MMC Command Descriptions for the Optical Security Subsystem Class

Draft Revision 0.8

22 February 2008

PERMISSIONS

The *MMC Command Descriptions for the Optical Security Subsystem Class* is published by DPHI, Inc.(Longmont, CO USA) and has been prepared in close co-operation with the Storage Working Group within the Trusted Computing Group. All rights are reserved. Reproduction in whole or in part is prohibited without express and prior written permission of DPHI, Inc.

DISCLAIMER

The information contained herein is believed to be accurate as of the date of publication, however, neither DPHI, Inc. nor the Trusted Computing Group will be liable for any damages, including indirect or consequential, from use of the *MMC Command Descriptions for the Optical Security Subsystem Class* or reliance on the accuracy of this document.

LICENSING

Application of the *MMC Command Descriptions for the Optical Security Subsystem Class* in host environments requires no license from either DPHI, Inc. or the OSSC.

CLASSIFICATION

The information contained in this document is being made available for the purpose of standardization. Permission is granted to members of INCITS, its technical committees and their associated task groups to reproduce this document for the purposes of INCITS standardization activities provided this notice is included.

NOTICE

For any further explanation of the contents of this document, or in case of any perceived inconsistency or ambiguity of interpretation, or for any information regarding the *MMC Command Descriptions for the Optical Security Subsystem Class*, please consult:

W. McFerrin

DPHI, Inc.

1900 Pike Road, Suite F

Longmont, CO 80501

email: bmcferrin@dataplay.com

Contents

Tables

Figures

This page is blank

1   INTRODUCTION

1.1   The Optical Security Subsystem Class

The Trusted Computing Group (TCG) is a not-for-profit industry-standards organization with the aim of enhancing the security of the computing environment in disparate computer platforms. TCG was formed in Spring 2003 and has adopted the specifications developed by the Trusted Computing Platform Alliance (TCPA). The distinguishing feature of TCG technology is the incorporation of "roots of trust" into computer platforms.

The TCG Storage Work Group (SWG) exists to build upon existing TCG technologies and philosophy, and focus on standards for security services on dedicated storage systems. Security Subsystem Classes define only TCG SWG related functionality. Other attributes such as host interface type, storage capacity, data rates, and seek times are not key Security Subsystem Class attributes, however the storage device resources such as available memory, storage capacity, and processing power influence the Security Subsystem Class definition.

The Optical Security Subsystem Class Sub-working Group was established by the TCG SWG to address the unique issues for security on optical storage drives and discs. The Optical Security Subsystem Class Specification [OSSC] defines the Optical Security Subsystem Class (OSSC). The [OSSC] describes a security implementation that is customized toward the unique characteristics of DVD, HD DVD, and BD devices:

1. Removable media,

2. Many variations of physical format, and

3. Limited Device Resources.

1.2   Scope

The *MMC Command Descriptions for the Optical Security Subsystem Class* is divided into several clauses according to the structure of the MMC-5 standard:

Clause 1 (this clause) is the introduction and scope.

Clause 2 contains lists of documents that may be needed by the reader for the correct understanding of this document.

Clause 3 contains Definitions, Symbols, Abbreviations, and Conventions. This is a glossary of terminology used in this document that may be absent from the MMC-5 standard.

Clause 4 describes modeling for the specific behaviors associated with the OSSC requirements. This provides an overview of internal drive operation.

Clause 5 specifies the changes to the lists of features and profiles for the support of OSSC capabilities.

Clause 6 specifies new commands and the changes to existing commands for the support of OSSC capabilities.

Clause 7 specifies new mode pages and the changes to existing mode pages for the support of OSSC capabilities.

2   REFERENCES

2.1   Normative References

The following standards contain provisions that, by reference in the text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

2.2   Approved References

Copies of the following documents may be obtained from ANSI: approved ANSI standards, approved and draft international and regional standards (ISO, IEC, CEN/CENELEC, ITUT), and approved and draft foreign standards (including BSI, JIS, and DIN). For further information, contact ANSI Customer Service Department at 212-642-4900 (phone), 212-302-1286 (fax) or via the World Wide Web at http://www.ansi.org.

ANSI NCITS 408-2005	SPC-3	SCSI Primary Commands – 3
ANSI INCITS 430-2007	MMC-5	SCSI Multi-Media Command Set – 5
ANSI INCITS 397-2005	ATA-7	AT Attachment with Packet Interface – 7
		Volume 1: ATA Command Set, Volume 2: Parallel ATA, Volume 3: Serial ATA
FIPS 197	AES	Advanced Encryption Standard, Federal Information Processing Standards Publication 197.
ISO/IEC 646:1991	ASCII	Information technology - ISO 7-bit coded character set for information interchange (third edition).
		See also: *ANSI INCITS 4-1986 (R2002) Information Systems - Coded Character Sets - 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)*
IEC 908:1987		Compact Disc Digital Audio System.
ISO/IEC 3901:2001	ISRC	International Standard Recording Code
ISO/IEC 10149:1995	CD-ROM	Information Technology-Data Interchange on Read-only 120 mm Optical Data Discs (CD-ROM).
ECMA 267	DVD-ROM	Information technology -- 120 mm DVD -- Read-only disk
ECMA 330	DVD-RAM	120 mm (4,7 Gbytes per side) and 80 mm (1,46 Gbytes per side) DVD Rewritable Disk (DVD-RAM)
ECMA 337	DVD+RW	120 mm 4,7Gbytes and 80 mm 1,46 GB DVD ReWritable Disk (DVD+RW)
ECMA 338	DVD-RW	80 mm (1,46 Gbytes per side) and 120 mm (4,70 Gbytes per side) DVD Re-recordable Disk (DVD-RW)
ECMA-349	DVD+R	Data Interchange on 120 mm and 80 mm Optical Disk using +R Format, 3rd Edition, Dec 2005
ECMA-359	DVD-R	80 mm (1,46 Gbytes per side) and 120 mm (4,70 Gbytes per side) DVD Recordable Disk (DVD-R), 1st Edition, Dec 2004
NIST SP 800-38A	NIST	National Institute of Standards and Technology (NIST), Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38A, Dec 2001

2.3 References Under Development

At the time of publication, the following referenced standards were still under development. For information on the current status of the document, or regarding availability, contact the relevant standards body or other organization as indicated.

