07-422R0

Optical Security Subsystem Class Reference – 0.4 draft

2007-09-20

Randal Hines

DPHI, Inc.

1900 Pike Road, Suite F

Longmont, CO 80501

Ph.: +1 303 952 2467

Fax.: +1 303 952 2451

email: rhines@dataplay.com

Contents

1 Introduction

1.1 Scope and Audience

Because optical discs are secondary rather than primary storage and removable rather than fixed media, they have different roles and benefits than other storage devices such as hard disk drives (HDD):

- Interchange and distribution, including 'slow mail' and 'sneaker net'
- Archival and backup
- Replication

These benefits induce different security issues than HDD. Disc interchange among optical drives is fundamental, but interchange opens two possibilities of attack. Since the medium is no longer coupled to a device, any optical drive is a potential attack platform, and worse, TCG discs may be inserted into legacy drives that are unaware of TCG security. These attack possibilities are mitigated with additional security measures, but TCG optical storage is always more complex and inherently more open than HDD.

This document defines a TCG compliant, optical TPer (**T**rusted **Per**ipheral), part of which is formed within a drive and part which is transported on an optical disc. The basis of the optical TPer is provided in an Optical SP (**S**ecurity **P**rovider).

The outline of this document is as follows. First, optical storage characteristics and requirements are presented. The T10 Multi-Media Command (MMC) standard, which defines commands, models, and behavior for optical drives, is the primary focus. Next, the requirements of a TPer within an optical drive are presented; included are cryptographic elements and use case summaries. These two sections include a few keyword statements, but their primary purpose is to inform and provide architectural rationale. Section 4, Optical SSC Definitions, is the formal definition of the optical TPer. Section 5, Entity Authentication, explains user and n-factor authentication. Finally, Section 6, Use Scenarios (Informative), provides examples of how to implement and use the optical TPer.

1.2 Key Words and Terminology

Key words are used to signify the requirements in the specification. The key words "SHALL," "SHOULD," "MAY," and "OPTIONAL" are used in this document. These words are a subset of the RFC-2119 key words used by TCG, and have been chosen since they map to key words used in T10 and MMC specifications. These key words are to be interpreted as described in [RFC-2119].

Description and specification of document elements are declaratory and use the semantics of the Object Constraint Language (see www.omg.org). In particular, invariants, preconditions, postconditions and descriptive assertions are used as appropriate.

Definitions:

- **Constant:** a value or a set of values that do not change
- **Drive:** supplier of services consumed by host
- **Host:** consumer of services supplied by drive
- **IHost:** MMC initiator to which an optical drive is directly attached
- **Invariant:** an assertion that is true over the lifetime of a specified entity
- **MMC:** Multi-Media Commands standard from the ANSI / INCITS T10 committee

- **Pass code:** a password, pass phrase, or PIN that is used to identify a user
- **Postcondition:** an assertion that is true after a procedure; the invoked entity is responsible for this guarantee.
- **Precondition:** an assertion that is true before a procedure; the invoking entity is responsible for this guarantee.
- **Protected Storage Area:** a confidential area of the optical disc managed by a TPer
- **R / RW / RW1:** fields are specified as **R**ead only / **R**ead and **W**rite / **R**ead many times and **W**rite **1** time
- **SA Core:** Storage Architecture Core Specification[15] published by the Trusted Computing Group
- **TCG disc:** the protected storage area as defined in the Optical SSC has been initialized
- **TPer:** Trusted Peripheral
- **Well-known:** a specified constant

1.3 References

References used in this document are in Section 7.

1.4 Document History

See Appendix D.

2 Optical Storage Requirements

2.1 Protected Storage Area

The SA Core requires a protected storage area for Security Provider (SP) tables – storage that is persistent, that is not included in the user address space and that is not effected by host partitioning and formatting. Rather than weaken security with secrets in hidden disc areas, the Optical SSC defines a protected storage area that is cryptographically protected and requires external agents to manage authentication and pass codes. The protected storage area is specified such that it does not interfere with any physical disc format; see the MMC-6 standard[15] for more information.

2.2 Disc Types

Three disc types shall be supported by the Optical SSC: ROM (read only), R (write once), and RW (rewritable). Users select their required data persistence by their choice of disc type, ROM, R, and RW. MMC compliant drives do not overwrite data on ROM or R discs; legacy, non-TCG drives can overwrite data on RW discs.

(Informative)

Users must consider their application requirements before selecting the recording characteristics of their optical disc:

- ROM discs cannot be written; changes to the on-disc Optical SP are not possible. ROM discs are typically used for mass distribution.
- R discs can only be written once. Changes to the on-disc Optical SP consume storage capacity. R discs are also used for distribution and archival applications.
- RW discs behave more like HDD. However, they are susceptible to reformatting and data overwriting in legacy drives. Reformatting does not expose user data, but it does destroy data. RW discs are typically chosen when users want to make changes to the disc without consuming capacity or reuse discs. RW discs support only a small number of rewrite cycles (~1000 average).

3 Optical TPer Requirements

An optical TPer has capabilities that allow optical storage to conform and support the access control policies of users and organizations.

3.1 Architectural Considerations (Informative)

There are four key themes that strongly influence the architecture of the optical TPer:

- Media Interchange
- Limited resources including protected storage area
- Read only (ROM), write once (R), and limited rewritable (RW) media
- Single process, synchronous MMC architecture

Because of the interchange requirement, parts of an Optical SP are written to a protected storage area on the disc. All TCG optical drives must be able to locate the Optical SP on any disc, and semantically read the tables that form the Optical SP. Because any drive may be able to read a TCG disc, TCG or legacy, the protected storage area is partially encrypted. The encryption key for the Optical SP is derived from external pass codes; it is not stored on the disc. Without appropriate credentials, the Optical SP cannot be decrypted and the data on the disc remains confidential.

Limited resource is a severe concern. There are two mandatory SP's, Admin and Optical. The Admin SP is formed entirely by device firmware. Many tables of the Admin SP, as defined in the SA Core, are not mandatory on the TPer, and convention (constant, well-known names and UID's) is chosen over discovery and versatility. These decisions minimize the TPer footprint in the optical drive. The Optical SP is also formed from device firmware, but some of its tables are stored in the protected storage area on the disc. The Optical SSC tables that are on disc are minimal because the size available for protected storage is limited.

Optical recording technologies severely constrain the TPer architecture. It is not possible to spool tables, and optical recording behaves best when recording is sequential. In general, performance suffers and/or capacity is consumed when changes are made to the on-disc Optical SP.

Historically, optical drives have been operated by a single process in a synchronous command/response pattern. The reasons for this limitation are because optical use cases depend on this environment. Streaming multimedia and write once recording break without a single process/synchronous model. The Optical SSC limits the SWG protocol stack and behavior so that the requirements imposed by the SCC are compatible with MMC and the device architectures that support optical use cases.

3.2 Security Elements

3.2.1 TPer Authentication

A TPer requires a certificate to participate in mutual authentication procedures. The Exchange method (SA Core 5.3.5.1.7) is used. See "Appendix B. Trusted Optical Disc Authority" for TPer certificates. A device certificate is a customary requirement for optical disc security systems.

3.2.2 Client Software Authentication

Client software must successfully participate in a mutual authentication procedure before using trusted TPer features. The Exchange method (SA Core 5.3.5.1.7) is used. See “Appendix B. Trusted Optical Disc Authority” for client software certificates. A client certificate is a customary requirement for optical disc security systems.

3.2.3 AES Encryption

Symmetric cryptographic functions are based on the Advanced Encryption Standard (AES) block cipher algorithm as specified in FIPS Publication 197. Both AES-128 and AES-256 are allowed; only AES-128 is mandatory.

CBC Mode

For encryption/decryption of all data streams, the AES cipher is used in the Cipher Block Chaining (CBC) mode. The CBC mode is specified in NIST Special Publication 800-38A.

For encryption/decryption of data in the user area, the message length is one ECC block. See “Appendix B. Trusted Optical Disc Authority” for the Initialization Vector (IV) of each message. Because of the interchange requirement, this algorithm is mandatory and all other algorithms that operate on user data streams are disallowed.

3.2.4 DeriveKey()

Users provide a pass code credential to connect to a disc. A derived key (DK) is generated from the pass code with the DeriveKey() algorithm. If a user is being added to the TPer, the DK is used to encrypt a user record. If a user is connecting to the TPer, the DK is used to decrypt the user record. See “Appendix B. Trusted Optical Disc Authority” for more information.

