

ENDL TEXAS

Date: 11 February 2004
 To: T10 Technical Committee & SNIA OSD TWG
 From: Ralph O. Weber
 Subject: OSD r09 Work List

This revision is the list from which OSD r09 is being built.

Problem, Issue, or Work To Do	Resolution
Are there any constraints on the interactions between concurrently processed commands? For example, does the setting of attributes by one command affect the retrieving of attributes by a concurrently processed command in any specific way?	No. Add a model subclause to specifically state that the only limitations on the interactions between concurrently processed commands are those specified by the Control mode page (see SPC-3).
Allow setting object logical length attribute to truncate the object.	In table 64, change "May Set" column to "Yes" for object logical length. Add the following to the definition of the object logical length attribute: "Setting the object logical length to a value that is smaller than the user object's logical length known to the OSD device shall cause the user object to be truncated to the specified length."
Can the requirements on quota enforcement be relaxed?	Incorporate T10/04-059.
Identify zero Object Creation Time credentials to simplify validation.	Zero creation time flag bit not needed because creation time is in Capability (see next item).
Move Object Creation Time from the Credential to the Capability.	Agreed to move in 12/17/03 conference call.
Single Unique Object ID	Deferred to OSD-2
Attribute Access	Access allowed ONLY to attributes associated directly with the object being accessed (e.g., no accessing partition attributes as part of user object READ).
Attribute directories should apply to the object with which they are associated and not be cumulative up the hierarchy (i.e., the Root Directory should contain only information root attributes pages).	Modify 4.6.3.5, 7.1.2.3, 7.1.2.4, 7.1.2.5, and possibly other clauses to reflect this change.
What happens when an attributes page does not contain an attribute number 0 to specify the attribute directory contents? N.B. the following statement in 7.1.2.2 and others like it are not acceptable: "...all attributes pages defined by this standard or any other document shall contain an identification of the page in attribute number 0h."	Rephrase the offending statement to place requirements only on this standard. Specify that the directory entries for attributes pages that do not have an attribute number 0 defined shall have a specific text content (e.g., "unidentified attributes page").

Problem, Issue, or Work To Do	Resolution
Persistence Model	Incorporate persistence_final.txt [T10/04-005r0] in various clauses with edits appropriate to T10 standards wording. Also modify the DPO bit definition.
Version Number	Incorporate the version number tag field in the Credential as described in Object Store Security Document rev 8. A marked copy of that document showing the concepts to be added is T10/03-279r2. Also define a version number tag attribute in the User Object Security attributes page. Put version number in capability 1OBJECT descriptor.
Format issue (aka OSD as delivered from the factory)	Incorporate Rev08-Formatv02.doc [T10/04-006r0] in various clauses with edits appropriate to T10 standards wording.
Current Command Attributes page	<p>Define one Current Command attributes page, page number FFFF FFFEh, with the following attributes:</p> <ul style="list-style-type: none"> • partition ID • object ID • object type • starting byte address of append • response integrity check value <p>Define attribute page range F000 0000h to FFFF FFFEh for attribute pages that are associated with all objects (i.e., accessible in conjunction with any access to any object).</p> <p>Require the response integrity check value to contain 0 for security levels 0 and 1.</p>
Is an object type user object attribute needed? Should its value be coordinated with the object type capability field?	This attribute is already included in the Current Command attributes page as proposed by Dave Nagle.
Combine LIST and LIST COLLECTION commands	Per 10/15/03 conference call, leave OSD r08 unchanged.
CREATE PARTITION should allow a requested partition ID.	Do this.
One CREATE XXX command per Credential	The 12/30/03 telephone conference call agreed to eliminate this requirement entirely in favor of using the object count attribute in the Partition Resources attributes page.