INCITS T10/1731D	SPC-4	SCSI Primary Command Set – 4
INCITS T13/1697D	ATA8-AST	AT Attachment – 8 Serial Transport (ATA8-AST)
INCITS T13/1698D	ATA8-APT	AT Attachment – 8 Parallel Transport (ATA8-APT)
INCITS T13/1699D	ATA8-ACS	AT Attachment – 8 ATA Command Set (ATA8-ACS)
INCITS T13/1700D	ATA8-AAM	AT Attachment – 8 Architecture Model (ATA8-AAM)

2.4 Other References

OSSC   Optical Security Subsystem Class Specification, Draft Version 1, Revision 0.8, 2008-02-21

3 DEFINITIONS, SYMBOLS, ABBREVIATIONS, and CONVENTIONS

3.1 Definitions

3.1.1 Authority

This is a security association between an authentication Operation and a Credential, such as a public-private key pair.

3.1.2 Full Disk Encryption (FDE)

Data written is encrypted before it is written and decrypted as it is read. Full Disk Encryption means that all user data through the main read-write functions shall be encrypted.

3.1.3 Host Application

A Trusted Component (software) that initiates ATA (T13) TRUSTED SEND/RECEIVE commands or SCSI (T10) SECURITY PROTOCOL IN/OUT commands.

3.1.4 N-factor Authentication

An Authentication factor is the minimal amount of information from a single source required for authorizing access. N-factor Authentication requires factors from multiple sources for the purpose of authorizing access. N is the explicit number of factors required.

3.1.5 Physical Volume

If an optical disc has a specific Profile associated with it, the Physical Volume is the sequence of sectors specified by the LBA space defined by that Profile.

3.1.6 Protected Storage Area (PSA)

On a disc that has been formatted for use as an OSSC format disc, the Protected Storage Area is an area in the user data area of the disc that is not in the LBA space of the Secure Volume reserved for storage of security information.

3.1.7 Public Key Encryption

In a public key encryption scheme, a public (not secret) key is used to encrypt data, while a private (secret) key is needed for decryption.

3.1.8 Security Subsystem Class (SSC)

For TCG Compliance and Conformance purposes the TCG-SWG defined functional core (TBD) specifies a Security Subsystem Class (SSC). An SSC identifies the core components that are Mandatory, Optional, Excluded, or Forbidden for a particular peripheral or subsystem.

3.1.9 Secure Volume

On a disc that has been formatted for use as an OSSC format disc, the every user data write to the Secure Volume is encrypted and each read from the Secure Volume is decrypted.

3.1.10 Security Provider

A security provider (SP) is an atomic collection of Tables and Methods that can be issued on behalf of a host software provider.

3.1.11 Symmetric Key (SymK)

Convenient notation for symmetric key (shared secret) cryptography.

3.1.12 Table

The basic data structures within an SP. Tables store persistent SP state defined in this specification.

3.1.13 TPer

A Trusted Peripheral. Referred to in this document as the Drive.

3.1.14   Trusted Session

A trusted session begins upon mutual authentication of the Host and Drive. A Trusted Session is prerequisite to seeking authorization for disc access.

3.1.15   Unique Identifier (UID)

Unique 8-byte identifier that identifies tables, table rows, and the SP itself.

3.1.16   VolumeZero

In the OSSC format, an 8 MB area is reserved beginning at the Physical Volume's LBA 0. This area is recorded in clear-text and is independent of the Secure Volume.

3.2   Abbreviations

AES	Advanced Encryption System
FDE	Full Disc Encryption
OSSC	Optical Security Subsystem Class
OSPB	Optical SP Basis
SP	Security Provider
SSC	Security Subsystem Class
TPer	Trusted Peripheral
UID	Unique Identifier
VZ	VolumeZero

4 MODELS

4.1 Introduction

The Optical Security Subsystem Class Reference [OSSC] is a framework for implementing Full Disk Encryption (FDE) for optical drives and discs. The primary capabilities specified by [OSSC] are:

o Authentication - Verification of identity

o Authorization - Verification of permissions for an authenticated entity

o Privacy/Confidentiality - Making secret that which is intended to be secret, and maintaining secret that which is intended to be secret

Security is defined for use with two groups of media:

o Write-once and rewritable disc types with profiles that support the track/session model: DVD-R, DVD-RW, DVD+R, HD DVD-R, HD DVD-RW, and BD-R.

o Rewritable disc types with profiles that support a random writable model: DVD-RAM, DVD+RW, HD DVD-RAM, and BD-RE.

According to [OSSC], users secure data with one or more pass-codes. A disc that is recorded according to [OSSC] may be shipped by non-secure carrier or even become lost, and the user may be confident that the data will not be exposed to unauthorized parties.

4.1.1 Optical Security Subsystem Class (OSSC)

OSSC security is managed by a set of tables and functions that operate on those tables. For a disc that has already been initialized by the OSSC, there are three types of tables:

    o Tables stored on the disc in clear text,

    o Tables stored on the disc encrypted,

    o Volatile tables that are created for OSSC session management.

When a blank disc is loaded, the Host is responsible for determining the usage. The Host may choose to initialize the disc as an OSSC disc, or the Host may choose to use the disc in a different way. It is possible to configure the Drive to allow only secure recording according to [OSSC].

OSSC Security operations permit the Host to use the OSSC tables for the intended security purposes. The Host requests specific OSSC Security operations by using Security Protocol = 01h and Security Protocol Specific = 7007h in both the SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands.

4.1.2 Cipher Schemes

[OSSC] specifies RSA public key encryption for initiating secure communications between Host and Drive. The Drive (TPer) may optionally use elliptic curve public key encryption.

[OSSC] specifies the Advanced Encryption Standard (AES) for securing user data. AES-128 is mandatory. AES-256 is optional.

4.2 Components

4.2.1 Disc Areas

4.2.1.1 Physical Volume

According to the profile for the medium, there is a PSN = D that is associated with LBA = 0. The Physical Volume is the sequence of sectors that begins at D and proceeds until the maximum capacity of the user data area. See Figure 1.
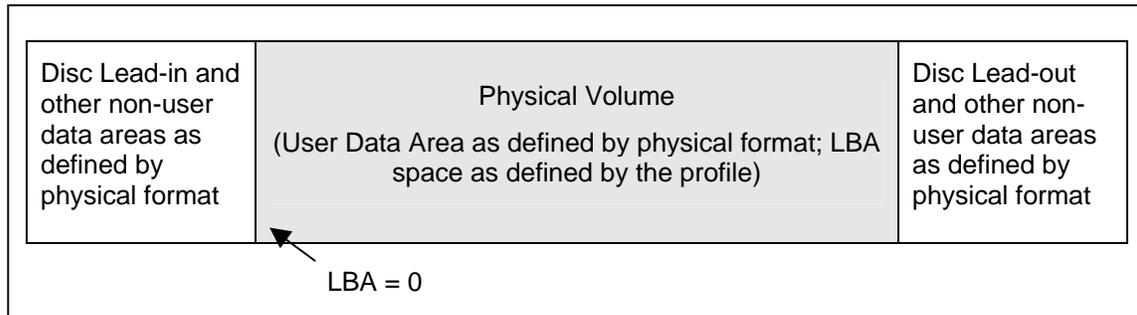
Figure 1 — Physical Volume

