, setting the sense key to ILLEGAL REQUEST and the additional sense code to SYSTEM RESOURCE FAILURE.

The usage of other CDB fields is specified in the description of each Diffie-Hellman step.

6.20.2 Seed exchange

The GET/SET CDBFMT field specifies the format of the get and set attributes parameters as described in 5.2.1.

The contents of the TIMESTAMPS CONTROL field are defined in 5.2.8.

The DH_GROUP field specifies the coded value selected from the Group Description list of coded values maintained by IANA (see http://www.iana.org/assignments/ipsec-registry) that identifies the DH_generator and DH_prime values to be used for the SEED EXCHANGE step. If the value in the DH_GROUP field does not appear in one of the DH group attributes in the Root Policy/Security attributes page (see 7.1.2.20) 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 KEY IDENTIFIER field is reserved for the SEED EXCHANGE step.

The PARAMETER LIST LENGTH field specifies the number of bytes of application client DH_data to be sent to the device server. The application client DH_data is computed as follows:

1) A random number, x, is generated having a value between 0 and DH_prime minus one observing the requirements in RFC 1750; and
2) The application client DH_data is equal to DH_generator^{x} modulo DH_prime, where the DH_generator and DH_prime values are identified by the code value in the CDB DH_GROUP field.

The ALLOCATION LENGTH field specifies the number of bytes available to receive the device server DH_data (see table 27) sent in response to the SET MASTER KEY command. If the allocation length is not sufficient to contain device sever DH_data, 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 27 — Device server DH_data format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				RESPONSE LENGTH (n-3)				(LSB)
4								
n				DEVICE SERVER DH_DATA				

The RESPONSE LENGTH field indicates the number of bytes of device server DH_data that follow.

The DEVICE SERVER DH_DATA field contains the DH_data computed by the device server as follows:

1) A random number, y, is generated having a value between 0 and DH_prime minus one observing the requirements in RFC 1750; and
2) The device server DH_data is equal to DH_generator^{y} modulo DH_prime, where the DH_generator and DH_prime values are identified by the code value in the CDB DH_GROUP field.

The get and set attributes parameters are defined in 5.2.1. The format of the Data-In Buffer and Data-Out Buffer when attributes are being retrieved or set is described in 4.11.

The security parameters are defined in 5.2.6. The authentication master key (see 4.9.5.3) shall be used to compute the capability key for this SET MASTER KEY command ~~4.9.8.2~~.

After GOOD status has been returned for the SET MASTER KEY command SEED EXCHANGE step and before the SET MASTER KEY command CHANGE MASTER KEY step is processed, the next authentication master key and next generation master key shall be computed as described in 4.9.8.2, using a seed value that is the concatenation of the following:

1) DH_generator^{xy} modulo DH_prime;
2) The contents of the OSD system ID attribute in the Root Information attributes page (see 7.1.2.8);
3) The contents of the product model attribute in the Root Information attributes page;
4) The contents of the serial number attribute in the Root Information attributes page;
5) The contents of the OSD name attribute in the Root Information attributes page; and
6) The contents of the username attribute in the Partition Information attributes page (see 7.1.2.9).

6.20.3 Change master key

The GET/SET CDBFMT field specifies the format of the get and set attributes parameters as described in 5.2.1.

The contents of the TIMESTAMPS CONTROL field are defined in 5.2.8.

The DH_GROUP field is reserved for the CHANGE MASTER KEY step.

The KEY IDENTIFIER field specifies a unique identifier to be associated with the new master key. Successful processing of the SET MASTER KEY command CHANGE MASTER KEY step shall include storing the key identifier value in the master key identifier attribute in the Root Policy/Security attributes page (see 7.1.2.20).

The PARAMETER LIST LENGTH field specifies the number of bytes in the CHANGE MASTER KEY parameter list (see table 28). If the parameter list length causes truncation of any field in the CHANGE MASTER KEY parameter list, 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.

Table 28 — Change master key DH_data format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			APPLICATION CLIENT DH_DATA LENGTH (k-3)				
3								(LSB)
4				APPLICATION CLIENT DH_DATA				
k								
k+1	(MSB)			DEVICE SERVER DH_DATA LENGTH (n-(k+4))				
k+4								(LSB)
k+5				DEVICE SERVER DH_DATA				
n								

The APPLICATION CLIENT DH_DATA LENGTH field specifies the number of bytes that follow in the APPLICATION CLIENT DH_DATA field.

The APPLICATION CLIENT DH_DATA field contains the application client DH_data from the SEED EXCHANGE step.

The DEVICE SERVER DH_DATA LENGTH field specifies the number of bytes that follow in the DEVICE SERVER DH_DATA field.

The DEVICE SERVER DH_DATA field contains the device server DH_data from the SEED EXCHANGE step.