3.2.5 MakeEAC(), CheckEAC()

The TPer maintains a unique record for each user; each user record holds the key that encrypts the protected storage area and also an **E**ntity **A**uthentication **C**ode (EAC) that validates a user’s pass code. Given a user pass code, a DK is generated. If a user is being added to the TPer, the MakeEAC() algorithm is executed, the EAC is added to the user record, and the user record is encrypted with DK. If a user is connecting to the TPer, the user record is decrypted, and the CheckEAC() algorithm is used to validate the user’s pass code. See “Appendix B. Trusted Optical Disc Authority” for more information.

3.3 Deviations from Core Specification

Table 1 lists the deviations between the Core Specification[15] and the Optical SSC.

Table 1. Deviations from the SA Core

SWG Section	Description	Comments
3.2.3	Stream Encoding	• Methods and transactions shall be sent in their entirety in a single interface command. • Exactly one ComPacket / Packet / Subpacket combination shall be allowed per interface command. • Flow control is not supported

3.3.2-3.3.3	ComID	• Static ComID values shall be used. The ComID 0x0777 will be used by default and is considered in the "Issued" state after POR. • GET_COMID, HANDLE_COMID_REQUEST, GET_COMID_RESPONSE are not supported.
3.4.3	SP Issuance, et al	• No host issuance is supported.
3.4.4	Sessions, Methods, Transactions	• A maximum of one open session is supported. • Transactions shall be sent in a single interface command. Each interface command shall send exactly one transaction, and subsequent interface commands will receive the results in a synchronous pattern. • Transactions shall not be nested.
3.4.6	Stream Flow Control	• Flow control shall not be supported. • There shall be no Credit negotiation. TPer and Host IF_SEND and IF_RECV buffers shall be 2k bytes in size. • There shall be no ACK/NACK protocol.
4	Life Cycle of SPs	• Only support Issue (Enabled). All other Life Cycle states are not supported.
5.3.3.6	Get Method	• The get method is limited to retrieving one row at a time from a table; multiple columns within a row may be selected. This limitation is to prevent overflowing the 2k buffer size limits imposed above.

3.4 Requirements from Use Cases

Use cases are target applications that guide the development process. The Optical SSC supports four use cases:

- Simple, personal password protection for sneaker net
- Plurality of passwords for disc distribution by slow mail
- Distribution of electronic health records
- Secure network endpoint for emergency response situations

3.4.1 Access Mechanisms

3.4.1.1 Full Disc Encryption (FDE)

A TCG optical drive supporting FDE is responsible for preventing host access until a valid pass code has been presented. Upon receipt of a valid pass code, all writes to the disc are encrypted, and all reads from the disc are decrypted. FDE is mandatory on TCG discs.

3.4.1.2 Application Specific Access Control

Application specific fields are provided for the disc and for each user. Use of these fields require registration. See "Appendix B. Trusted Optical Disc Authority" for more information.

3.4.2 Strength of Symmetric Cryptography

AES-128 is required, and AES-256 is optional. The Optical SSC supports both.

3.4.3 Mandatory Full Disc Encryption

Mandatory full disc encryption is a personalization option that forces FDE writing on all discs. With presentation of proper credentials, the option may be programmatically overridden. This option supports an organizational policy that requires all disc writing to be confidential.

4 Optical SSC Definitions

4.1 Admin SP

The Admin SP includes a Base template, an Admin template, and a Disc table. The SA Core[15] provides definitions for the Base template and Admin template; section references are provide in Table 7. The SA Core requires exactly one Admin SP in every TPer; the Admin SP for the Optical SSC is read only.

Table 2. Mandatory Admin SP Tables

Table	Section	Comment
SA Core Tables	Appendix C. SA Core Tables	Table 14
Properties	Section 4.1.1	SA Core 5.2.2
Disc	Section 4.1.2	Use to discover state of optical disc

Admin SP invariant:

- UID and Name fields of the first two rows of SP Table (Admin SP) are well-known

UID	Name	ORG	Effective Auth	Date Of Issue	Bytes	Life Cycle State	Frozen
00 00 02 05 00 00 00 01	Admin					0	false
00 00 02 05 77 77 77 01	Optical					0	false

4.1.1 Properties Table

The Optical SSC Properties table extends the SA Core with version information.

Table 3. Optical Properties Table

Property	Type	Value	Description
SessionVersion	bytes		SWG 5.2.2.1, Table 30
Packet	uinteger	2048 bytes	SWG 5.2.2.1, Table 30
ComIDPacket	uinteger	2048 bytes	SWG 5.2.2.1, Table 30
MaxSessions	uinteger	2	SWG 5.2.2.1, Table 30
MaxReadSessions	uinteger	1	SWG 5.2.2.1, Table 30
MaxIndTokenSize	uinteger		SWG 5.2.2.1, Table 30
MaxAggTokenSize	uinteger		SWG 5.2.2.1, Table 30
MaxAuthentications	uinteger	2	SWG 5.2.2.1, Table 30
MaxTransactionLimit	uinteger		SWG 5.2.2.1, Table 30
MaxSessionTimeout	uinteger		SWG 5.2.2.1, Table 30
MinSessionTimeout	uinteger		SWG 5.2.2.1, Table 30
DefSessionTimeout	uinteger		SWG 5.2.2.1, Table 30
MaxComIDTime	uinteger		SWG 5.2.2.1, Table 30
RealTimeClock	boolean		SWG 5.2.2.1, Table 30
OpticalSPVersion	uinteger{4}	0,0,0,1	Version of this document = 0,0,0,1
OpticalProtocolVersion	uinteger{4}	0,0,0,1	Version of Optical SSC protocol = 0,0,0,1

4.1.2 Disc Table

The Disc table publishes information about the optical disc that is inserted in the drive; it exhibits dynamic, asynchronous behavior as discs are inserted, written, and removed. The Disc table provides a TCG method for discovering whether a disc is inserted or not and the properties of an inserted disc.

Table 4. Disc Table Description

Column	Type	R/W	Description
UID	uid	R	UID of row = 7777 0005 0001 0000h; assigned and maintained by the TPer
DiscState	uinteger{4}	R	bit field of disc state; see Table 5
DiscType	uinteger{2}	R	enumeration of disc format; see Table 6

Table invariants:

- UID of the Disc table is 7777 0005 0000 0000h
- Disc shall have exactly one row
- Disc is read only

Table 5. DiscState Description

DiscState Value	Description
0	No disc
1	Blank disc
2	Format is permitted
4	Disc is TCG (protected storage area has been initialized)
8	Protected Storage Area is not full
10h	Disc is finalized

Table 6. DiscType Description

DiscType Value	Description
0	No disc
1	CD-Audio
2	CD-ROM
3	CD-R
4	CD-RW
5 – 0Fh	reserved
10h	DVD-ROM
11h	DVD-RAM
12h	DVD-R
13h	DVD-RW
14h	DVD-R DL
15h	DVD-RW DL
16h – 17h	reserved
18h	DVD+RW
19h	DVD+R
1Ah	DVD+RW DL
1Bh	DVD+R DL
1Ch – 1Fh	reserved
20h	HDDVD-ROM
21h	HDDVD-RAM
22h	HDDVD-R
23h	HDDVD-RW
24h	reserved

28h	BD-ROM
29h	BD-R
2Ah	BD-RE

4.2 Optical SP and Template

The Optical SP includes a Base template and an Optical template. The Base template provides authorities, methods and access control primitives. The Optical template contains disc keys, user information and an application specific access control mechanism, and is partially contained in the protected storage area of the disc.

Tables of the Base template are defined in the SA Core[15]; references are provided in Table 7. The Optical template is defined in this document.

Table 7. Mandatory Optical SP Tables

Table	Template	Section	Comment
SA Core Tables	Base	Appendix C. SA Core Tables	Formed by TPer and not on disc, Table 15
DriveInfo	Optical	Section 4.2.1.1	Formed by TPer and not on disc, Table 8
Anchor	Optical	Section 4.2.1.2	On disc, Table 10
DiscInfo	Optical	Section 4.2.1.3	On disc, Table 11
C_User	Optical	Section 4.2.1.4	On disc, Table 12

4.2.1 Optical Template

The Optical template includes:

- DriveInfo table: information about the drive, exactly one row
- Anchor table: well-known start of optical template as stored on the disc, one row per table
- DiscInfo table: information about the disc, exactly one row
- C_User table: vital information about users, one row per user
- ISO9660 table: default clear text volume that announces TCG disc

4.2.1.1 DriveInfo Table

The DriveInfo table is formed from TPer firmware; it is not written to the disc. It provides information about the optical drive capabilities and a personalization option to force encrypted writing.