4.2.1.2 VolumeZero

In the OSSC Format, VolumeZero (Figure 2) begins at PSN = D and has a length of approximately 4 096 sectors (8 MB). VolumeZero is made available to the Host as a small, clear-text volume. One use for VolumeZero is to contain a read-only file system that may aid the Host in dealing with backward compatibility issues.
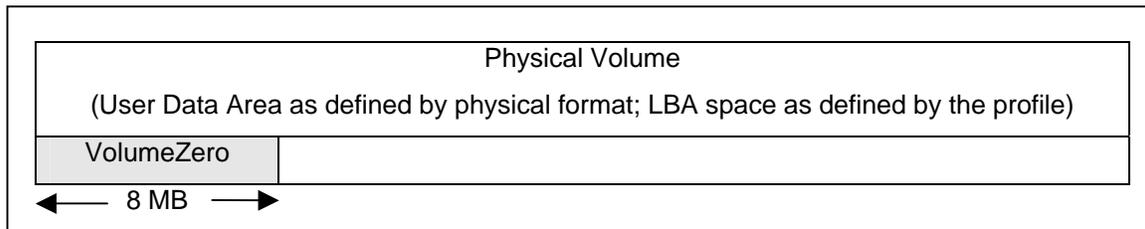
Figure 2 — VolumeZero

4.2.1.3 Protected Storage Area (PSA)

The [OSSC] requires a Protected Storage Area (PSA) – storage that is persistent, not included in the LBA space of the encrypted area, and not affected by Host partitioning. The PSA is defined in the disc's user data area in order to provide common security mechanisms over a wide range of optical media.

A PSA follows VolumeZero, however, the exact starting location and size are determined by the physical format of the media. When the media profile permits only sequential recording, additional areas may be taken for updating the PSA content.
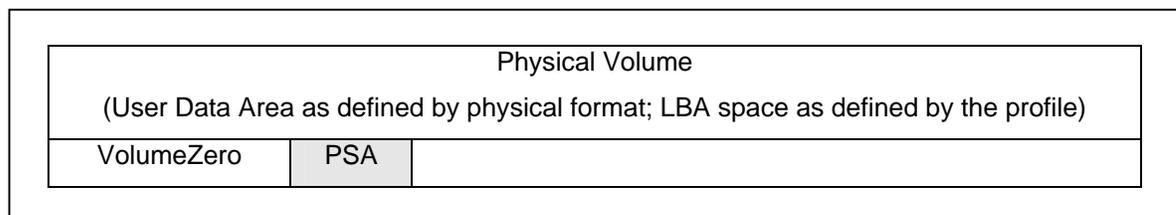
Figure 3 — General Location of the PSA

4.2.1.4   Secure Volume

The Secure Volume follows the PSA, however, the exact starting location and size are determined by the physical format of the media. When used according to the [OSSC], all user data sectors in the Secure Volume are encrypted.

Physical Volume		
(User Data Area as defined by physical format; LBA space as defined by the profile)		
VolumeZero	PSA	Secure Volume
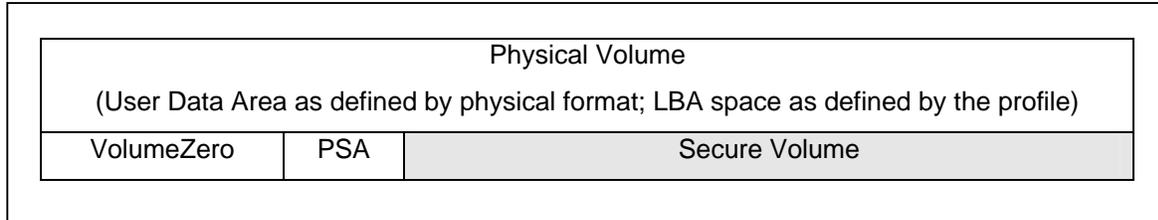
Figure 4 — General Location of the Secure Volume

4.2.2   OSSC Tables

The Optical Security Provider (OSP) is a set of tables described in [OSSC]. Some of these tables are written to the disc while others are constructed from Drive and general disc information. The part of the OSP that is written into the PSA is the OSP Basis (OSPB). Certain content in the OSPB is encrypted. [OSSC] contains the detailed specifications for each table. An overview is presented in Table 1.

Table 1 — OSSC Tables in the OSPB

Table	Description
Anchor	Anchor enables interchange and indexes all tables that are on-disc.
Disc	Disc is a descriptor that includes properties that apply to the entire disc.
C_User	Each row in C_User represents a single user. Each user is associated with an identifier (Name), a Passcode and, optionally, multiple authentication factors. A row in C_User is known as a user record.
SessionMap	The TPer uses this table to manage PSA updates on disc formats that require a track/session recording methodology.

There are 2 user types:

1. Initializer

   An Initializer user has change access over the OSPB. Consequently, the Initializer may enroll Common users. The Initializer may modify or delete any user record. The Initializer is not permitted to provide access to the Secure Volume.

2. Common

   A Common user is not permitted to modify any other user's record. A Common user may provide LBA access only to the Secure Volume.

4.2.3   OSP Methods

OSP methods are security functions in the Drive that may be requested by the Host. A method execution is requested via the SECURITY PROTOCOL OUT command with Security Protocol Code set to 01h and Security Protocol Specific Code set to 7007h (or 7008h to receive authentication factors from external hosts). Results of the method execution are requested via the SECURITY PROTOCOL IN command with Security Protocol Code set to 01h and Security Protocol Specific Code set to 7007h. The methods used in implementing the OSSC are described in [OSSC].

The methods may be divided into two classes:

- o Many of the methods are associated only with the security features of the OSSC and have no storage device/media dependencies. Sequences are described in [OSSC] for general, higher level results. See Table 2.

- o Some methods have been included for the specific management of on disc structures defined by the OSSC. See Table 3.