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 CHANGE MASTER KEY parameter data fails to compare in any of the following ways with the data exchanged in the SEED EXCHANGE step that was most recently processed on this I_T_L nexus since a I_T nexus loss event, logical unit reset event, or reset event (see SAM-3), if any:

a) The contents of the APPLICATION CLIENT DH_DATA LENGTH field do not match the contents of the PARAMETER LIST LENGTH field in the SEED EXCHANGE step;
b) The contents of the APPLICATION CLIENT DH_DATA field do not match the contents of the parameter data in the SEED EXCHANGE step;
c) The contents of the DEVICE SERVER DH_DATA LENGTH field do not match the contents of the RESPONSE LENGTH field in the SEED EXCHANGE step; or
d) The contents of the DEVICE SERVER DH_DATA field do not match the contents of the DEVICE SERVER DH_DATA field in the SEED EXCHANGE step.

The ALLOCATION LENGTH field is reserved for the CHANGE MASTER KEY step.

The get and set attributes parameters are defined in 5.2.1. The format of the Data-In Buffer and Data-Out Buffer when attributes are being retrieved or set is described in 4.11.

The security parameters are defined in 5.2.6. The next authentication master key computed after the return of GOOD status for the most recent SET MASTER KEY command SEED EXCHANGE step (see 6.20.2) shall be used to compute the capability key for this SET MASTER KEY command.

Successful processing of a SET MASTER KEY command CHANGE MASTER KEY step shall:

a) Replace the authentication master key with the next authentication master key computed after the return of GOOD status for the most recent SET MASTER KEY command SEED EXCHANGE step (see 6.20.2);
b) Replace the generation master key with the next generation master key computed after the return of GOOD status for the most recent SET MASTER KEY command SEED EXCHANGE step;
c) Invalidate all of the following keys (see 4.9.8):
    a) The ~~drive~~ root key;
    b) The partition key for every partition on the OSD logical unit; and
    c) Every working key in every partition on the OSD logical unit.

For every key that is invalidated by a SET MASTER KEY command CHANGE MASTER KEY step, the associated key identifier attribute shall have its attribute length set to zero.

7.1.2 OSD attributes pages

7.1.2.1 Attributes pages overview

...

The attributes pages defined by this standard are shown in table 29.

Table 29 — Attributes pages defined by this standard

Page Number	Page Name	Reference	Page Format Defined	Support Requirements
0h	User Object Directory	7.1.2.7	No	Mandatory
1h	User Object Information	7.1.2.11	No	Mandatory
2h	User Object Quotas	7.1.2.14	Yes	Mandatory
3h	User Object Timestamps	7.1.2.18	Yes	Mandatory
4h	Collections	7.1.2.19	Yes	Optional
5h	User Object Policy/Security	7.1.2.23	Yes	Mandatory
6h to 7Fh	Reserved			
C+0h	Collection Directory	7.1.2.6	No	Mandatory
C+1h	Collection Information	7.1.2.10	No	Mandatory
C+2h	Reserved			
C+3h	Collection Timestamps	7.1.2.17	Yes	Mandatory
C+4h	Reserved			
C+5h	Collection Policy/Security	7.1.2.22	Yes	Mandatory
C+6h to C+7Fh	Reserved			
P+0h	Partition Directory	7.1.2.5	No	Mandatory
P+1h	Partition Information	7.1.2.9	No	Mandatory
P+2h	Partition Quotas	7.1.2.13	Yes	Mandatory
P+3h	Partition Timestamps	7.1.2.16	Yes	Mandatory
P+4h	Reserved			
P+5h	Partition Policy/Security	7.1.2.21	Yes	Mandatory
P+6h to P+7Fh	Reserved			
R+0h	Root Directory	7.1.2.4	No	Mandatory
R+1h	Root Information	7.1.2.8	No	Mandatory
R+2h	Root Quotas	7.1.2.12	Yes	Mandatory
R+3h	Root Timestamps	7.1.2.15	Yes	Mandatory
R+4h	Reserved			
R+5h	Root Policy/Security	7.1.2.20	Yes	Mandatory
R+6h to R+7Fh	Reserved			
F000 0000h to FFFF FFFDh	Reserved			
FFFF FFFEh	Current Command	7.1.2.24	Yes	Mandatory

7.1.2.20 Root Policy/Security attributes page

The Root Policy/Security attributes page (R+5h) shall contain the attributes listed in table 30.

Table 30 — Root Policy/Security attributes page contents

Attribute Number	Length (bytes)	Attribute	Application Client Settable	OSD Logical Unit Provided
0h	40	Page identification	No	Yes
1h	1	Default security method	Yes	Yes
2h	6	Oldest valid nonce limit	No	Yes
3h	6	Newest valid nonce limit	No	Yes
4h to 5h		Reserved	No	
6h	1	Partition default security method	Yes	Yes
7h	2	Supported security methods	No	Yes
8h		Reserved	No	
9h	6	Adjustable clock	Yes	Yes
Ah to 7FFCh		Reserved	No	
7FFDh	0 or 7	Master key identifier	No	Yes
7FFEh	0 or 7	Root key identifier	No	Yes
7FFFh to 7FFF FFFFh		Reserved	No	
8000 0000h to 8000 000Fh	1	Supported integrity check value algorithm	No	Yes
8000 0010h to 8000 001Fh	1	Supported DH group	No	Yes
8000 0020h to FFFF FFFEh		Reserved	No	

The page identification attribute (number 0h) shall have the format described in 7.1.2.2 with the VENDOR IDENTIFICATION field containing the ASCII characters "INCITS" and the ATTRIBUTES PAGE IDENTIFICATION field containing the ASCII characters "T10 Root Policy/Security".