Table 8 DriveInfo Table (Object Table)

Column	Type	R/W	Description
UID	uid	R	DriveInfo object = 7777 0004 0001 0000h
MaxUsers	uinteger{4}	R	maximum number of users that drive can enroll or authenticate
DriveAES	uinteger{1}	R	Drive encryption capability bit field; 1= AES-128; 2= AES-256
ForceEncryptionDefault	uinteger{1}	RW	=TRUE and ForceEncryption shall revert to ForceEncryption =TRUE with each disc change
ForceEncryption	uinteger{1}	RW	=TRUE and all writes shall be encrypted; =FALSE and writes shall not be encrypted

Note: R: Read only; RW: Read and Write

Table invariants:

- UID of DiscInfo table = 7777 0004 0000 0000h
- DriveInfo shall contain exactly one row.
- Only a Host authority shall write or read DriveInfo

4.2.1.2 Anchor Table

The Anchor table enables interchange and lists the tables that are the on disc. The RowType and Name fields of the first three rows of an Anchor table (Table 10) are mandatory and constant. This invariant allows the Anchor table to be used as a signature for TCG initialized discs. The first sector of the user data area of all disc formats is a well-known starting location to begin searching for the most recent Anchor table. The Anchor table may span more than one sector, and it is terminated by the RowType =7777FFFF h and Name =ISO9660.

Table 9. Anchor Table Definition (Object Table)

Column	IsOrdered	Type	Description
RowType	yes	uinteger{4}	Four most significant bytes of the UID of the table written to disc
Name		uinteger{16}	Table name; character set = UTF-8; right padded with zeroes
PSARSA		uinteger{4}	Protected Storage Area Relative Sector Address; sector address relative to the start of the Protected Storage Area
Offset		uinteger{2}	byte offset from start of a sector
SeqOrSeg		uinteger{2}	RowType ≠7777003h and field is a sequence number of the table or RowType =7777003h and field contains a C_User segment number; C_User is constructed with segments, where each segment is 2048 bytes; segments are ordered according to their position in the anchor table; a sequence number represents a monotonically increasing version number
Size		uinteger{4}	size of table

Table Invariant:

- All access to the Anchor table shall not be allowed and the result of any method shall be NOT_AUTHORIZED.

Table 10. Initial Anchor Table Mandatory Rows

RowType	Name	PSARSA	Offset	SegOrSeq	Size	Comment
77 77 00 01 h	Anchor	0	0	1	1952	this table
77 77 00 02 h	DiscInfo	0	1952	1	96	Disc descriptor; written exactly once; see Table 11
77 77 00 03 h	C_User	1	0	1	256	Used to authenticate users; see Table 12
77 77 00 03 h	C_User	2	0	2	0	2nd sector of C_User records
more C_User rows …						
77 77 00 03 h	C_User	31	0	2	0	31st sector of C_User records
77 77 FF FE h	EMPTY	0	0	0	0	1st empty row in Anchor
more EMPTY rows …						
77 77 FF FE h	EMPTY	0	0	0	0	27th empty row in Anchor
77 77 FF FF h	ISO9660	16	0	FF FF h	see Comment	cleartext ISO 9660 volume; Size field is measured in sectors; terminates Anchor table sequence

Table Invariants:

- All Anchor tables shall include the first three rows in the given order

- DiscInfo.SegOrSeq = 1 because DiscInfo is a write once table; subsequent updates to the protected storage area shall be exact copies of the initial DiscInfo
- Rows of RowType =77770003 h (C_User) shall be located in monotonically increasing row positions
- The minimum number of C_User rows shall be the number of sectors in a single recordable unit minus the number of sectors in the Anchor table sequence, where a single recordable unit is defined by a disc format
- Rows of RowType =7777FFFD h are for tables that are not defined in the Optical SSC and shall be located in monotonically decreasing row positions; this RowType is optional
- Rows of RowType =7777FFFE h (Name =EMPTY) shall begin after RowType =7777000D h and shall end at the row position before RowType =7777FFFF h
- There shall be exactly one row of RowType =7777FFFF h (Name =ISO9660) which shall begin 128 bytes from the end of the last sector of the Anchor Table sequence

4.2.1.3 DiscInfo Table

The DiscInfo table is a disc descriptor that includes parameters that apply to the entire disc. DiscInfo is initially formed by the TPer with default values. During connection to TCG a disc, the TPer overwrites the default values with DiscInfo from the disc. At disconnect, the TPer reverts DiscInfo to its default values.

DiscInfo or a copy of DiscInfo shall be located in the last 96 bytes of the last sector of an Anchor table sequence. As DiscInfo is a write once table, it shall not be changed after it is initially written and subsequent instances of DiscInfo shall be copies of the initial table.

DiscInfo includes a field for application specific metadata. Use of this field requires registration. See “Appendix B. Trusted Optical Disc Authority” for more information.

Table 11. DiscInfo Table (Object Table)

Column	Type	IsEncrypted	R/W	Description
UID	uid	F	R	DiscInfo object = 7777 0002 0001 0000h
CurrentUser	uinteger{4}	F	R	row number in C_User of the currently connected user; = 0 and no user connected
PSAsize	uinteger{4}	F	RW1	size in sectors of protected storage area
ISO9660size	uinteger{4}	F	RW1	size in sectors of default ISO9660 clear text volume
CryptoType	uinteger{1}	F	RW1	=0 and not initialized; =1 and AES-128; =2 and AES-256
AppIsEncrypted	uinteger{1}	F	RW1	=0 and Application field is not stored encrypted or =1 and Application field is encrypted with C_User.PSAkey
AppType	uinteger{2}	F	RW1	=0 and Application = 0 or ≠0 and Application field is valid; applications shall register AppType; see “Appendix B. Trusted Optical Disc Authority”
Application	bytes{32}	AppIsEncrypted	RW1	Application specific field determined by AppType
FDEkey	bytes{32}	T		AES-128 or AES-26 key used for full disc encryption; =0 and not initialized; key size is specified by CryptoType; CryptoType = AES-128 and 16 most significant bytes = 0; this field is encrypted with C_User.PSAkey;
Area12	bytes{12}	F		reserved for future use

Note: R: Read only; RW: Read and Write; RW1: Read many times and Write 1 time

Table invariants:

- UID of DiscInfo table = 7777 0002 0000 0000h
- DiscInfo shall contain exactly one row

- Column ≠ UID and default value = 0
- DiscInfo shall be written exactly once per disc by the Host authority
- Only a Host authority shall be able to read DiscInfo

4.2.1.4 C_User Table

Each row in the C_User table represents a single user. Each user is associated with a pass code and, optionally, other authentication factors. Users may be optionally identified with the UserName column. The pass code is not stored in this table, but rather is used to generate a derived key which decrypts a user record.

Each user record includes an encryption key (PSAkey) that is used to encrypt sensitive fields in the protected storage area and an **E**ntity **A**uthentication **C**ode (EAC) that verifies the validity of the pass code. Advantageously, multiple user records may exist, each having a different derived key that is used to encrypt the same PSAkey, thereby allowing different users access to the disc even though they have individualized pass codes.

C_User is initially formed by the TPer with default values. During connection to a TCG disc, the TPer overwrites the default values with C_User from the disc. On disconnect, the TPer reverts C_User to its default values.

Table 12. C_User Table (Object Table)

Column	Type	IsEncrypted	R/W	Description
User	uid	F	R	Unique ID of this row, which represents a user
IsValid	uinteger{1}	F	R	=0 and this row is uninitialized; =1 and this row is erased; =2 and this row is valid
IsKingpin	uinteger{1}	F	RW	=1 and this row has privilege to add, erase and modify arbitrary rows and columns of this table
UserName	bytes{64}	F	RW	Optional text to identify and select users of this disc; has no cryptographic value; character set = Unicode; right padded with zeroes
Nfactors	uinteger{1}	F	RW	number of authentication factors
AppIsEncrypted	uinteger{1}	F	RW	=0 and Application field is not encrypted or =1 and Application field is encrypted with DeriveKey() result
AppType	uinteger{2}	F	RW	=0 and Application = 0 or ≠0 and Application field is valid; applications shall register AppType; see "Appendix B. Trusted Optical Disc Authority"
Application	uinteger{32}	AppIsEncrypted	RW	Application specific field specified by AppType
Area51	bytes{50}	T		reserved future use
Salt	bytes{32}	F		Used in calculation to derive key from pass code
PSAKey	bytes{32}	T		Protected storage area key encrypted with DeriveKey() result; key size is specified by DiscInfo.CryptoType; DiscInfo.CryptoType = AES-128 and 16 most significant bytes = 0
EAC	bytes{32}	T		entity authentication code used to validate user pass code

Note: R: Read only; RW: Read and Write;

Note: shaded rows are hidden.