Table 2 — Storage Device/Media Independent Method Sequences

Method Sequence	Purpose
TS	Establish a Trusted Session (secure communications between Host and Drive)
CU	Connect (authenticate) a user
EU	Enroll a user (create a new C_User record)
DU	Erase (delete) a user (remove a C_User record)
MU	Modify a user (Change information in a C_User record)

Table 3 — Methods Specific to OSSC Devices

OSSC Specific Methods	Purpose
PSAbegin	Announce to Drive that the OSPB may change
PSAend	Announce to the Drive that changes to the OSPB are complete
MountSV	If SV is not mounted, dismount current volume and MountSV.
VolumeZeroBegin	It is permitted to record VolumeZero.
VolumeZeroEnd	Recording of VolumeZero is complete.

The command sequence for recording VolumeZero (RVZ) is shown in Table 4.

Table 4 — Sequence for Recording VolumeZero RVZ

Command/Method	Purpose
VolumeZeroBegin	Initiate VolumeZero recording
WRITE (10), ..., WRITE (10)	Record VolumeZero
SET VolumeZero signature	SET method stores Host provided signature in Disc table (optional)
VolumeZeroEnd	VolumeZero recording is completed; In the Track/Session model, the VolumeZero Logical Track is closed and the VolumeZero session is closed

4.3 OSSC Disc Formats

4.3.1 Introduction

Given a disc type with a supported OSSC format:

1. A common profile is selected for that disc type.

2. A small, contiguous area beginning with LBA 0 is allocated for a small, fixed length clear-text volume: VolumeZero. VolumeZero is followed by the initial PSA. The amount of the user data zone allocated for the PSA includes the disc type specific space allocated for the PSA plus any overheads associated with the method selected for the allocation.

3. The remainder of the disc is specified as the Secure Volume and is represented to the Host as a disc capable of the selected profile. LBA 0 is realigned to the first usable user data sector following the PSA allocation.

Two groups of OSSC formats are defined for:

1. Disc types and profiles that support a random writable model:

    DVD-RAM   DVD-RAM Profile (0012h),

    DVD+RW   DVD+RW Profile (001Ah),

    DVD+RW DL   DVD+RW DL Profile (002Ah),

    HD DVD-RAM HD DVD-RAM Profile (0052h), and

    BD-RE   BD-RE Profile (0043h).

2. Disc types and profiles that support a track/session model:

    DVD-R   DVD-R Sequential Recording Profile (0011h),

    DVD-RW SL   DVD-RW Sequential Recording Profile (0014h),

    DVD+R   DVD+R Profile (001Bh),

    DVD+R DL   DVD+R DL Profile (002Bh),

    HD DVD-R   HD DVD-R Profile (0051h), and

    BD-R   BD-R Sequential Recording Profile (0041h).

4.3.2   OSSC Formats for the random writable model

4.3.2.1   Overview

This format may be applied to:

- o   DVD-RAM   DVD-RAM Profile (0012h),
- o   DVD+RW   DVD+RW Profile (001Ah),
- o   DVD+RW DL   DVD+RW DL Profile (002Ah),
- o   HD DVD-RAM   HD DVD-RAM Profile (0052h), and
- o   BD-RE   BD-RE Profile (0043h).

Prior to being converted to the OSSC Format, the media shall be formatted according to the methods used for the specific media and applicable profile.

The OSSC Disc Format divides the physical volume into 3 distinct areas: VolumeZero, the PSA, and the Secure Volume. See Figure 5.
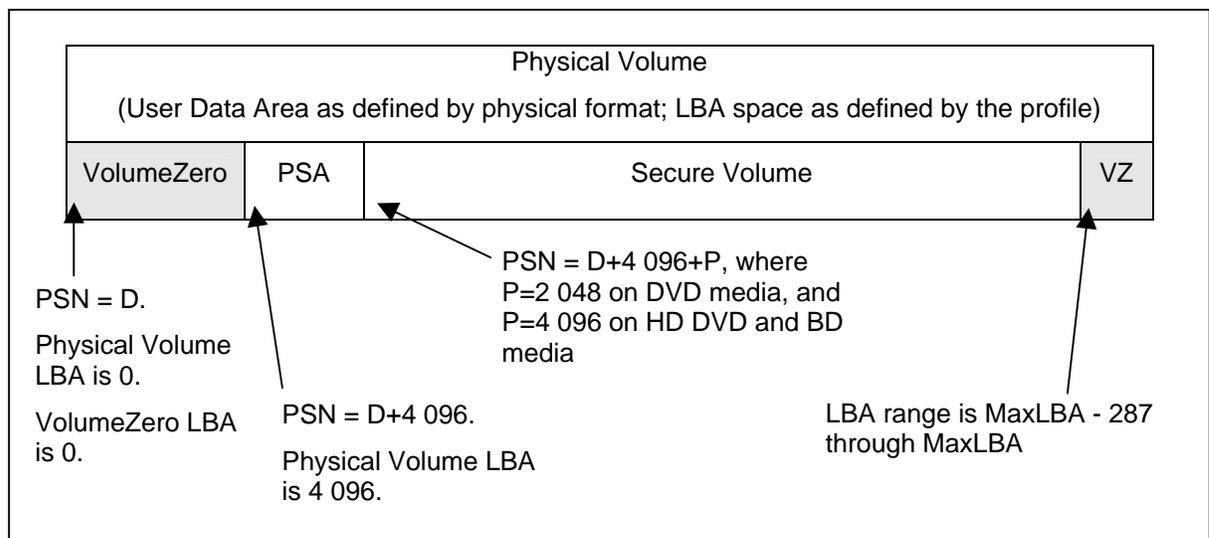
Figure 5 — OSSC Disc Format on the random writable model

4.3.2.2   VolumeZero

When the specified profile has the random writable model, VolumeZero has 2 components:

- o   The region of 4 096 sectors beginning at Physical Volume LBA = 0 and ending at Physical Volume LBA = 4 095.
- o   The region of 288 sectors beginning at Physical Volume LBA = Physical Volume Maximum LBA - 287 and ending at Physical Volume Maximum LBA.

This allocation in two disjoint areas permits the UDF file system to record mandatory structures at LBA = 256, LBA = MaxLBA, and LBA = MaxLBA - 256.

4.3.2.3   PSA Allocation

When the OSSC Format is applied to the random writable model:

- o   The PSA begins at the Physical Volume LBA = 4 096.
- o   The PSA size is set to 128 writable units. The writable unit size on DVD media is 16 sectors, the writable unit size on HD DVD media is 32 sectors, and the writable unit size on BD media is 32 sectors.

4.3.2.4   The Secure Volume

The start address (LBA = 0) of the Secure Volume is Physical Volume LBA = 4 096+P, where P is the length of the PSA in sectors. The maximum address of the Secure Volume is Physical Volume Maximum LBA - (4 096 + P + 288).