Problem, Issue, or Work To Do	Resolution
Task Management Functions	Prohibit support for task management functions when the security level is not zero. Add a PERFORM TASK MANAGEMENT command with a coded value for task management function, identification of mandatory and optional, and provision for a command tag. Add a permissions bit for the new command. Require all task management requests except ABORT TASK and QUERY TASK to be addressed to the root object, with an appropriate capability (i.e., a capability allowing access to the root object with the Device Management permission bit set). Require the ABORT and QUERY TASK task management requests be addressed to the same object as the command being aborted with an appropriate capability (i.e., the same capability as the command being aborted or a capability for the object with the Device Management permission set).
Persistent Reservations	Modify the model to prohibit OSD devices from supporting Persistent Reservations globally (per 12/17/03 conference call). Indicate this in table 29 too.
Finish the removal of support for EXTENDED COPY	Remove the following commands from table 29 CHANGE ALIASES, RECEIVE COPY RESULTS, and REPORT ALIASES
Commands needing security protection	Modify table 29 to indicate that the following commands are prohibited with the security level is not zero: LOG SELECT, LOG SENSE, MODE SELECT(10), MODE SENSE(10), PREVENT ALLOW MEDIUM REMOVAL, READ BUFFER, RECEIVE DIAGNOSTIC RESULTS, SEND DIAGNOSTIC, START STOP UNIT, and WRITE BUFFER. In table 29 make SEND DIAGNOSTIC support optional. Add a PERFORM SCSI COMMAND command that provides for delivery of the CDBs and parameter data for the above commands in concert with a Capability. Add a permissions bit for the new command (i.e., Device Management). Require all of the new command to be addressed to the root object. Prohibit the use of the new command for delivery of any CDBs other than those listed.
REQUEST SENSE and TEST UNIT READY -- Owing to existing operating system implementations, these two commands cannot be prohibited when the security level is not zero. However, they have the ability to return/clear pending Unit Attention information that might be valuable to host software. Thus they might be viewed as security threats.	Since OSD currently has no special reliance on Unit Attention conditions, resolution for any issues in this area is being left to OSD-2.

Problem, Issue, or Work To Do	Resolution
INQUIRY and REPORT LUNS -- Operating system device configuration software requires that these two commands be supported regardless of OSD security level. These commands do not clear pending Unit Attention conditions and so do not represent a known security threat.	No changes required. No SNIA OSD TWG action required, unless there are concerns about allowing these two commands regardless of OSD security level.
Does FORMAT OSD return a progress indication in sense data in the same way that the FORMAT commands for other device types do? Note: the answer affects one's view of REQUEST SENSE which is the way such information is usually retrieved.	Reporting progress on long running commands has been deferred to OSD-2.
Do Permissions Bits identify commands or functions? Different people reading OSD r08 get opposite views from the same text. So, some clarification is needed. The nature of the clarification depends on which view is adopted as the standard.	The last revision of T10ized_Permission_Bits_v7.pdf, as agreed by discussions on the SNIA OSD TWG reflector, will be included in OSD r09.
Clarify which secret key is used to compute a credential integrity check value.	KeysCorrections-r2.pdf, as agreed by discussions on the SNIA OSD TWG reflector, will be included in OSD r09.
Should the REPORT TARGET PORT GROUPS and SET TARGET PORT GROUPS commands be supported? This would allow Active/Standby OSD controller (aka asymmetric logical unit) implementations ala RAID controllers.	Add REPORT TARGET PORT GROUPS and SET TARGET PORT GROUPS as optional commands and cover them with the PERFORM SCSI COMMAND described above.
Man-in-the-middle DOS attacks	As just a command level standard, OSD is not designed to address all known security threats. Some threats are appropriately addressed by the SCSI transport protocol (e.g., data encryption) and thus are not covered by OSD. The DOS attacks raised as issues fall in to this category. No changes will be made.
Attribute size hint (i.e., add an attribute that specifies the bytes of overhead associated with each attribute so that host software can calculate OSD space usage)	Host software should be relying on the OSD attributes and quotas to manage space usage. Attempting to mirror the calculations in host software is redundant and extremely error prone. No changes will be made.
C.2 (General bibliography) is out of date	Subclause C.2 will be removed in OSD r09.
An OSD-specific sense data descriptor is required and should include the following: <ul style="list-style-type: none"> • partition ID • user object ID • object byte offset where error detected • number of bytes actually transferred • integrity check value 	Ralph to write a T10 proposal for inclusion SPC-3.
Incorporate Error Handling model subclause requested during November T10 editing meeting.	Incorporate T10/04-044r0.