Table invariants:

- UID of C_User table = 7777 0003 0000 0000h
- Column ≠ User and default value = 0
- TPer assigns UID with template 7777 0003 0001 xxxxh

- Ciphertext fields are encrypted with the result of the DeriveKey()
- The Set method on C_User is not allowed and shall return NOT_AUTHORIZED
- A row is not valid until the host executes a successful AddUserEnd [ ] upon the row
- All successor rows of a row with IsValid = 0 also have IsValid = 0.

C_User Methods

Method	UID	Description
AddUserBegin [ ]	7777 0003 CC00 0001 h	Begin procedure to add a user
AddUserEnd [ ]	7777 0003 CC00 0002 h	End procedure to add a user and connect the added user
ConnectBegin [ ]	7777 0003 CC00 0003 h	Begin procedure to connect a user
ConnectEnd [ ]	7777 0003 CC00 0004 h	End procedure to connect a user and connect an authenticated user
Authenticate [ ]	7777 0003 CC00 0005 h	Combine an external factor when adding or connecting a user
SetUser [ ]	7777 0003 CC00 0006 h	Modify a user
EraseUser [ ]	7777 0003 CC00 0007 h	Invalidate a user
Disconnect [ ]	7777 0003 CC00 0008 h	Disconnect a user

TPer State Associated with C_User

The TPer is required to maintain three state variables that are associated with adding a row to C_User and authenticating a user. They are defined in the table below and they are exposed in more detail in Section 5, Entity Authentication.

State Variable	Type	Comment
user	uid	C_User row that is being authenticated
factor_count	uinteger{1}	number of factors that have authenticated
DK_accumulator	bytes{32}	holds incremental result of combining authentication factors

C_UserUID.AddUserBegin [ ]

Parameters	Type	Comment
PassCode	bytes{128}	user PIN, password, or pass phrase
Row	uid	C_User row to set
IsKingpin	uinteger{1}	=1 and user is a member of Kingpin Authority
UserName	bytes{64}	owned and managed by Host
Nfactors	uinteger{1}	number of authentication factors required for user
AppIsEncrypted	uinteger{1}	=0 and Application field is cleartext or =1 and Application field is stored encrypted
AppType	uinteger{2}	=0 and Application = 0 or ≠0 and Application field is stored; applications shall register AppType
Application	uinteger{32}	Application specific field as determined by AppType

=>[Result : boolean]

- UID of AddUserBegin[ ] = 7777 0003 CC00 0001h
- *Description*: begin procedure to add a new user with the IHost authentication factor; see Section 5.4, Procedure to Add User
- *Precondition*: *Row*.IsValid < 2
- *Invariant*: Row = 7777 0003 0001 0000h (initial user is being created) and Row.IsKingpin = 1; TPer ignores IsKingpin parameter

- *Invariant*: Row > 7777 0003 0001 0000h (initial user exists) and only a member of the Kingpin class, C_User[DiscInfo.CurrentUser].IsKingpin = 1, shall have authority to invoke this method
- *Postcondition*: { TRUE = AddUserBegin[ ] and authentication state is initialized, user = *Row*, factor_count = 1, DK_accumulator = DeriveKey(*PassCode*) } or { FALSE = AddUserBegin[ ] and authentication state is reset, user = 0, factor_count = 0, DK_accumulator = 0 }

C_UserUID.AddUserEnd [void]

=>[Result : boolean]

- UID of AddUserEnd[ ] = 7777 0003 CC00 0002h
- *Description*: ends procedure to enroll a new user; See Section 5.4, Procedure to Add User
- *Precondition*: AddUserBegin[ ] has been invoked, factor_count ≥ 1
- *Postcondition*: { TRUE = AddUserEnd[ ] and the given row becomes active and DiscInfo.DiscKey is decrypted with the PSAkey } or { FALSE = AddUserEnd[ ] and C_User is unchanged }
- *Postcondition*: authentication state is reset, user = 0, factor_count = 0, DK_accumulator = 0

C_UserUID.ConnectBegin [ ]

Parameter	Type	Comment
PassCode	bytes{512}	pass code provided by IHost
Row	uid	C_User row to authenticate

=>[Result : boolean]

- UID of Factor = 7777 0003 CC00 0003h
- *Description*: begin procedure to authenticate user with the IHost authentication factor; see Section 5.3, Procedure to Authenticate User
- *Precondition*: *Row*.IsValid = 2
- *Postcondition*: authentication state, Figure 2, user = *Row*, factor_count = 1, DK_accumulator = DeriveKey(*PassCode*) is initialized

C_UserUID.ConnectEnd [void]

=>[Result : boolean]

- UID of ConnectEnd = 7777 0003 CC00 0004h
- *Description*: begin procedure to authenticate user with the IHost authentication factor; see Section 5.3, Procedure to Authenticate User
- *Postcondition*: (result = TRUE and the given row becomes active and DiscInfo.DiscKey is decrypted with the PSAkey) or (result = FALSE)
- *Postcondition*: authentication state, Figure 2, is reset, user = 0, factor_count = 0, DK_accumulator = 0

C_UserUID.Authenticate [ ]

Parameter	Type	Comment
Reserved	bytes{8}	authority reference in SA Core[15]
PassCode	bytes{32}	pass code provided by external authentication factor

=>[Result : boolean]

UID of Authenticate[ ] = 0000 0006 0000 000C h

- *Description*: external authentication factor provides credential
- *Precondition*: AddUserBegin[ ] or ConnectBegin[ ] has been invoked
- *Postcondition*: PassCode is accumulated; see Section 5.3, Procedure to Authenticate User and Section 5.4, Procedure to Add User

C_UserUID.Get [ ]

Parameter	Type	Comment
Cellblock	cell_block	Row = C_User.User startColumn = User endColumn = Area50

=>[Result : boolean]

Response	Type	Comment
User	uid	unique ID of row
IsVaid	uinteger{1}	=0 and this row is uninitialized; =1 and this row is erased; =2 and this row is valid
IsKingpin	uinteger{1}	=1 and user is a member of Kingpin Authority
UserName	bytes{64}	owned and managed by Host
Nfactors	uinteger{1}	number of authentication factors required for user
AppIsEncrypted	uinteger{1}	=0 and Application field is cleartext or =1 and Application field is stored encrypted
AppType	uinteger{2}	=0 and Application = 0 or ≠0 and Application field is stored; applications shall register AppType
Application	uinteger{32}	Application specific field as determined by AppType

- UID of Get[ ] = 0000 0006 0000 0006h
- *Precondition*: *Cellblock* shall request exactly one C_User row
- *Precondition*: Cellblock shall request all non-hidden columns in a C_User row, cell_block.startColumn = User and cell_block.endColumn = Area51

C_UserUID.SetUser [ ]

Parameters	Type	Comment
PassCode	bytes{512}	user PIN, password, or pass phrase
Row	uid	row to set
UserName	bytes{64}	owned and managed by Host
IsKingpin	uinteger{1}	=1 and user is a member of Kingpin Authority
Nfactors	uinteger{1}	number of authentication factors required for user
AppIsEncrypted	uinteger{1}	=0 and Application field is cleartext or =1 and Application field is stored encrypted
AppType	uinteger{2}	=0 and Application = 0 or ≠0 and Application field is stored; applications shall register AppType; see “Appendix B. Trusted Optical Disc Authority”
Application	uinteger{32}	Application specific field as determined by AppType

=>[Result : boolean]

- UID of SetUser[ ] = 7777 0003 CC00 0006h
- *Description*: modify a C_User row
- *Precondition*: Row.IsValid = 2

- *Invariant*: after the initial user has been created, only a member of the Kingpin class shall have authority to invoke this method on an arbitrary row and arbitrary field.
- *Invariant*: Users who are not Kingpin members shall have privilege to change only their own row; however, the user shall only be able to change their Passcode and UserName.

C_UserUID.EraseUser [void]

Parameter	Type	Comment
Row	uid	user, represented by a C_User row, to invalidate

=>[Result : boolean]

- UID of EraseUser [ ]= 7777 0003 CC00 0007h
- *Description*: invalidates a user
- *Precondition*: Row > 7777 0003 0001 0000h; initial user cannot be erased
- *Invariant*: only a member of the Kingpin class shall have authority to invoke this method

C_UserUID.Disconnect [void]

=>[Result : boolean] = 1

- UID of Disconnect = 7777 0003 CC00 0008h
- *Description*: disconnects a user
- *Postcondition*: DiscInfo.CurrentUser = 0

4.2.1.5 ISO9660 Table (Byte Table)

ISO9660 is a byte table that contains a clear text ISO9660 volume that announces a TCG disc.