4.3.2.5   Initializing a Disc to the OSSC Format

The OSSC Format is derived from the format established by the overlying profile. The entire disc shall be formatted for use according to that profile. If Hardware Defect Management is available, the disc should be formatted with the recommended defect management capability.

The Host arranges the enrollment of the initial user with the following sequence:

TS	A Trusted Session is necessary for any user enrollment
PSAbegin	PSA initialize/update
RVZ	The currently connected user may be used to record the VolumeZero
EU (Initializer) EU (Common)	If more than one user is to be enrolled, the initial user shall be the Initializer. The Initializer may enroll any number of Common users - including zero.
PSAend	Any changes made to the OSPB shall be committed to the PSA.
MountSV (or Disconnect)	Send a Media Removal Event (dismount Physical Volume) then Send a New Media Event. The Host may also choose to disconnect from the Secure Volume.

If the disc is blank and not formatted, the response to the PSAbegin method is CHECK CONDITION status with sense keys SK/ASC/ASCQ set to ILLEGAL REQUEST/MEDIUM NOT FORMATTED. The Trusted Session is closed and the sequence is aborted.

The initial Anchor table of the OSPB is written in the first writable unit of the PSA. Fixed characteristics of the Anchor provide a signature for an OSSC initialized disc.

4.3.2.6   Mounting a Disc with the OSSC Format

A disc is loaded, spun up, and initialized according to the media physical format and established profile definitions. If the Drive is OSSC capable and the disc is not blank, the Drive shall also read the first writable unit starting at the Physical Volume that should correspond to the start of the PSA and test for an OSSC signature. If the OSSC signature is found, the current bit in the Trusted Computing Feature is set to one.

It is now the Host's responsibility to act upon the configuration information. If the Host is OSSC capable and discovers that the Trusted Computing Feature is current, then the Host may initiate further action with the following minimal sequence:

TS	A Trusted Session is necessary prior to any user connection
CU (Initializer) or CU (Common)	
MountSV (or Disconnect)	Send a Media Removal Event (dismount Physical Volume) then Send a New Media Event. The Host may also choose to disconnect the just connected user.

Once connected the Host may read or write the Secure Volume. If the Host attempts to connect any other user, a Disconnect is automatically performed. If the Host chooses to eject the media, a Disconnect is automatically performed.

4.3.2.7 Updating the OSPB

Host may attempt to modify the OSPB with the following sequence:

TS	A Trusted Session is necessary for any user enrollment
PSAbegin	PSA initialize/update
CU (Initializer) EU, DU, MU	A Initializer may enroll, erase, or modify any number of Common users - including zero.
PSAend	Any changes made to the OSPB shall be committed to the PSA.
MountSV (or Disconnect)	Send a Media Removal Event (dismount Physical Volume) then Send a New Media Event. The Host may also choose to disconnect from the Secure Volume.

If the disc is not OSSC, the Drive shall permit TS, if the disc is in a condition to be converted to OSSC, the Drive shall permit PSAbegin, but the CU shall fail and the Trusted Session is closed and the sequence is aborted.

Updating the OSPB in the PSA should have a generally sequential character in order to minimize the effects of rewrite wear-out. The first writable unit of the PSA shall be recorded with the first writable unit of the OSPB when the disc is converted to OSSC. This writable unit shall not be rewritten as part of an OSPB update. This is done for the purpose of consistent OSSC signature identification.
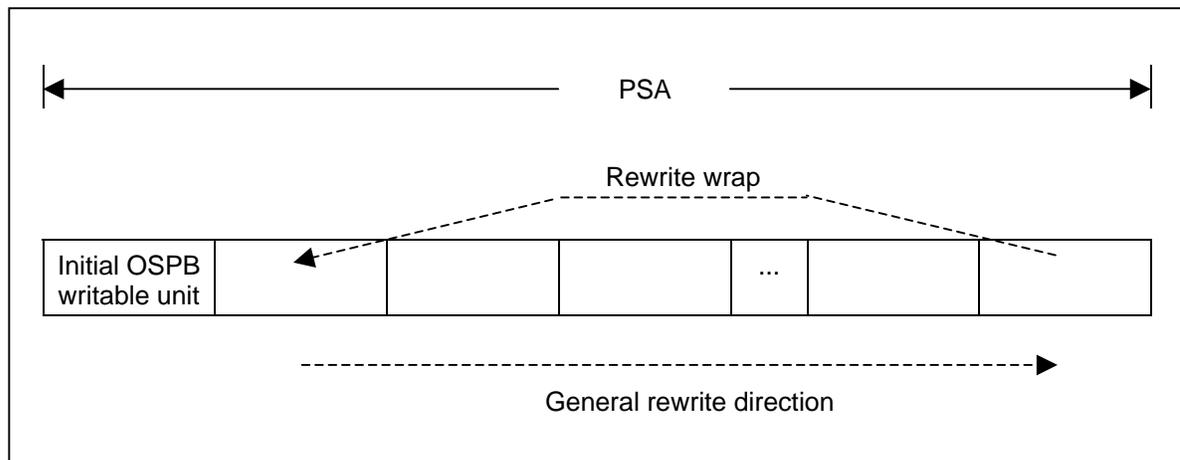
Figure 6 — OSPB Updates using Rewrite

4.3.2.8 Using a Mounted Secure Volume

When the Secure Volume is mounted, commands execute according to the overlying profile of the Physical Volume with the restriction that the LBA space of the media is according to the OSSC format.

4.3.3   OSSC Formats for the track/session model

4.3.3.1   Overview

This format may be applied to:

- o   DVD-R   DVD-R Sequential Recording Profile (0011h),
- o   DVD-RW SL   DVD-RW Sequential Recording Profile (0014h),
- o   DVD+R   DVD+R Profile (001Bh),
- o   DVD+R DL   DVD+R DL Profile (002Bh),
- o   HD DVD-R   HD DVD-R Profile (0051h), and
- o   BD-R   BD-R Sequential Recording Profile (0041h).

Only blank write-once media, blank rewritable media, or fully blanked rewritable media may utilize the OSSC format.

Due to the incremental recording nature of profiles that support the track/session model, the PSA and Secure Volume layout on the disc may vary with a given recorded state.

4.3.3.1.1   VolumeZero

Logical Track 1 is reserved for VolumeZero with a length of 4 096 sectors. Once Logical Track 1 is closed, session 1 is also closed.