Problem, Issue, or Work To Do	Resolution
Invalid CapKey effects on CHECK CONDITION responses.	Replace the following 4.6.4.2.4 text: "If the validation fails, the application client should cease communications with the device server." with "If the application client fails in validating the integrity check value as described in this section, it should take a recovery action not specified by this standard. 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 executing a denial of service attack should be considered."
OSD System ID should have a format that matches that defined for the Device Identification VPD page, to provide compatibility with all SCSI transport protocols, especially iSCSI.	Define the OSD System ID attribute by reference to the identification descriptor in the Device Identification VPD page (see SPC-3). Restrict the code set, protocol identifier, identifier type, association, and identifier length values to fit previously agreed OSD System ID constraints.
Define the ordering relationships between command actions, getting attributes, and setting attributes in 4.6.3.2.	The 12/30/03 telephone conference call agreed to swap items 2 and 3 in the first list in 4.6.3.2.
Does more need to be said about dynamically creating attributes pages?	Sami to post specific propose changes to the reflector for discussion, agreement, and eventual inclusion in OSD r09.
The Capability Nonce Audit and Nonce Random Number fields are agreed to be "optional". What values do they contain when they are optionally meaningless?	The 12/30/03 telephone conference call agreed to rename the capability NONCE AUDIT to just AUDIT, to rename capability NONCE RANDOM NUMBER field to the CAPABILTIY DISCRIMINATOR field to be defined as "The CAPABILTIY DISCRIMINATOR field contains a nonce that differentiates one capability and credential from another", and to remove all discussion of a capability nonce since that implies to some readers a device server requirement to verify the uniqueness of all values received.
In the third paragraph after the a,b,c list on page 34, is it acceptable to add "Of particular concern is any change that causes the clock to be set backwards."? Why is this concern special? Are there other 'particular concerns' that need to be mentioned? Since someone is likely to ask these questions in the T10 Letter Ballot review, it would be best to address them now and explain them completely in OSD r09.	The 12/30/03 telephone conference call agreed to change the parenthetical expression in the last sentence of the cited paragraph from "(i.e., it should not be possible for an adversary to change the time of either the device server or security manager and thus thwart the checking of capability expiration checking)" to "(e.g., it should not be possible for an adversary to set the clock in the device server backwards to enable the replay of expired credentials)".

Problem, Issue, or Work To Do	Resolution
Should the nonce in a Credential that has previously been found to be invalid be tracked to reject future uses of that nonce?	From Seagate technical comment 6. Note that IBM specific comment 19 indicates that the last sentence in the 4th paragraph of 4.6.4.4.4 [Credential and capability validation] will be affected if there are no cases where previously received nonces are rejected. The text stays as is, such messages can be rejected at a layer below the command layer (if desired), and security group to review simple denial of service attacks such as this one and propose a resolution, which may be a white paper (i.e., no changes to the standard).
What minimum level of FIPS 140-2 should be specified for coprocessors mentioned in the last paragraph of 4.6.4.7.1?	The 12/30/03 telephone conference call agreed to delete the one paragraph that references FIPS 140 and the normative reference.
Should the unused (or pad) bytes between segments in the Data-In Buffer and Data-Out Buffer be included in the integrity check value computations required by security level 3?	No. Clarify this.
Should the priority fields be removed from all the CDBs in which they appear?	The 12/30/03 telephone conference call agreed to remove these.
What attributes are returned when a CREATE command creates more than one user object? How are these attributes associated with a given user object?	The 12/30/03 telephone conference call agreed to define the following behaviors: set attributes applies to all objects, get attributes applies to all objects, get page format not allowed. Also r09 must restore get attributes list format with object identification information so that the get attributes can identify the objects for which attributes are returned.
Should a new attribute be added that prohibits requesting specific User_Object_IDs in CREATE and CREATE AND WRITE commands? Should a new attribute be added that prohibits requesting specific Partition_IDs in CREATE PARTITION?	The authors of this comment agreed to withdraw it out of respect for past agreements to allow partitions that concurrently use both OSD assigned and user requested User_Object_IDs.
Should the GET ATTRIBUTES and SET ATTRIBUTES commands be replaced by a single NOP command?	The 12/30/03 telephone conference call agreed to modify 4.6.3.2 to specify that GET ATTRIBUTES does gets first whereas SET ATTRIBUTES does the set first. Thus GET ATTRIBUTES and SET ATTRIBUTES are different and both need to exist.
Clarify what the FLUSH OBJECT command flushes.	Add a new field to the FLUSH OBJECT specifying what the FLUSH OBJECT command flushes, with 00b meaning all data and attributes of a single object are flushed, 01b meaning that only the attributes of the object are flushed; and 10b meaning that all data and attributes in the object and all contained objects are flushed.