4.3 SA Core Access Control

4.3.1 Authorities

4.3.1.1 Host Software Exchange Authority

The host software authority is used by all IHost software; its purpose is to authenticate and create a secure channel. Only IHost software applications which have been issued a certificate shall successfully authenticate with the Optical SP. The host software authority shall establish an implicitly secure channel using the Exchange Authority as specified in SA Core 5.3.5.1.7.

Column	Type	Value	R/W	Comment
UID	uid	00 00 00 09 77 78 00 01	R	Constant
Name	name	"Trusted Optical Disc Software"	R	Well-known-name for the authority.
CommonName	name	"Host"	R	
IsClass	boolean	FALSE	R	Not a class authority.
Class	Authority_Ref	NULL	R	Not applicable
Enabled	Enabled	TRUE	R	Default enabled
Secure	messaging_type	17	R	AES_CBC_128
HashAndSign	hash_protocol	0	R	None.
PresentCertificate	boolean	TRUE	R	The host software is required to present a certificate in StartSession to authenticate itself.
Operation	auth_method	2	R	"Exchange" authentication.
Credential	cred_object_uidref	00 00 00 16 77 78 00 01	R	Certificate authority used to validate the certificates passed by the host in StartSession. See section 6.2.1.
ResponseSign	Authority_Ref	NULL	R	Not used
ResponseExch	Authority_Ref	00 00 00 09 77 78 00 02	R	Optical SP Exchange Authority (section 4.3.1.2)
ClockStart	Date	NULL	R	Not Applicable
ClockEnd	Date	NULL	R	Not Applicable
Limit	uint_4_def_0	00 00 00 00	R	No Limit
Uses	uint_4_def_0	00 00 00 00	R	Not applicable.
Log	log_select	00	R	None
LogTo	ref_def_00	NULL	R	Null reference

4.3.1.2 Optical SP Exchange Authority

The Optical SP exchange authority is used by the Optical SP as its Exchange Authority for the purposes of creating a secure channel between the Optical SP and the host.

Column	Type	Value	R/W	Comment
UID	uid	00 00 00 09 77 78 00 02	R	Constant
Name	name	"Optical SP Exchange Authority"	R	Well-known-name for the authority.
CommonName	name	"SP"	R	
IsClass	boolean	FALSE	R	Not a class authority.
Class	Authority_Ref	NULL	R	Not applicable
Enabled	Enabled	TRUE	R	Default enabled
Secure	messaging_type	17	R	AES_CBC_128
HashAndSign	hash_protocol	0	R	None.
PresentCertificate	boolean	TRUE	R	The Optical SP is required to present a certificate in SyncSession to authenticate itself.
Operation	auth_method	2	R	"Exchange" authentication.
Credential	cred_object_uidref	00 00 00 16 77 78 00 01	R	Certificate authority used to validate the certificates passed to the host in SyncSession. See section 6.2.1.

ResponseSign	Authority_Ref	NULL	R	Not used
ResponseExch	Authority_Ref	NULL	R	Not used
ClockStart	Date	NULL	R	Not Applicable
ClockEnd	Date	NULL	R	Not Applicable
Limit	uint_4_def_0	00 00 00 00	R	No Limit
Uses	uint_4_def_0	00 00 00 00	R	Not applicable.
Log	log_select	00	R	None
LogTo	ref_def_00	NULL	R	Null reference

4.3.1.3 Certificate Authority Credential

The certificate authority credential is a static value as defined in the C_EC_163 table.

Column	Type	Value	R/W	Comment
UID	uid	00 00 00 16 77 78 00 01	R	Constant.
Name	name (02 0C)	"Trusted Optical CA"	R	Well-known-name for the certificate authority.
CommonName	name (02 0C)	""	R	
k1	uinteger{1}		R	See SWG Table 64 for the values.
k2	uinteger{1}		R	
k3	uinteger{1}		R	
r	uinteger{21}		R	
a	uinteger{1}		R	
b	uinteger{21}		R	
x	uinteger{21}		R	
y	uinteger{21}		R	
alpha	uinteger{21}	NULL	R	CA Private key – not stored in SP.
u	uinteger{21}	Public Key	R	CA Public key – x coordinate
v	uinteger{21}	Public Key	R	CA Public key – y coordinate
Hash	hash_protocol	0	R	None
ChainLimit	uinteger{1}	0	R	No certificate chaining.
Certificate	Cerfiicates_ref	NULL	R	No certificate chaining.

4.3.1.4 Optical SP Public Key Credential

The certificate authority credential is a static value as defined in the C_EC_163 table.

Column	Type	Value	R/W	Comment
UID	uid	00 00 00 16 77 78 00 02	R	Constant.
Name	name (02 0C)	"Optical SP Public Key"	R	Well-known-name for the optical SP public key.
CommonName	name (02 0C)	""	R	
k1	uinteger{1}		R	See SWG Table 64 for the values.
k2	uinteger{1}		R	
k3	uinteger{1}		R	
r	uinteger{21}		R	
a	uinteger{1}		R	
b	uinteger{21}		R	
x	uinteger{21}		R	
y	uinteger{21}		R	
alpha	uinteger{21}	NULL	R	Optical SP Private key – hidden.
u	uinteger{21}	Public Key	R	Optical SP Public key – x coordinate
v	uinteger{21}	Public Key	R	Optical SP Public key – y coordinate
Hash	hash_protocol	0	R	None
ChainLimit	uinteger{1}	0	R	No certificate chaining.
Certificate	Cerfiicates_ref		R	Reference to the Optical SP's certificate.

4.3.1.5 Optical SP Certificates Table

The Certificates table has exactly one row which stores the reference to the Optical SP's certificate byte table.

Column	Type	Value	R/W	Comment
UID	uid	00 00 00 0A 77 78 00 01	R	Constant.
Name	name	"Optical SP Certificate"	R	Well-known-name for the optical SP certificate.
CommonName	name	""	R	
CertData	byte_table_ref	77 78 00 01 77 77 00 01	R	UID for the byte table with the Optical SP certificate.
CertSize	uinteger_4	xx xx xx xx	R	Size of the certificate in bytes.

4.3.1.6 Optical SP Certificate Byte Table

This byte table stores the actual bytes of the Optical SP's certificate as referenced by the Certificates table. This byte table has UID : 7778 0001 7777 0001h.

Column	Type	Value	R/W	Comment
<unnamed>	uinteger_1*	TBD	R	Raw byte storage for the Optical SP certificate.

4.3.2 Access Control Element (ACE) Table

The access control elements provide the basis for constructing access control lists (ACL's). One ACE is defined which indicates Host software is authenticated.

4.3.2.1 Host Software (Host)

The Host access control element allows the host to create/delete rows in the C_User table.

Column	Type	Value	R/W	Comment
UID	uid	00 00 00 08 77 78 00 01	R	Constant
Name	name	"Host"	R	
CommonName	name	"ACE"	R	
BooleanExpr	AC_element	Host Software Exchange Authority	R	Host software authority is authenticated.
RowStart	row_selection	0	R	First Row
RowEnd	row_selection	0	R	Last Row
ColStart	name	0	R	First Column
ColEnd	name	0	R	Last Column

4.3.3 Access Control Lists (ACL's)

4.3.3.1 Admin SP

Table	Get Method
Properties	Anybody
Serial Number Contents	Anybody
SP	Anybody
TperInfo	Anybody
SPInfo	Anybody
Disc	Anybody