4.3.3.1.2   PSA Allocation

The initial PSA is a Logical Track, reserved as Logical Track 2 with a length of 1 024 sectors. Once the initial OSPB has been written, Logical Track 2 is closed and session 1 is closed. At this point, session 2 (open and empty) contains the Secure Volume. See Figure 7.

When the OSSC Format is applied to the track/session model:

- o   The PSA begins at the start of Logical Track 2 according to the Physical Volume.
- o   The PSA size is set to 64 writable units. The writable unit size on DVD media is 16 sectors, the writable unit size on HD DVD media is 32 sectors, and the writable unit size on BD media is 32 sectors.

Once the initial version of the OSPB has been recorded, Logical Track 1 is closed, Logical Track 2 is closed, and session 2 is closed.
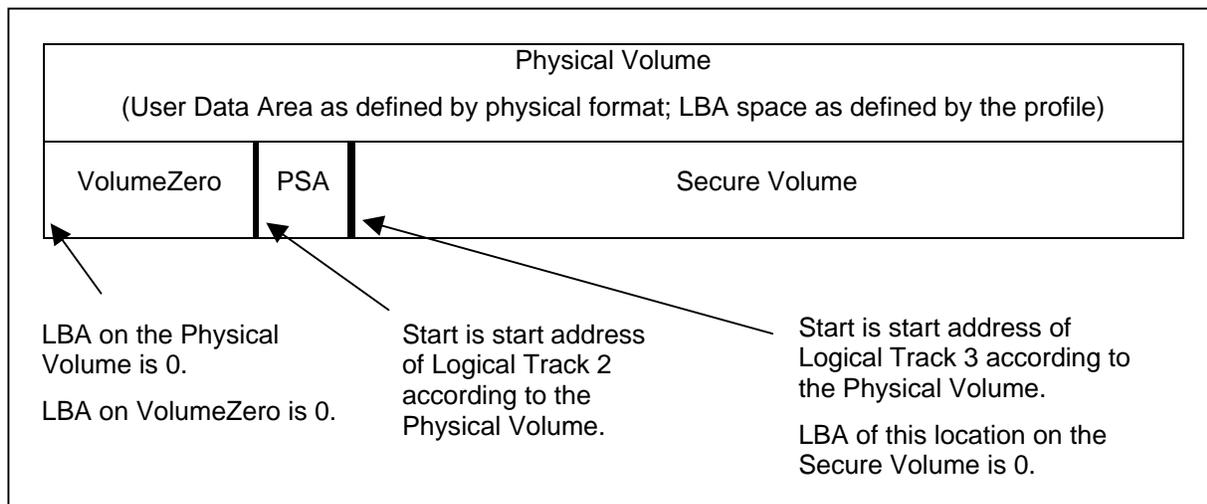

Figure 7 — OSSC Disc Format - initial state

The OSPB may be updated by appending a PSA update session to the last closed session in the Secure Volume. Each PSA update session is a single session containing a single Logical Track consisting of 64 writable units.

4.3.3.1.3   Secure Volume

The Secure Volume begins at the start of Logical Track 3 according to the profile for the physical volume. The length of the Secure Volume is the remainder of the Physical Volume.

4.3.3.2   Initializing a Disc to the OSSC Format

The OSSC Format is derived from the format established by the overlying profile. If formatting is required, the disc shall be formatted for use according to the associated profile. If Hardware Defect Management is available, the disc should be formatted with the recommended defect management capability.

The Host arranges the enrollment of the initial user with the following sequence:

TS	A Trusted Session is necessary for any user enrollment
PSAbegin	PSA initialize/update. Because the disc is blank, reserve Logical Track 1 for VolumeZero. Reserve Logical Track 2 for the initial PSA.
RVZ	The currently connected user may be used to record the ZeroVolume.
EU (Initializer) EU (Common)	If more than one user is to be enrolled, the initial user shall be the Initializer. The Initializer may enroll any number of Common users - including zero.
PSAend	Any changes made to the OSPB shall be committed to the PSA. Close Logical Track 2 (completed OSPB), padding if necessary. Close session 2.
MountSV (or Disconnect)	Send a Media Removal Event (dismount Physical Volume) then Send a New Media Event. The Host may also choose to disconnect the initial user.

The disc shall be ready for use: either blank or formatted when formatting is required. If the disc is not blank, the response to PSAbegin is CHECK CONDITION status with sense bytes SK/ASC/ASCQ set to BLANK CHECK/NO ADDITIONAL SENSE INFORMATION. If formatting is required and formatting has not been performed, the response to PSAbegin is CHECK CONDITION status with sense bytes SK/ASC/ASCQ set to ILLEGAL REQUEST/MEDIUM NOT FORMATTED. The Trusted Session is closed and the sequence is aborted.

The initial Anchor table of the OSPB is written the first writable unit of the PSA. Fixed characteristics of the Anchor provide a signature for an OSSC initialized disc.

After PSAend, the connection of the currently authenticated user remains in effect, but changes to the OSPB are no longer permitted. OSPB updating may occur only within a new PSA session. See 4.3.3.5.

4.3.3.3   Mounting a Disc with the OSSC Format

A disc is loaded, spun up, and initialized according to the media physical format and established profile definitions.

If the Drive is OSSC capable and the disc is not blank, the drive shall also read the first writable unit of Logical Track 2 (relative to the Physical Volume) and test for an OSSC signature. If the OSSC signature is found, the current bit in the Trusted Computing Feature is set to one.

It is now the Host's responsibility to act upon the configuration information. If the Host is OSSC capable and discovers that the Trusted Computing Feature is current, then the Host may initiate further action with the following minimal sequence:

TS	A Trusted Session is necessary prior to any user connection
CU (Initializer) or CU (Common)	
MountSV (or Disconnect)	Send a Media Removal Event (dismount Physical Volume) then Send a New Media Event. The Host may also choose to disconnect the just connected user.