Problem, Issue, or Work To Do	Resolution
Should the Root bit be removed from the parameter data returned by the LIST command?	The 12/30/03 telephone conference call agreed to keep the Root bit while applying the IBM editorial changes that remove discussion of identifier lengths.
Should the LIST COLLECTION command have all the restart complexity currently specified for the LIST command?	The 12/30/03 telephone conference call answered this question with an emphatic YES.
Should OSDs be limiting the number of objects and collections created to the number that can be represented in a single LIST or LIST COLLECTION command?	The 12/30/03 telephone conference call agreed to delete statements in LIST and LIST COLLECTION that require a CHECK CONDITION to be returned when the total list length exceeds a 64-bit value. The statements to be deleted are from T10 boilerplate definitions of the allocation length field and are rendered incorrect by the next change (also agreed).
Should an Additional Length of FFFF FFFF FFFF FFFFh indicate "too big to fit in this field" in the parameter data returned by the LIST and LIST COLLECTION commands?	The 12/30/03 telephone conference call agreed to add these statements.
A READ command that crosses the logical end of an object should return all the bytes that are present in the object and then return a CHECK CONDITION status with sense data that indicates how many bytes are returned.	Do this!
What is the SET KEY command Key Identifier field? Should attributes be added to return the Key Identifier values?	Incorporate Key Identifier description information (including new attributes definitions) posted on the SNIA OSD TWG reflector.
Should CHECK CONDITION status be returned for SET KEY and SET MASTER KEY commands when the Seed lsb is one?	The 12/30/03 telephone conference call agreed to add these requirements.
Does the SET MASTER KEY command invalidate the drive, partition, and working keys?	The 12/30/03 telephone conference call agreed to add this requirement.
What creation time is used to construct the Credential for a SET MASTER KEY command?	The 12/30/03 telephone conference call agreed that zero or the creation time of the root object shall be used to construct the Credential for a SET MASTER KEY command.
Is the mechanism for maintaining the root clock attribute's value beyond the scope of the standard?	The 12/30/03 telephone conference call agreed to add this statement.
Because the clock value has a significant impact on Credential formation, setting it should require the Security permission to be set.	The 12/30/03 telephone conference call agreed to address this making the clock attribute in the root information attributes page not user settable and by adding a copy of the clock attribute in the root security attributes page.