The default security method attribute (number 1h) specifies the security method (see table 35 in 7.1.2.21) used for the processing of the SET KEY command (see 6.23) and SET MASTER KEY command (see 6.24) in the absence of conditions that specify a different security method (see 4.9.m). The value of the default security method attribute shall not be changed by a FORMAT OSD command (see 6.9). The value placed in the default security method attribute when the OBSD (see 3.1.26) is manufactured is vendor specific. If the value of the default security method attribute is changed, the working keys for partition zero should be invalidated using the SET KEY command.

The oldest valid nonce limit attribute (number 2h) specifies the largest value allowed in the oldest valid nonce attribute in any Partition Policy/Security attributes page (see 7.1.2.21) (i.e., the maximum number of milliseconds prior to the value in the clock attribute in the Root Information attributes page (see 7.1.2.8) to which the device server constrains the contents of the TIMESTAMP field in a request nonce (see 4.9.6)).

The newest valid nonce limit attribute (number 3h) specifies the largest value allowed in the newest valid nonce attribute in any Partition Policy/Security attributes page (i.e., the maximum number of milliseconds subsequent to the value in the clock attribute in the Root Information attributes page to which the device server constrains the contents of the TIMESTAMP field in a request nonce).

The partition default security method attribute (number 6h) specifies the value to be placed in the default security method attribute of each partition, when it is created. The value of the partition default security method attribute shall not be changed by a FORMAT OSD command (see 6.9). The value placed in the partition default security method attribute when the OBSD is manufactured is vendor specific.

The supported security methods attribute (number 7h) indicates which security methods (see 4.9.3) are supported by the OSD logical unit (see table 31).

Table 31 — Supported security methods attribute format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved				ALLDATA	CMDRSP	CAPKEY	NOSEC
1	Reserved							

The NOSEC (NOSEC security method supported) bit is set to zero if the NOSEC security method is not supported. The NOSEC bit is set to one if the NOSEC security method is supported.

The CAPKEY (CAPKEY security method supported) bit is set to zero if the CAPKEY security method is not supported. The CAPKEY bit is set to one if the CAPKEY security method is supported.

The CMDRSP (CMDRSP security method supported) bit is set to zero if the CMDRSP security method is not supported. The CMDRSP bit is set to one if the CMDRSP security method is supported.

The ALLDATA (ALLDATA security method supported) bit is set to zero if the ALLDATA security method is not supported. The ALLDATA bit is set to one if the ALLDATA security method is supported.

The adjustable clock attribute (number 9h) shall contain the current time in use by the OSD device server represented as the count of the number of milliseconds elapsed since midnight, 1 January 1970 UT (see 3.1.47). The value shall be set to the UT when the OBSD (see 3.1.26) is manufactured and may be modified by the application client after that. The mechanism used to maintain the adjustable clock attribute value is outside the scope of the standard. The adjustable clock attribute value should not gain or lose more than one second in any 24-hour interval.

The master key identifier attribute (number 7FFDh) contains the key identifier value from the most recent successful SET MASTER KEY command (see 6.24). If a SET MASTER KEY command has never been processed, the master key identifier attribute length shall be seven and the master key identifier attribute value shall be the ASCII characters "1st key".

The root key identifier attribute (number 7FFEh) contains the key identifier value from the most recent successful SET KEY command (see 6.23) with the KEY TO SET field set to 01b (i.e., update root key). If the root key is invalid (i.e., never set or invalidated by a SET MASTER KEY command), the root key identifier attribute length shall be zero. Regardless of the root key identifier attribute length, the used capacity attribute in the Partition Information attributes page (see 7.1.2.9) for partition zero (see 3.1.31) shall reflect an attribute length of seven (i.e., it shall not be possible for a SET KEY command to cause the partition zero used capacity attribute value to exceed the capacity quota attribute in the Partition Quotas attributes page (see 7.1.2.13) for partition zero and generate a quote error).

The supported integrity check value algorithm attributes (numbers 8000 0000h to 8000 000Fh) contain coded values (see table 32) identifying the supported algorithms that the OSD device server supports for computing integrity check values. The supported integrity check value algorithm with the lowest valued attribute number (i.e., 8000 0000h) identifies the most preferred integrity check value algorithm and the highest valued attribute number (i.e., 8000 000Fh) identifies the least preferred algorithm. If a supported integrity check value algorithm attribute contains zero, then all supported integrity check value algorithm attributes with higher valued attribute numbers also shall contain zero. The low order four bits of the attribute number are the value that appears in the INTEGRITY CHECK VALUE ALGORITHM field (see 4.x.2.2) in each capability (e.g., attribute number 8000 0007h identifies the integrity check value algorithm used if the INTEGRITY CHECK VALUE ALGORITHM field contains seven).