4.3.3.2 Optical SP

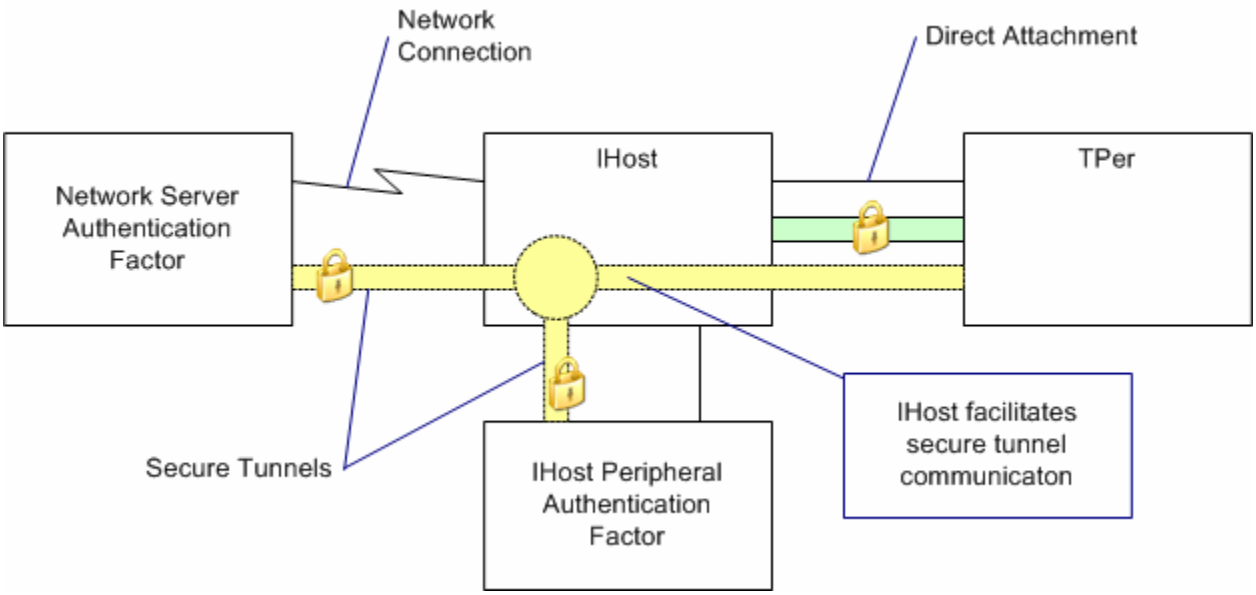
Table	Get Method	Set Method	ConnectEnd, AddUserBegin, EraseUser, Disconnect
ACE	Anybody	Nobody	not applicable
Authority	Anybody	Nobody	not applicable
SPInfo	Anybody	Nobody	not applicable
C_EC_163	Anybody	Nobody	not applicable
Anchor	Anybody	Nobody	not applicable
DiscInfo	Host	Host	not applicable
DriveInfo	Host	Host	not applicable
C_User	Anybody	Nobody	Host
ISO9660	Host	Host	not applicable

5 Entity Authentication

5.1 TPer Initiating Host

A TPer is directly attached to exactly one MMC initiator, known as IHost. IHost is responsible for managing user authentication with the TPer and facilitating communication between external authentication factors and the TPer. The set of authentication factors includes IHost applications (users and IHost software), IHost peripherals (tokens and storage devices), and network servers. IHost applications use the secure channel established by the IHost authority; other authentication factors establish their own secure tunnel directly with the TPer. IHost facilitates communication, but message semantics are known only to the endpoints. IHost application authentication shall always occur and shall always occur first, but the number of factors is determined by an IHost application. Furthermore, each user can have a different set of factors and a different set order.

Figure 1 Authentication Logical Communication Paths



5.2 Authentication Factors

An IHost authentication factor is a user or IHost application and is an entity that can:

- Use the secure channel established with the IHost authority
- Execute ConnectBegin[ ] on the Optical SP

An external authentication factor is an entity that can:

- Establish a secure tunnel to a TPer, with communication facilitated by IHost
- Execute Authenticate[ ] on the Optical SP
- Manage a list of users and their associated pass codes

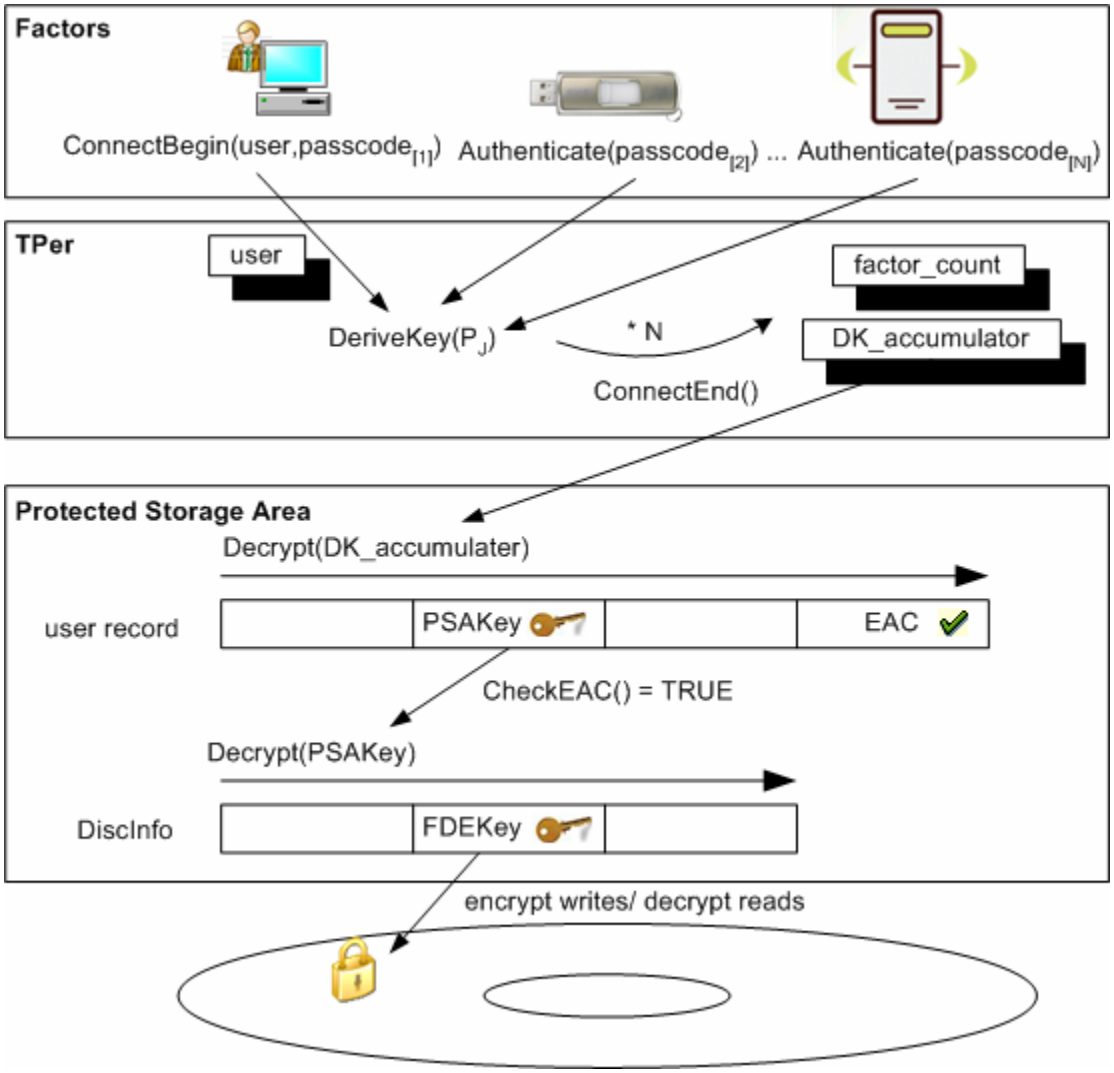
5.3 Procedure to Authenticate User

Let N be the number of factors that are required for authentication, and let $F_{[J]}$ represent an authentication factor with a pass code, $P_{[J]}$, where J = 1 to N. The following procedure is required:

1. IHost establishes a secure channel to the TPer with StartSession[ ] and StartSecureSession[ ]. IHost iterates C_User to select a user to authenticate and to determine the number of authentication factors, N, that is required. IHost is responsible for determining which factors are required.
2. IHost invokes ConnectBegin[ ] on the TPer.
3. The TPer executes ConnectBegin[*row*, $P_{[1]}$] by setting local variables
   - factor_count to 1
   - user to *row*
   - DK_accumulator to the result of applying DeriveKey() to $P_{[1]}$. DK_accumulator stores the accumulated results of the $F_{[J]}$ factors
4. IHost requests $F_{[J]}$ to perform a remote connection.
5. $F_{[J]}$ establishes a secure tunnel to the TPer using StartSession[ ] and StartSecureSession[ ].
6. $F_{[J]}$ invokes Authenticate($P_{[J]}$) on the TPer.
7. The TPer executes Authenticate($P_{[J]}$) by applying DeriveKey() to $P_{[J]}$ and combining the result in DK_accumulator.
8. $F_{[J]}$ returns the results to IHost, including the result of Authenticate[ ].
9. *IHost repeats steps 4-8 for each authentication factor $F_{[J]}$.*
10. IHost application establishes a secure channel with the TPer using StartSession[ ] and StartSecureSession[ ]; IHost invokes ConnectEnd[ ] on the TPer.
11. The TPer executes ConnectEnd[ ] by using DK_accumulator to decrypt the ciphertext fields of the C_User record. CheckEAC() is then applied to the decrypted C_User record. If CheckEAC() fails, then the user has not been validated and the result of ConnectEnd[ ] is FALSE. If CheckEAC() succeeds, then the result of ConnectEnd[ ] is TRUE and all fields in the decrypted C_User record are available. The TPer uses the PSAKey to decrypt the DiscInfo table and the FDEKey to encrypt/decrypt user data.