Once connected the Host may read or write the Secure Volume. If the Host attempts to connect any other user, a Disconnect is automatically performed. If the Host chooses to eject the media, a Disconnect is automatically performed.
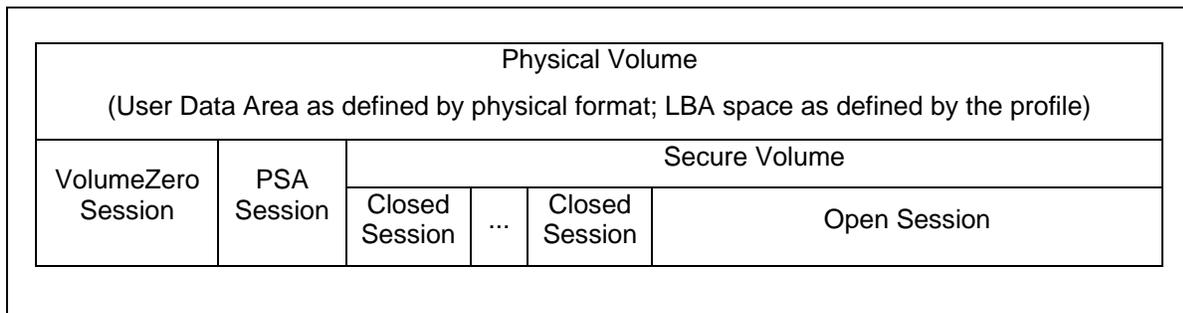
4.3.3.4   Using a Mounted Secure Volume

When the Secure Volume is mounted, commands execute according to the overlying profile of the physical media with the restriction that the LBA space of the media is according to the OSSC format, session and Logical Track numbers presented to the Host are adjusted downward to exclude the initial PSA and the PSA updates.

4.3.3.5   PSA Updates

When the profile used for the OSSC disc follows the track/session model, updating the PSA is optional behavior for the Drive.

After some number of recordings, the Secure Volume may have multiple sessions (Figure 8).

Physical Volume (User Data Area as defined by physical format; LBA space as defined by the profile)					
VolumeZero Session	PSA Session	Secure Volume			
		Closed Session	...	Closed Session	Open Session

Figure 8 — OSSC Disc Format - after recording multiple Secure Volume sessions

A PSA update is a session that may be appended to the existing session string. A PSA update is a session that contains a single Logical Track with a length of 64 writable units.

Host may attempt to modify the OSPB with the following sequence:

TS	A Trusted Session is necessary for any user enrollment
PSAbegin	PSA initialize/update
CU (Initializer) EU, DU, MU	A Initializer may enroll, erase, or modify any number of Common users - including zero.
PSAend	Any changes made to the OSPB shall be committed to the PSA.
MountSV (or Disconnect)	Send a Media Removal Event (dismount Physical Volume) then Send a New Media Event. The Host may also choose to disconnect from the Secure Volume.

If the disc is finalized, then the response to the PSAbegin is CHECK CONDITION with sense bytes SK/ASC/ASCQ set to ILLEGAL REQUEST/CANNOT WRITE MEDIUM - INCOMPATIBLE FORMAT.

If the last session is not empty, then the response to the PSAbegin is CHECK CONDITION with sense bytes SK/ASC/ASCQ set to BLANK CHECK/NO ADDITIONAL SENSE INFORMATION.

Once the Host has made changes to the OSPB and issued the PSAend method request, the Drive:

1. Reserves a Logical Track for the PSA,

2. Records the updated OSPB,

3. Closes the Logical Track, and

4. Closes the session.

4.4   Command Behavior

When an OSSC format disc is mounted, but no user has connected to the Secure Volume, the disc is viewed as the physical volume. Commands execute according to their definitions as specified by the profile.

Once a user has connected to the Secure Volume, commands execute according to their definitions as specified by the profile, but location references are likely to be different.

Table 5 shows how commands change behavior due to an LBA, Logical Track number or session number change.

Table 5 — Command Execution Change due to Addressing Reference Change

Command	Addressing Reference Change
BLANK	When a user is connected to the Secure Volume, the blanking operation is not performed and no error is reported.
FORMAT UNIT	When a user is connected to the Secure Volume, the formatting operation is not performed and no error is reported. When no user is connected and a disc that has a profile that is random writable and is in the OSSC format, the format shall overwrite the first writable unit in the PSA with zeros.
READ (10) READ (12) WRITE (10) WRITE (12) READ CAPACITY	The OSSC format for the random writable model specifies a sector offset. i.e. D_1 is the PSN that maps to LBA = 0 on the Secure Volume. If L is an LBA reference into the Secure Volume, the Drive shall map L to $L+D_1$. The OSSC format for the track/session model offsets the LBA space to the start of the first session that is not in the SessionMap. D_2 is the PSN of the first sector of the first session not in the SessionMap. If L is an LBA reference into the Secure Volume, the Drive shall map L to $L+D_2$. If writing to VolumeZero and the 8MB capacity is exceeded, the data is taken and no error is reported.
READ TOC/PMA/ATIP READ TRACK INFORMATION READ DISC INFORMATION RESERVE TRACK	The OSSC format for the random writable model shall behave according to the overlying profile with appropriate changes associated with the capacity difference. In the case of the track/session model, PSA sessions and PSA Logical Tracks are mapped out of existence relative to the Host.

The OSPB contains a SessionMap table. SessionMap is a list of Session numbers and Logical Tracks numbers that do not belong to the Secure Volume. Those numbers are given relative to the Physical Volume.

An example of Logical Track and session mapping is shown in Table 6.

Table 6 — Example of Logical Track and Session Mapping

Area Usage	Session relative to Physical Volume	Logical Track relative to Physical Volume	Session relative to Secure Volume	Logical Track relative to Secure Volume	SessionMap entry
VolumeZero	1	1	N/A	N/A	1,1
PSA	2	2	N/A	N/A	2,2
User Data	3	3	1	1	-
User Data	4	4	1	2	-
PSA	5	5	N/A	N/A	5,5
User Data	6	6	2	4	-
User Data	6	7	2	5	-
User Data	6	8	2	6	-
User Data	7	9	3	7	-
User Data	7	10	3	8	-
PSA	8	11	N/A	N/A	8,11
Empty	9	12	4	9	-

Since VolumeZero is never explicitly mounted, the Logical Track/Session numbering for VolumeZero are coincident with the Physical Volume and reported accordingly.

The example shows Logical Track/Session numbering responses for the Physical Volume and the Secure Volume. Certain behavior is shown:

o Logical Tracks and Sessions are defined according to the overlying profile of the Physical Volume. The numbering is reported differently only when the Secure Volume is mounted.

o When the Secure Volume is mounted, all Logical Tracks and Sessions that do not contain user data are viewed as non-existent and their numbers are not reported.

o The SessionMap contains 4 entries.

5   FEATURES and PROFILES

5.1   Trusted Computing Feature

When Trusted Computing Feature is present in the feature list, the Drive claims support for the Trusted Computing Group capabilities.

Table 7 — Trusted Computing Feature Descriptor Format

Bit Byte	7	6	5	4	3	2	1	0
0	Feature Code = 0142h							
1								
2	Reserved		Version				Persistent	Current
3	Additional Length = 2*P+2							
4	PSAU	LOSPB	Reserved					ME
5	Number of Profiles (P)							
6	1st Profile Number							
7								
8	2nd Profile Number							
9								
...								
2*P+4	Last Profile Number							
2*P+5								

The Feature Code field shall be set to 0142h.