Table 32 — Supported integrity check value algorithm codes

Value	Algorithm	Reference
00h	No algorithm supported	
01h	HMAC-SHA1	FIPS 180-1 (1995) and FIPS 198 (2002)
02h - DFh	Reserved	
E0h - FFh	Vendor specific	

The supported DH group attributes (numbers 8000 0010h to 8000 001Fh) contain coded values identifying the supported values in the DH_GROUP field of a SET MASTER KEY command (see clause 6.20). The values of the supported DH group attributes are the values associated with the Group Description class (i.e., class code value 4) in the Internet Key Exchange Attributes registry maintained by IANA (see http://www.iana.org/assignments/ipsec-registry). The DH group indicated by each value is as specified by IANA in that registry.

Every DH group identified by a supported DH group attribute shall be a MODP DH group. The code values 1h (i.e., the 768-bit MODP DH group defined by RFC 2409) and 2h (i.e., the 1024-bit MODP DH group defined by RFC 2409) shall not appear in any supported DH group attribute.

NOTE 2 The constraint to MODP DH groups eliminates usage of all elliptic curve DH groups (e.g., the DH groups having code values 3, 4, and 6 through 13, inclusive).

One of the supported DH group attributes shall contain Dh (i.e., 14) indicating the 2048-bit MODP DH group defined by RFC 3526.

The supported DH group with the lowest valued attribute number (i.e., 8000 0000h) identifies the most preferred DH group and the highest valued attribute number (i.e., 8000 000Fh) identifies the least preferred DH group. If a supported DH group attribute contains zero, then all supported DH group attributes with higher valued attribute numbers also shall contain zero

If a set attributes list (see 5.2.1.3) contains an entry specifying the number of an attribute that table 30 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field (see 5.2.1.2) specifies the number of an attribute that table 30 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The page format for the Root Policy/Security attributes page is shown in table 33.

Table 33 — Root Policy/Security attributes page format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				PAGE NUMBER (R+5h)				(LSB)
4	(MSB)							
7				PAGE LENGTH (3Fh)				(LSB)
8				DEFAULT SECURITY METHOD				
9				PARTITION DEFAULT SECURITY METHOD				
10								
11				SUPPORTED SECURITY METHODS				
12	(MSB)							
17				OLDEST VALID NONCE LIMIT				(LSB)
18	(MSB)							
23				NEWEST VALID NONCE LIMIT				(LSB)
24				Reserved			MKI_VALID	RKI_VALID
25	(MSB)							
31				MASTER KEY IDENTIFIER				(LSB)
32	(MSB)							
38				ROOT KEY IDENTIFIER				(LSB)
39				Most preferred SUPPORTED INTEGRITY CHECK VALUE ALGORITHM (attribute number 8000 0000h)				
				⋮				
54				Least preferred SUPPORTED INTEGRITY CHECK VALUE ALGORITHM (attribute number 8000 000Fh)				
55				Most preferred SUPPORTED DH GROUP (attribute number 8000 0010h)				
				⋮				
70				Least preferred SUPPORTED DH GROUP (attribute number 8000 001Fh)				

The PAGE NUMBER field contains the attributes page number of the Root Policy/Security attributes page.

The PAGE LENGTH field contains the number of additional bytes in the page format of the Root Policy/Security attributes page.

The OLDEST VALID NONCE LIMIT field contains the value of the oldest valid nonce limit attribute.

The NEWEST VALID NONCE LIMIT field contains the value of the newest valid nonce limit attribute.

The DEFAULT SECURITY METHOD field contains the value of the default security method attribute.

The PARTITION DEFAULT SECURITY METHOD field contains the value of the partition default security method attribute.

The SUPPORTED SECURITY METHODS field contains the value of the supported security methods attribute.

The MKI_VALID (master key identifier valid) bit shall be set to zero if the master key identifier attribute length is zero. Otherwise, the MKI_VALID bit shall be set to one.

The RKI_VALID (root key identifier valid) bit shall be set to zero if the root key identifier attribute length is zero. Otherwise, the RKI_VALID bit shall be set to one.

If the MKI_VALID bit is set to one, the MASTER KEY IDENTIFIER field contains the value of the master key identifier attribute. Otherwise, the contents of the MASTER KEY IDENTIFIER field are undefined.

If the DKI_VALID bit is set to one, the ROOT KEY IDENTIFIER field contains the value of the root key identifier attribute. Otherwise, the contents of the ROOT KEY IDENTIFIER field are undefined.

The sixteen SUPPORTED INTEGRITY CHECK VALUE ALGORITHM fields contain the supported integrity check value attribute values in ascending attribute number order. The SUPPORTED INTEGRITY CHECK VALUE ALGORITHM field with the smallest byte offset in the page identifies the most preferred integrity check value algorithm. The SUPPORTED INTEGRITY CHECK VALUE ALGORITHM field with the largest byte offset in the page identifies the least preferred algorithm.

The sixteen SUPPORTED DH GROUP fields contain the supported DH group attribute values in ascending attribute number order. The SUPPORTED DH GROUP field with the smallest byte offset in the page identifies the most preferred DH group to be used by the SET MASTER KEY command (see clause 6.20). The SUPPORTED DH GROUP field with the largest byte offset in the page identifies the least preferred DH group.

7.1.2.21 Partition Policy/Security attributes page

The Partition Policy/Security attributes page (P+5h) shall contain the attributes listed in table 34.