The procedure is illustrated in the following figure.

Figure 2 User Authentication N-factor Procedure



5.4 Procedure to Add User

Adding a user with N authentication factors is similar to authenticating a user with N factors: Let N be the number of factors that are required for authentication, and let $F_{[J]}$ represent an authentication factor with pass code $P_{[J]}$, where J = 1 to N.

1. IHost establishes a secure channel to the TPer with StartSession[ ] and StartSecureSession[ ]. IHost iterates C_User to an erased or uninitialized user record.
2. IHost invokes AddUserBegin[ ] on the TPer.
3. The TPer executes AddUserBegin[$P_{[1]}$, *row*, …] by:
   - copying method parameters to the user record *row*
   - setting DK_accumulator to the result of applying DeriveKey() to $P_{[1]}$. DK_accumulator stores the accumulated results of the $F_{[J]}$ factors
   - setting local variable factor_count to 1
4. IHost requests $F_{[J]}$ to perform a remote connection.
5. $F_{[J]}$ establishes a secure tunnel to the TPer with StartSession[ ] and StartSecureSession[ ].
6. $F_{[J]}$ invokes Authenticate($P_{[J]}$) on the TPer.
7. The TPer executes Authenticate[$P_{[J]}$] by applying DeriveKey() to $P_{[J]}$. The result is combined in DK_accumulator, and factor_count is incremented.
8. $F_{[J]}$ returns the results to IHost, including the result of Authenticate[ ].
9. *IHost repeats steps 4-8 for each authentication factor*.
10. IHost establishes a secure channel to the TPer with StartSession[ ] and StartSecureSession[ ]; IHost invokes AddUserEnd[ ] on the TPer.
11. The TPer executes AddUserEnd[ ] by applying MakeEAC(), setting the EAC field, and encrypting the row using DK_accumulator as the encryption key. The result from AddUserEnd[ ] indicates the result of this procedure.

6 Use Scenarios (Informative)

6.1 Discover the Optical SP

The following precondition is required to proceed:

- Host uses the well-known-UID (0x777) for the Optical SSC.

A host obtains the UID of the Optical SP with the Get[ ] method on the Admin SP Table. This activity requires establishing a non-secure, read-only session with the Admin SP. This scenario is based upon SA Core, Section 5.3.7.1.1. It is included because it is the simplest SWG example; it is not required because the Optical SP is '00 00 02 05 77 77 00 01', well-known by convention.

6.1.1 Start Session: Anybody Authority

SPUID.StartSession [ ]

Parameters	Type	Value	Comment
Host session number	uinteger{4}	aa aa aa aa	Assigned by host
SP to connect	SP_ref	00 00 02 05 00 00 00 01	UID of the Admin SP
Write permission	boolean	0	0 = read-only session

=> SPUID.SyncSession [ ]

Parameters	Type	Value	Comment
Host session number	uinteger{4}	aa aa aa aa	Assigned by host
TPer session number	uinteger{4}	ss ss ss ss	Assigned by TPer

The following postcondition is true:

- Host has obtained session number

6.1.2 Get Optical SP

The following precondition is required to proceed:

- Host has obtained session number

SP.Get [ ]

Parameter	Type	Value	Comment
Cell to get	cell_block	00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 02 "UID" "UID"	Start Row End Row Start Column End Column

=>

Parameter	Type	Value	Comment
UID	uid	00 00 02 05 77 77 00 01	Optical SP

6.2 Authentication of the Client Application

Client application software shall authenticate and establish a secure channel before performing secure TPer activities. Only applications that have been issued a certificate shall successfully complete authentication. The Exchange method in the SA Core, section 5.3.5.1.7, shall be used.

The following precondition is required to proceed:

- Host uses the well-known UID (0x0777) for the Optical SSC.

6.2.1 Start Session

SMUID.StartSession [ ]

Parameters	Type	Value	Comment
Host session number	uinteger{4}	aa aa aa aa	Assigned by host.
SP to connect	SP_ref	00 00 02 05 77 78 00 01	UID of the Optical SP.
Write	Boolean	0	=0 for read-only session; =1 for write/read session.
HostChallenge	challenge	NULL	Not used.
HostExchangeAuthority	Authority_ref	00 00 00 09 77 78 00 01	Software Exchange Authority referenced in the authority table. The authority's credential is used to validate the HostExcchangeCert. (See section 4.3.1.1)
HostExchangeCert	certificate		Host certificate that contains the host public key for the secure session key exchange. This certificate is validated by the HostExchangeAuthority.
HostSigningAuthority	Authority_ref	00 00 00 00 00 00 00 00	Not used..
HostSigningCert	certificate	00 00 00 00 00 00 00 00	Not used.
SessionTimeout	uinteger{4}	00 00 00 00	No timeouts used in this method.
SignedHash	signed_hash	00	No hash.

Upon receipt, the Optical SP performs the following actions:

1) Looks up the authority referenced in HostExchangeAuthority.
2) Validates the authenticity of the certificate in HostExchangeCert against a certificate authority's public key.

=> ThisSP.SyncSession [ ]

Parameters	Type	Value	Comment
Host session number	uinteger{4}	aa aa aa aa	Assigned by host
TPer session number	uinteger{4}	ss ss ss ss	Assigned by TPer
SPChallenge	challenge	NULL	Not used
SPExchangeCert	certificate		SP certificate which holds the SP's public key. This must be validated by a certificate authority's public key (held by the host). The public key in this certificate is the SP public key for use as the SP Exchange Authority public key.
SPSigningCert	certificate	NULL	Not used.
SignedHash	signed_hash	NULL	Not used.

The following postcondition is true:

- Host has obtained session number

Upon receipt, the host performs the following actions:

1) Validates the authenticity of the SPExchangeCert using a certificate authority's public key.
2) Generates a host session key.

3) Encrypts the host session key with the Optical SP public key and returns as HostEncryptSessionKey in StartTrustedSession.

6.2.2 StartTrustedSession

ThisSP.StartTrustedSession [ ]

Parameters	Type	Value	Comment
Host session number	uinteger{4}	aa aa aa aa	Assigned by Host.
TPer session number	uinteger{4}	ss ss ss ss	Assigned by TPer
HostResponse	response	NULL	Not used
HostEncryptSessionKey	session_key_encrypt	Encrypted Host Session Key	Generated by host as : Encrypt (Host Session Key, Optical SP public key)
HostIntegritySessionKey	session_key_integrity	NULL	Not used.
SignedHash	signed_hash	NUL	Not used.

Upon receipt of StartTrustedSession, the Optical SP:

1) Decrypts HostEncryptSessionKey using the Optical SP private key to recover the Host Session Key. Stores the host session key securely into internal RAM.
2) Generates SPSessionKey (random number) and stores it securely into internal RAM.
3) Encrypts the SPSessionKey with the host's public key and returns this value as SPEncryptedSessionKey in SyncTrustedSession.

=> ThisSP.SyncTrustedSession [ ]

Parameters	Type	Value	Comment
Host session number	uinteger{4}	aa aa aa aa	Assigned by host.
TPer session number	uinteger{4}	ss ss ss ss	Assigned by TPer
SPResponse	response	NULL	Not used.
SPEncryptSessionKey	session_key_encrypt	Encrypted Host Session Key	Generated by host as : Encrypt (SP Session Key, Host public key)
SPIntegritySessionKey	session_key_integrity	NULL	Not used.
SignedHash	signed_hash	NULL	Not used.

The host, upon receipt of SyncTrustedSession:

1) Decrypts SPEncryptSessionKey using the host's private key to recover the SP Session Key. Stores the SP session key securely.

The session is now considered open, implicitly authenticated and secure. All subsequent communications between the host and SP occurs via secure messaging packets.

6.3 Disc Insertion Procedure

Upon insertion of a disc, the TPer determines if an Anchor table exists on the disc.

If an Anchor table is present, then the drive:

1) Marks the TCG feature current.
2) Prepares a TCG media arrival event.

3) Waits for the Connection Procedure (see Section 6.5).

If an Anchor table is not present, then the TPer waits for the Disc Initialization Procedure (see Section 6.6), or if there is no request for disc initialization, the drive and the disc behave as normal optical storage.

6.4 Iterate C_User

The following precondition is required:

- Client application authentication with the Optical SP (see Section 6.2).