Problem, Issue, or Work To Do	Resolution
Should there be a lower limit on the value that may be set in the minimum security level attribute in the partition security attributes page? If there should be a lower limit, how should that limit be specified (e.g., as a new attribute in the root security attributes page)?	Provide a security level (method) attribute in each root and partition security attributes pages specifying the exact (not minimum) security level applied to the partition (partition 0 is the root partition). Provide a default security level in the root security attributes page that is inherited by newly created partitions. Provide a separate security level attribute in the root object for SET KEY and SET MASTER KEY commands. Make several other changes in this regard as proposed by Michael Factor on the SNIA OSD TWG reflector.
Is it desired to add a Security Level field to the Capability (or CDB) indicating the level to which the CDB was prepared?	No. Define security level attributes as described above instead.
Are the root minimum security level and partition minimum security level attributes 0 after a FORMAT OSD command?	No. Clarify this.
Is there a desire to add an OSD-specific VPD page in r09? What information (in addition to root minimum security level) should be included in the page? What would be a good length for the page to provide enough reserved space for future uses?	Yes. Call it the OSD Information VPD page (page code B0h). Make the page large enough to accommodate potential future additions. Include the partition 0 security level as well as the SET KEY and SET MASTER KEY security level.
Should all discussion of minimum security levels be removed?	Yes, and it should be replaced with the discussion of exact security levels described above.
Security levels are not a hierarchy.	Change 'security level' to 'security method'. Eliminate all discussion of 'higher' security method.
Should the security version tag attribute be placed in the user object information attributes page or in a (to be created) user object security attributes page?	The 12/30/03 telephone conference call agreed to place the attribute in the user object security attributes page.
Use of the NONE object descriptor in capabilities should be minimized to simplify invalidating credentials.	Add a GLOBAL permissions bit that is combined with the DEV_MGMT permissions bit in a capability that allows PERFORM XXX commands that may affect more than one object or task. Then require such capabilities to be associated with the root (i.e., 1OBJECT object descriptor with the single object_id field set to zero. Once these changes are applied, the NONE object descriptor is used only for create commands that create multiple user objects.
Do not compute a response integrity check value (and return 0) if the computed integrity check value for the CDB may be incorrect.	Incorporate the changes posted to the SNIA OSD TWG reflector to reduce the cases where a known incorrect response integrity check value is returned.
Should the partition count and object count attribute names be changed to partition count quota and object count quota?	Change names as described in T10/04-059.

Problem, Issue, or Work To Do	Resolution
Should a new attribute called length of the write or append be added?	Do not do this.
Why do we need the starting byte address of the last write or append in the current command attributes page? How will this be used?	Move the starting byte address of the last write or append attribute to the Current Command attributes page (the one described by Dave Nagle) and rename it to starting byte address for append (thus limiting its applicability to the APPEND command which is the historical reason for the attribute's existence).
Are attributes accessed and attributes modified timestamps updated when actions other than when CDB fields explicitly specify the getting or setting of attributes?	Clarify that 'side-effect updates' (e.g., WRITE updating logical length) do not cause applicable timestamp attribute to be updated.
Should a new attribute be added to disable the updating of timestamp values? In what attributes pages should the new attribute be added?	Add a one byte attribute disabling timestamp updates in the information attributes page using the definitions and other requirements posted on the SNIA OSD TWG reflector.
Should the partition information attributes page contain a count of the number total number of user objects (to coordinate with the quota on the number of user objects in the partition found in the partition resources attributes page)?	Add number of partitions attribute to Root Information attributes page and number of user objects attribute to Partition Information page. See T10/04-059.
Should CREATE PARTITION set the object count attribute in the partition resources attributes from a default value in the root object resources attributes page, or (as currently defined) set the value to all one's?	Add partition object count quota attribute to Root Resources attributes page. Specify that the root partition object count quota attribute is copied to the partition object count quota attribute by a CREATE PARTITION command. See T10/04-059.
Should fill-in bytes in sparse WRITES be set to zero?	Add the following in the definition of the READ command: "Attempts to read bytes that have never been written shall result in zeros being returned." Note this is not a requirement that WRITES store zeros, only a requirement on the behavior of subsequent READs in such cases. How the sparse object is represented in vendor specific.
How does one support a truly read-only OSD?	This issue appears to be related to timestamp updates. The 1/5/04 telephone conference agreed to defer further consideration of this issue to OSD-2.
Apply numerous editorial changes received since r08 published and editorial changes from the 11/7 T10 Editing Meeting	No SNIA OSD TWG action required.