Table 34 — Partition Policy/Security attributes page contents

Attribute Number	Length (bytes)	Attribute	Application Client Settable	OSD Logical Unit Provided
0h	40	Page identification	No	Yes
1h	1	Default security method	Yes	Yes
2h	6	Oldest valid nonce	Yes	Yes
3h	6	Newest valid nonce	Yes	Yes
4h	2	Request nonce list depth	No	Yes
5h	2	Frozen working key bit mask	No	Yes
6h to 7FFEh		Reserved	No	
7FFFh	0 or 7	Partition key identifier	No	Yes
8000h to 4000 0000h	0 or 7	Working key identifier	No	Yes
4000 0001h	4	Policy access tag	Yes	Yes
4000 0002h	4	User object policy access tag	Yes	Yes
4000 0003h to FFFF FFFEh		Reserved	No	

The page identification attribute (number 0h) shall have the format described in 7.1.2.2 with the VENDOR IDENTIFICATION field containing the ASCII characters "INCITS" and the ATTRIBUTES PAGE IDENTIFICATION field containing the ASCII characters "T10 Partition Policy/Security".

The default security method attribute (number 1h) specifies the security method (see table 35) used for the processing of all commands except the SET KEY command and SET MASTER KEY command in the absence of conditions that specify a different security method (see 4.9.m).

Table 35 — Security method attribute values

Value	Security Method	Reference
00h	NOSEC	4.9.3.2
01h	CAPKEY	4.9.3.3
02h	CMDRSP	4.9.3.4
03h	ALLDATA	4.9.3.5
04h to FFh	Reserved	

A CREATE PARTITION command (see 6.7) shall copy the partition security method attribute from the Root Policy/Security attributes page (see 7.1.2.20) to the security method attribute in new Partition Policy/Security attributes page. The value of the security method attribute for partition zero shall not be changed by a FORMAT OSD command (see 6.9). The value placed in the security method attribute for partition zero when the OBSD (see 3.1.26) is manufactured is vendor specific. If the value of the security method attribute is changed, the working keys for affected partition should be invalidated using the SET KEY command (see 6.23).

The oldest valid nonce attribute (number 2h) indicates the number of milliseconds prior to the value in the clock attribute in the Root Information attributes page (see 7.1.2.8) to which the device server constrains the contents of the TIMESTAMP field in a request nonce (see 4.9.6) received in a command addressed to the partition, a collection in the partition, or a user object in the partition. The processing of request nonces affected by this constraint is described in 4.9.6.2.

If a set attributes list (see 5.2.1.3) contains a request to set the oldest valid nonce attribute to a value that is larger than the value in the oldest valid nonce limit attribute in the Root Policy/Security attributes page (see 7.1.2.20), the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field contains 2h (i.e., the oldest valid nonce attribute) and the set attributes data specified by the SET ATTRIBUTES OFFSET field (see 5.2.1.2) contains a value that is larger than the value in the oldest valid nonce limit attribute in the Root Policy/Security attributes page, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The newest valid nonce attribute (number 3h) indicates the number of milliseconds later than the value in the clock attribute in the Root Information attributes page to which the device server constrains the contents of the TIMESTAMP field in a request nonce (see 4.9.6) received in a command addressed to the partition, a collection in the partition, or a user object in the partition. The processing of request nonces affected by this constraint is described in 4.9.6.2 .

If a set attributes list (see 5.2.1.3) contains a request to set the newest valid nonce attribute to a value that is larger than the value in the newest valid nonce limit attribute in the Root Policy/Security attributes page, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field contains 3h (i.e., the newest valid nonce attribute) and the set attributes data specified by the SET ATTRIBUTES OFFSET field (see 5.2.1.2) contains a value that is larger than the value in the newest valid nonce limit attribute in the Root Policy/Security attributes page, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The request nonce list depth attribute (number 4h) shall contain the minimum number of request nonce list entries (see 4.9.6.3) available to one application client.

The frozen working key bit mask attribute (number 5h) indicates which working key versions (see table 36) have been frozen as part of request nonce list processing (see 4.9.6.3.3).

Table 36 — Frozen working key bit mask attribute format

Bit / Byte	7	6	5	4	3	2	1	0
0	WK07_FZN	WK06_FZN	WK05_FZN	WK04_FZN	WK03_FZN	WK02_FZN	WK01_FZN	WK00_FZN
1	WK0F_FZN	WK0E_FZN	WK0D_FZN	WK0C_FZN	WK0B_FZN	WK0A_FZN	WK09_FZN	WK08_FZN

A WK00_FZN (working key 0h frozen) bit set to zero indicates that device server is not rejecting commands that contain capabilities with the working key with a key version of zero as part of request nonce list processing (see 4.9.6.3.3). A WK00_FZN bit set to one indicates that device server is rejecting commands that contain capabilities with the working key with a key version of zero as part of request nonce list processing. Once the WK00_FZN bit is set to one, it shall not be set to zero until a new working key with key version zero is established using the SET KEY command (see 6.19).

The WK01_FZN bit, WK01_FZN bit, WK02_FZN bit, WK03_FZN bit, WK04_FZN bit, WK05_FZN bit, WK06_FZN bit, WK07_FZN bit, WK08_FZN bit, WK09_FZN bit, WK0A_FZN bit, WK0B_FZN bit, WK0C_FZN bit, WK0D_FZN bit, WK0E_FZN

bit, and WK0F_FZN have the same bit value definitions as the WK00_FZN bit, except that the definitions apply to the working keys with key versions one to fifteen, respectively.

