

# ENDL TEXAS

Date: 18 August 2005  
 To: T10 Technical Committee & SNIA OSD TWG  
 From: Ralph O. Weber  
 Subject: REMOVE PARTITION Security Controlled by Root Attributes

Late in OSD development, it was discovered that REMOVE PARTITION usage was not covered by the Root Object security attributes. Because this was a technical change and making it would have delayed OSD publication, it was agreed to defer correcting the error until OSD-2. This proposal specifies the change needed to correct the problem.

Similar problems were noted regarding mention of REMOVE PARTITION, REMOVE COLLECTION and REMOVE in the table specifying where the Policy Access Tag is to be found when any these commands are processed. Changes in table 13 are also specified by this proposal.

All change reference osd2r00.pdf.

## Detailed changes proposed for OSD-2

### 4.9.2 Capabilities

#### 4.9.2.1 Introduction

...

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 4.10.6.1) 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 6.22) or SET MASTER KEY (see 6.23); or
- b) The default security method attribute in the Partition Policy/Security attributes page (see 7.1.2.21) specifies a default security method other than NOSEC for the partition identified as follows:
  - A) For the CREATE PARTITION command (see 6.6), FLUSH OSD command (see 6.9), FORMAT OSD command (see 6.11), or REMOVE PARTITION command (see 6.20), the identified partition is partition zero (see 3.1.32);
  - B) For any command not listed in item A), the partition is identified by the contents of the CDB PARTITION\_ID field.

...

**Table 13 — Policy access tag usage for OSD object types and commands**

<b>Command</b>	<b>Object Type</b> (see table 9)	<b>Attributes page containing policy access tag attribute to which CDB POLICY ACCESS TAG field is compared</b>
CREATE PARTITION or REMOVE PARTITION	PARTITION	Partition Policy/Security attributes page (see 7.1.2.21) for partition zero (see 3.1.32)
CREATE COLLECTION or REMOVE COLLECTION	COLLECTION	Partition Policy/Security attributes page
CREATE or CREATE AND WRITE or REMOVE	USER	Partition Policy/Security attributes page
All other commands	ROOT	Partition Policy/Security attributes page for partition zero
	PARTITION	Partition Policy/Security attributes page
	COLLECTION	Collection Policy/Security attributes page (see 7.1.2.22)
	USER	User Object Policy/Security attributes page (see 7.1.2.23)