The Version Field shall be set to 0000b.

The Persistent bit shall be set to zero.

If the Current bit is set to zero, the currently mounted medium is not recognized as a TCG initialized medium. If the Current bit is set to one, the currently mounted medium is recognized as a TCG initialized medium.

The Additional Length field shall be set to 2*P+2, where P is the Number of Profiles.

When PSAU is set to zero, the Drive does not support PSA updates on write-once media. When PSAU is set to one, the Drive supports PSA updates on write-once media.

When LOSPB is set to zero, the Drive does not support linked OSPBs, limiting the number of users to independently connectable users to 112. When LOSPB is set to one, the Drive does supports linked OSPBs.

When ME (Mandatory Encryption) is set to one, the Drive is restricted to recording only the OSSC Disc Format.

The Number of Profiles field specifies the number of profiles for which the Trusted Computing Feature may become current.

The list of profile numbers that follow the Number of Profiles field is a list of profiles for which the Trusted Computing Feature may become current. Each profile number shall appear in the list exactly once. The list shall be sorted from smallest to largest profile number.

Drives that claim the Trusted Computing Feature shall implement the commands specified in Table 8.

Table 8 — Trusted Computing Feature Commands

Op Code	Command Description	Reference
A2h	SECURITY PROTOCOL IN Security Protocol 01h with Security Specific codes 7007h and 7008h shall be supported	6.2
B5h	SECURITY PROTOCOL OUT Security Protocol 01h with Security Specific codes 7007h and 7008h shall be supported	6.3

6   COMMAND DESCRIPTIONS

6.1   Overview

The commands described in this clause are those that are either unique to the Trusted Computing Feature or have modified behavior when the Trusted Computing Feature is present.

Table 9 — Commands for Multi-Media Drives

Command Name	Op Code	Reference
SECURITY PROTOCOL IN	A2h	6.2
SECURITY PROTOCOL OUT	B5h	6.3

6.2 SECURITY PROTOCOL IN command

6.2.1 Overview

The SECURITY PROTOCOL IN command (see Table 10) is used to retrieve security protocol information (see) or the results of one or more SECURITY PROTOCOL OUT commands (see).

6.2.2 The CDB and its Parameters

6.2.2.1 The CDB

The SECURITY PROTOCOL IN CDB is shown in Table 10.

Table 10 — SECURITY PROTOCOL IN command

Bit Byte	0	1	2	3	4	5	6	7
0	OPERATION CODE (A2h)							
1	SECURITY PROTOCOL							
2	SECURITY PROTOCOL SPECIFIC							
3								
4	INC_512	Reserved						
5	Reserved							
6	ALLOCATION LENGTH							
7								
8								
9								
10	Reserved							
11	CONTROL							

6.2.2.2 SECURITY PROTOCOL

The SECURITY PROTOCOL field specifies which security protocol is being used. OSSC drives support only SECURITY PROTOCOL = 00h, 01h.

6.2.2.3 SECURITY PROTOCOL SPECIFIC

The contents of the SECURITY PROTOCOL SPECIFIC field depend on the protocol specified by the SECURITY PROTOCOL field. OSSC drives support only SECURITY PROTOCOL SPECIFIC field = 0001h.

Level 0 Discovery: 1,1

Local Host doing real work: 1, 7007

External Host providing a factor: 1,7008

6.2.2.4 INC_512

If INC_512 is set to one, the ALLOCATION LENGTH field multiplied by 512 is the maximum number of bytes to be transferred.

If INC_512 is set to zero, the ALLOCATION LENGTH field is the maximum number of bytes to be transferred.

MMC Drives that implement the Trusted Computing Feature shall support only INC_512 = 0b.

6.2.2.5   ALLOCATION LENGTH

The ALLOCATION LENGTH field specifies the maximum number of bytes that the Host has allocated in the Data-In Buffer.

An allocation length of zero specifies that no data shall be transferred. This condition shall not be considered as an error.

6.2.3   Command Processing

SECURITY PROTOCOL OUT command is used to request that the OSSC drive execute a security method (function). Upon completion, the SECURITY PROTOCOL IN command is used to request that the OSSC Drive return the response from the most recently processed method.

The format of each method response block is described in [OSSC].

6.3   SECURITY PROTOCOL OUT command

6.3.1   Overview

The SECURITY PROTOCOL OUT command is used to send data to the Drive. The data sent specifies one or more operations to be performed by the Drive. The Host may use the SECURITY PROTOCOL IN command (see Table 11) to retrieve data derived from these operations.

6.3.2   The CDB and its Parameters

6.3.2.1   The CDB

The SECURITY PROTOCOL OUT CDB is shown in Table 11.

Table 11 ─ SECURITY PROTOCOL OUT command

Bit / Byte	0	1	2	3	4	5	6	7
0	OPERATION CODE (B5h)							
1	SECURITY PROTOCOL							
2	SECURITY PROTOCOL SPECIFIC							
3								
4	INC_512	Reserved						
5	Reserved							
6	TRANSFER LENGTH							
7								
8								
9								
10	Reserved							
11	CONTROL							

6.3.2.2   SECURITY PROTOCOL

The SECURITY PROTOCOL field specifies which security protocol is being used. OSSC drives support only SECURITY PROTOCOL = 00h, 01h.

6.3.2.3   SECURITY PROTOCOL SPECIFIC

The contents of the SECURITY PROTOCOL SPECIFIC field depend on the protocol specified by the SECURITY PROTOCOL field. OSSC drives support only SECURITY PROTOCOL SPECIFIC field = 0001h.

Level 0 Discovery: 1,1

Local Host doing real work: 1, 7007

External Host providing a factor: 1,7008

6.3.2.4   INC_512

If INC_512 is set to one, the TRANSFER LENGTH field is the number of 512 byte increments to be transferred.

If INC_512 is set to zero, the TRANSFER LENGTH field is the number of bytes to be transferred.

MMC Drives that implement the Trusted Computing Feature shall support only INC_512 = 0b.

6.3.2.5   TRANSFER LENGTH

The TRANSFER LENGTH field specifies the number of bytes to be transferred.

6.3.3   Command Processing

SECURITY PROTOCOL OUT command is used to request that the OSSC drive execute a security method (function). The request is made by sending a security method request block to the OSSC Drive. The format of each method request block is described in [OSSC].

7   MODE PARAMETERS

No new mode pages are defined for the support of OSSC.

No existing mode page has been modified for the support of OSSC.

END