The partition key identifier attribute (number 7FFFh) contains the key identifier value from the most recent successful SET KEY command (see 6.23) with the KEY TO SET field set to 10b (i.e., update partition key). If the partition key is invalid (i.e., never set, invalidated by a SET MASTER KEY command (see 6.24), or invalidated by a SET KEY command), the partition key identifier attribute length shall be zero. Regardless of the partition key identifier attribute length, the used capacity attribute in the Partition Information attributes page (see 7.1.2.9) shall reflect an attribute length of seven (i.e., it shall not be possible for a SET KEY command to cause the partition's used capacity attribute value to exceed the capacity quota attribute in the Partition Quotas attributes page (see 7.1.2.13) and generate a quote error).

The working key identifier attributes (numbers 8000h to 800Fh) contain the key identifier value from the most recent successful SET KEY command with:

a) The KEY TO SET field set to 11b (i.e., update working key); and
b) The KEY VERSION field set to the attribute number minus 8000h (e.g., a version key of three sets attribute 8003h and a version key of eight sets attribute 8008h).

If a working key is invalid (i.e., never set, invalidated by a SET MASTER KEY command, or invalidated by a SET KEY command), the working key identifier attribute length for the associated working key shall be zero. Regardless of the lengths of any of the working key identifier attributes, the used capacity attribute in the Partition Information attributes page shall reflect an attribute length of seven for all sixteen working key identifier attributes (i.e., it shall not be possible for a SET KEY command to cause the partition's used capacity attribute value to exceed the capacity quota attribute in the Partition Quotas attributes page and generate a quote error).

The policy access tag attribute (number 4000 0001h) specifies the expected non-zero contents of the POLICY ACCESS TAG field in any capability (see 4.x.2.2) that allows access to this partition. The format, use, and attribute setting restrictions for the policy access tag attribute are described in 4.x.3. A CREATE PARTITION command (see 6.7) shall set the policy access tag attribute to 7FFF FFFFh.

The user object policy access tag attribute (number 4000 0002h) specifies the value to be placed in the policy access tag attribute of each collection or user object, when it is created. A CREATE PARTITION command (see 6.7) shall set the user object policy access tag attribute to 7FFF FFFFh.

If a set attributes list contains an entry specifying the number of an attribute that table 34 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field specifies the number of an attribute that table 34 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The page format for the Partition Policy/Security attributes page is shown in table 37.

Table 37 — Partition Policy/Security attributes page format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				PAGE NUMBER (P+5h)				(LSB)
4	(MSB)							
7				PAGE LENGTH (8Fh)				(LSB)
8								
10				Reserved				
11				DEFAULT SECURITY METHOD				
12	(MSB)							
17				OLDEST VALID NONCE				(LSB)
18	(MSB)							
23				NEWEST VALID NONCE				(LSB)
24	(MSB)							
25				REQUEST NONCE LIST DEPTH				(LSB)
26								
27				FROZEN WORKING KEY BIT MASK				
28	(MSB)							
31				POLICY ACCESS TAG				(LSB)
32	(MSB)							
35				USER OBJECT POLICY ACCESS TAG				(LSB)
36				Reserved				PKI_VALID
37	WKI07_VLD	WKI06_VLD	WKI05_VLD	WKI04_VLD	WKI03_VLD	WKI02_VLD	WKI01_VLD	WKI00_VLD
38	WKI0F_VLD	WKI0E_VLD	WKI0D_VLD	WKI0C_VLD	WKI0B_VLD	WKI0A_VLD	WKI09_VLD	WKI08_VLD
39	(MSB)							
45				PARTITION KEY IDENTIFIER				(LSB)
46	(MSB)							
64				WORKING KEY IDENTIFIER (for attribute number 8000h)				(LSB)
				⋮				
144	(MSB)							
150				WORKING KEY IDENTIFIER (for attribute number 800Fh)				(LSB)

The PAGE NUMBER field contains the attributes page number of the Partition Policy/Security attributes page.

The PAGE LENGTH field contains the number of additional bytes in the page format of the Partition Policy/Security attributes page.

The DEFAULT SECURITY METHOD field contains the value of the default security method attribute.

The OLDEST VALID NONCE field contains the value of the oldest valid nonce attribute.

The NEWEST VALID NONCE field contains the value of the newest valid nonce attribute.

The REQUEST NONCE LIST DEPTH field contains the value of the request nonce list depth attribute.

The FROZEN WORKING KEY BIT MASK field contains the value of the frozen working key bit mask attribute.

The POLICY ACCESS TAG field contains the value of the policy access tag attribute.

The USER OBJECT POLICY ACCESS TAG field contains the value of the user object policy access tag attribute.

The PKI_VALID (partition key identifier valid) bit shall be set to zero if the partition key identifier attribute length is zero. Otherwise, the PKI_VALID bit shall be set to one.

The WKI00_VLD (working key identifier 0h valid) bit shall be set to zero if the working key identifier attribute number 8000h has a length of zero. Otherwise, the WKI00_VLD bit shall be set to one.

The WKI01_VLD bit, WKI01_VLD bit, WKI02_VLD bit, WKI03_VLD bit, WKI04_VLD bit, WKI05_VLD bit, WKI06_VLD bit, WKI07_VLD bit, WKI08_VLD bit, WKI09_VLD bit, WKI0A_VLD bit, WKI0B_VLD bit, WKI0C_VLD bit, WKI0D_VLD bit, WKI0E_VLD bit, and WKI0F_VLD have the same bit value definitions as the WKI00_VLD bit, except that the definitions apply to the attributes with numbers 8001h to 800Fh, respectively.

The sixteen WORKING KEY IDENTIFIER fields contain the working key identifier attribute values in ascending attribute number order. If a working key identifier valid bit is set to one, the corresponding WORKING KEY IDENTIFIER field contains the value of the working key identifier attribute. Otherwise, the contents of the WORKING KEY IDENTIFIER field are undefined.

7.1.2.22 Collection Policy/Security attributes page

The Collection Policy/Security attributes page (C+5h) shall contain the attributes listed in table 38.

Table 38 — Collection Policy/Security attributes page contents

Attribute Number	Length (bytes)	Attribute	Application Client Settable	OSD Logical Unit Provided
0h	40	Page identification	No	Yes
1h to 4000 0000h		Reserved	No	
4000 0001h	4	Policy access tag	Yes	Yes
4000 0002h to FFFF FFFEh		Reserved	No	

The page identification attribute (number 0h) shall have the format described in 7.1.2.2 with the VENDOR IDENTIFICATION field containing the ASCII characters "INCITS" and the ATTRIBUTES PAGE IDENTIFICATION field containing the ASCII characters "T10 Collection Policy/Security".

The policy access tag attribute (number 4000 0001h) specifies the expected non-zero contents of the POLICY ACCESS TAG field in any capability (see 4.x.2.2) that allows access to this collection. The format, use, and attribute setting restrictions for the policy access tag attribute are described in 4.x.3. A CREATE COLLECTION command

(see 6.6) shall copy the user object policy access tag attribute from the Partition Policy/Security attributes page (see 7.1.2.21) to the policy access tag attribute in new Collection Policy/Security attributes page.

If a set attributes list contains an entry specifying the number of an attribute that table 38 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field specifies the number of an attribute that table 38 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The page format for the Collection Policy/Security attributes page is shown in table 39.

Table 39 — Collection Policy/Security attributes page format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				PAGE NUMBER (C+5h)				(LSB)
4	(MSB)							
7				PAGE LENGTH (4h)				(LSB)
8	(MSB)							
11				POLICY ACCESS TAG				(LSB)

The PAGE NUMBER field contains the attributes page number of the Collection Policy/Security attributes page.

The PAGE LENGTH field contains the number of additional bytes in the page format of the Collection Policy/Security attributes page.

The POLICY ACCESS TAG field contains the value of the policy access tag attribute.

7.1.2.23 User Object Policy/Security attributes page

The User Object **Policy/**Security attributes page (5h) shall contain the attributes listed in table 40.

Table 40 — User Object Policy/Security attributes page contents

Attribute Number	Length (bytes)	Attribute	Application Client Settable	OSD Logical Unit Provided
0h	40	Page identification	No	Yes
1h to 4000 0000h		Reserved	No	
4000 0001h	4	Policy access tag	Yes	Yes
4000 0002h to FFFF FFFEh		Reserved	No	

The page identification attribute (number 0h) shall have the format described in 7.1.2.2 with the VENDOR IDENTIFICATION field containing the ASCII characters "INCITS" and the ATTRIBUTES PAGE IDENTIFICATION field containing the ASCII characters "T10 User Object Policy/Security".

The policy access tag attribute (number 4000 0001h) specifies the expected non-zero contents of the POLICY ACCESS TAG field in any capability (see 4.x.2.2) that allows access to this user object . The format, use, and attribute setting restrictions for the policy access tag attribute are described in 4.x.3. A CREATE command (see 6.4) or CREATE AND WRITE command (see 6.5) shall copy the user object policy access tag attribute from the Partition Policy/Security attributes page (see 7.1.2.21) to the policy access tag attribute in new User Object Policy/Security attributes page.

If a set attributes list contains an entry specifying the number of an attribute that table 40 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field specifies the number of an attribute that table 40 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The page format for the User Object Policy/Security attributes page is shown in table 41.

Table 41 — User Object Policy/Security attributes page format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE NUMBER (5h)				
3								(LSB)
4	(MSB)			PAGE LENGTH (4h)				
7								(LSB)
8	(MSB)			POLICY ACCESS TAG				
11								(LSB)

The PAGE NUMBER field contains the attributes page number of the User Object Policy/Security attributes page.

The PAGE LENGTH field contains the number of additional bytes in the page format of the User Object Policy/Security attributes page.

The POLICY ACCESS TAG field contains the value of the policy access tag attribute.

7.1.2.24 Current Command attributes page

The Current Command attributes page (FFFF FFFEh) shall contain the attributes listed in table 42.

Table 42 — Current Command attributes page contents

Attribute Number	Length (bytes)	Attribute	Application Client Settable	OSD Logical Unit Provided
0h	40	Page identification	No	Yes
1h	20	Response integrity check value	No	Yes
2h	1	Object Type	No	Yes
3h	8	Partition_ID	No	Yes
4h	8	Collection_Object_ID or User_Object_ID	No	Yes
5h	8	Starting byte address of append	No	Yes
6h to FFFF FFFEh		Reserved	No	

The page identification attribute (number 0h) shall have the format described in 7.1.2.2 with the VENDOR IDENTIFICATION field containing the ASCII characters "INCITS" and the ATTRIBUTES PAGE IDENTIFICATION field containing the ASCII characters "T10 Current Command".

If the NOSEC security method or the CAPKEY security method (see 4.9.3) is used to process the command or if status returned for the command is CHECK CONDITION, the response integrity check value attribute (number 1h) shall contain zero. Otherwise, the response integrity check value attribute shall contain an integrity check value (see 4.9.7) that is computed as described in 4.9.3.4.

NOTE 3 If a command terminates with a CHECK CONDITION status, the response integrity check value is returned in the sense data (see 4.13).

The object type attribute (number 2h) shall identify the type of OSD object on which the current command is operating using the code values shown in table 4 (see 4.x.2.2).

The Partition_ID attribute (number 3h) shall contain the Partition_ID (see 4.6.4) of partition containing the OSD object on which the current command is operating.

If the object type attribute contains COLLECTION (see table 4 in 4.x.2.2), the Collection_Object_ID or User_Object_ID attribute (number 4h) shall contain the Collection_Object_ID (see 4.6.6) of the collection on which the current command is operating. Otherwise, the Collection_Object_ID or User_Object_ID attribute shall contain the User_Object_ID (see 4.6.5) of the user object on which the current command is operating.

If the current command is an APPEND (see 6.2), the starting byte address of append attribute (number 5h) shall contain the starting byte address used for the append command function. If the current command is not an APPEND, the starting byte address of append attribute shall contain zero.

If a set attributes list (see 5.2.1.3) contains an entry specifying the number of an attribute that table 42 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the CDB SET ATTRIBUTE NUMBER field (see 5.2.1.2) specifies the number of an attribute that table 42 states is not application client settable, the command shall be terminated with a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense code set to INVALID FIELD IN CDB.

The page format for the Current Command attributes page is shown in table 43.

Table 43 — Current Command attributes page format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				PAGE NUMBER (FFFF FFFEh)				(LSB)
4	(MSB)							
7				PAGE LENGTH (30h)				(LSB)
8	(MSB)							
27				RESPONSE INTEGRITY CHECK VALUE				(LSB)
28				OBJECT TYPE				
29								
31				Reserved				
32	(MSB)							
39				PARTITION_ID				(LSB)
40	(MSB)							
47				COLLECTION_OBJECT_ID OR USER_OBJECT_ID				(LSB)
48	(MSB)							
55				STARTING BYTE ADDRESS OF APPEND				(LSB)

The PAGE NUMBER field contains the attributes page number of the Current Command attributes page.

The PAGE LENGTH field contains the number of additional bytes in the page format of the Current Command attributes page.

The RESPONSE INTEGRITY CHECK VALUE field contains the value of the response integrity check value attribute.

The OBJECT TYPE field contains the value of the object type attribute.

The PARTITION_ID field contains the value of the Partition_ID attribute.

The COLLECTION_OBJECT_ID OR USER_OBJECT_ID field contains the value of the Collection_Object_ID or User_Object_ID attribute.

The STARTING BYTE ADDRESS OF APPEND field contains the value of the starting byte address of append attribute.

7.5 Vital product data parameters

7.5.1 Overview

This subclause defines the VPD pages used with OSD type devices.

See SPC-3 for VPD pages used with all device types.

The VPD page codes that are specific to OSD type devices are defined in table 44.

Table 44 — OSD specific VPD page codes

Page code	Description	Reference	Support Requirements
B0h	OSD Information	7.5.2	Optional
B1h	Security Token	7.5.3	Optional
B2h to BFh	Reserved for OSD type devices		

7.5.3 Security Token VPD page

The Security Token VPD page (see table 45) contains a security token for use in the CAPKEY security method (see 4.9.3.3).

Table 45 — Security Token VPD page

Bit / Byte	7	6	5	4	3	2	1	0
0	PERIPHERAL QUALIFIER			PERIPHERAL DEVICE TYPE				
1	PAGE CODE (B1h)							
2	PAGE LENGTH (n-3)							
3								
4	SECURITY TOKEN							
n								

The PERIPHERAL QUALIFIER field and the PERIPHERAL DEVICE TYPE field are defined in SPC-3.

The PAGE LENGTH field specifies the length of the following VPD page data. The page length shall be at least sixteen. If the allocation length is less than the length of the data to be returned, the page length shall not be adjusted to reflect the truncation.

The SECURITY TOKEN field contains a value that is unique to the I_T_L nexus that sent the INQUIRY command. The security token shall be random as defined by RFC 1750. An I_T nexus loss event, logical unit reset event, or reset event (see SAM-3) shall cause the security token to change.