C_UserUID.Get [ ]

Parameters	Type	Value	Comment
Row to read	cell_block	7777 0003 0001 00ii 7777 0003 0001 00ii	iterator: Start Row; invariant: one row per Get iterator: End Row; invariant: one row per Get

=>

Column	Type	Value	Comment
Row	uid	7777 0003 0001 00ii	UID of row
UserName	bytes{64}	"humpty dumpty"	owned by host
IsKingpin	uinteger{1}	1	=1 and member of Kingpin authority
IsValid	uinteger{1}	1	=0 and not initialized; =1 and erased; =2 and valid
Nfactors	uinteger{1}	1	number of authentication factors required for user
AppIsEncrypted	uinteger{1}	0	=0 and Application field is not encrypted or =1 and Application field is stored encrypted
AppType	uinteger{2}	0	not in use; registered type of Application field
Application	bytes{32}	0	application specific field as determined by AppType

For each successful Get[ ], the host applies the appropriate criteria to continue or discontinue iteration. For example, if IsValid = 2, then the host may attempt connection. If IsValid < 2, the host may add a user in this row. IsValid = 0 is a sentinel that is used to terminate iteration.

6.5 Connection Procedure (1-Factor)

The following preconditions are required:

- Client application has authenticated with the Optical SP (see Section 6.2).
- Host has iterated C_User and selected the desired row (see Section 6.4).

This scenario uses DiskInfo.CryptoType = AES-128; the host executes the C_User.ConnectBegin method, which requires IHost authority and uses secure messaging.

C_UserUID.ConnectBegin [ ]

Parameter	Type	Value	Comment
UID	uid	7777 0003 0001 0000	Row selected by C_User iteration
PassCode	bytes{512}	"put together again"	Actual PIN, password, or pass phrase

Upon receipt of this request, the TPer:

1) Derives a key from "put together again" (*PassCode*), decrypts row 1 (*UID*), and performs CheckEAC().
2) If CheckEAC() fails, =>[Result : boolean] = FALSE; [method status] = NOT_AUTHORIZED.

3) If CheckEAC() validates, uses C_User.PSAkey to decrypt DiscInfo.DiscKey.
4) If DiscInfo.DriveHasAES = 1, enables drive encryption.
5) Sets DiscInfo.CurrentUser = 1 (RowNumber).
6) The drive:
    a. Marks the TCG feature current.
    b. Prepares a media removal event.
    c. After the media removal event has been emitted, prepares a media arrival event.

=>[Result : boolean] = 1

C_UserUID.ConnectEnd [ ]
=>[Result : boolean] = 1

The following postconditions are true:

- DiscInfo.CurrentUser is valid
- Encryption engine has DiscKey.
- Host has been notified of a disc arrival

6.6 Disc Initialization Procedure

The following preconditions are required to proceed:

- Client application has authenticated with the Optical SP (see Section 6.2).
- Protected storage area does not exist

The host performs the following activities to initialize a disc. Each numbered item shall be executed as a single transaction. These transactions use secure messaging.

1) Initialize DiscInfo (See Section 6.6.1)
2) Add the Kingpin user (see Section 6.6.2).
3) Authenticate the new Kingpin password (see Section 6.5).

6.6.1 Initialize DiscInfo

The host sets the one and only DiscInfo. This method requires IHost authority and uses secure messaging. This example instructs the TPer to use 128-bit encryption key.

DiscInfoUID.Set [ ]

Parameters	Type	Value	Comment
Cells to write	cell_block	00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 01	Start Row End Row
PSAsize	uinteger{4}	2080	size in sectors of protected storage area
ISO9660size	uinteger{4}	32	size in sectors of default ISO9660 clear text volume
CryptoType	uinteger{1}	1	Use AES-128
AppIsEncrypted	uinteger{1}	0	=0 and Application field is not stored encrypted or =1 and Application field is stored encrypted
AppType	uinteger{2}	0	=0 and not in use; registered type of Application field

Application	uinteger{32}	0	Application specific field as determined by AppType

Upon receipt of this request the TPer:

1) Validates that the DiscInfo table has not been written previously; return status = NOT_AUTHORIZED on failure.
2) Encrypts the DiscKey with the PSAkey and stores it securely within its internal memory.

=>[Result : boolean] = 1

6.6.2 Add Initial User (1-Factor)

The host invokes the AddUserBegin [ ] method. This method requires IHost authority and uses secure messaging.

C_UserUID.AddUserBegin [ ]

Parameters	Type	Value	Comment
PassCode	bytes{512}	"all the king's horses"	Proof of authority
UID	uid	7777 0003 0001 0000	row to set
UserName	bytes{64}	"Root User"	used by host for selection
IsKingpin	uinteger{1}	1	=1 and user is a member of Kingpin Authority
Nfactors	uinteger{1}	1	number of authentication factors required for user
AppIsEncrypted	uinteger{1}	0	=0 and Application field is not stored encrypted or =1 and Application field is stored encrypted
AppType	uinteger{2}	0	=0 and not in use; registered type of Application field
Application	uinteger{32}	0	Application specific field as determined by AppType

Upon receipt of this request, the TPer:

1) Writes method parameters (*Username, IsKingpin, Nfactors, AppType, Application*) to row 0 (*UID*).
2) Calculates a derived key, DK, from "all the king's horses" (*PassCode*).
3) Generates a PSAkey, encrypts it with DK and writes the result to PSAkey of row 0 (*UID*).
4) Generates an FDEkey, encrypts it with PSAKey, and writes the result to DiscInfo.FDEkey.
5) Calculates MakeEAC() and writes it to the EAC column of row .
6) Writes a value 2 to the IsValid column of row 0 (*UID*).

=>[Result : boolean] = 1

C_UserUID.AddUserEnd [ ]
=>[Result : boolean] = 1

The following postcondition is true:

- Row 0 holds a valid user of class Kingpin.
- DiscInfo.CurrentUser = Row 0 (7777 0003 0001 0000)

6.7 Add a Subsequent User (1-Factor)

The following preconditions shall be required to proceed:

- Client application authentication with the Optical SP (see Section 6.2).
- Host has iterated C_User and selected the desired row (see Section 6.4)

- DiscInfo.CurrentUser is member of Kingpin class or RowNumber = DiscInfo.CurrentUser

The host invokes the AddUserBegin [ ] method. This method requires Host authority and uses secure messaging.

C_UserUID.AddUserBegin [ ]

Parameters	Type	Value	Comment
PassCode	bytes{512}	"put together again"	Proof of authority
UID	uid	7777 0003 0001 0001	Row number to set
UserName	bytes{64}	"humpty dumpty"	Used by host for selection
IsKingpin	uinteger{1}	1	=1 and user is a member of Kingpin Authority
Nfactors	uinteger{1}	1	number of authentication factors required for user
AppType	uinteger{2}	0	Registered type of Application field
Application	uinteger{32}	0	Application specific field as determined by AppType

Upon receipt of this request, the TPer:

1) Writes UserName *(UserName*), IsKingpin in row 1 (*UID*).
2) Calculates a derived key, DK, from "put together again" (*PassCode*).
3) Encrypts PSAkey with DK and writes the result to PSAkey of row 1 (*UID*)
4) Calculates MakeEAC() and writes it to the EAC column of row 1.
5) Writes a value 2 to the IsValid column of row 1 (*UID*).

=>[Result : boolean] = 1

C_UserUID.AddUserEnd [ ]
=>[Result : boolean] = 1

The following postcondition is true:

- Row 1 holds a valid user.
- DiscInfo.CurrentUser = Row 1 (7777 0003 0001 0001)

6.8 Remove a User

The following preconditions shall be required:

- Client application authentication with the Optical SP (see Section 6.2).
- Host has iterated C_User and selected the desired row (see Section 6.4
- DiscInfo.CurrentUser is member of Kingpin class

C_UserUID.EraseUser [ ]

Parameters	Type	Value	Comment
UID	uid	7777 0003 0001 0001	Row to erase

Upon receipt of this request, the TPer:

1) Writes 0 in IsValid column of row 1 (UID)

=>[Result : boolean] = 1

The following postcondition is true:

- Row 1 does not hold a valid user, and the row is available for reuse.

7 References

1 ECMA-130, Data Interchange on read only 120 mm optical discs (CD-ROM), 2nd Edition, 1996-06

2 ECMA-267, 120 mm DVD – Read-Only Disk, 3rd Edition, 2001-04

3 ECMA-337, Data Interchange on 120 mm and 80 mm Optical Disk using +RW Format, 3rd Edition, 2005-12

4 ECMA-338, Data Interchange on 120 mm and 80 mm DVD Re-recordable (DVD-RW), 2002-12

5 ECMA-349, Data Interchange on 120 mm and 80 mm Optical Disk using +R Format, 3rd Edition, 2005-12

6 ECMA-359, Data Interchange on 120 mm and 80 mm DVD Recordable (DVD-R), Format, 2004-12

7 National Institute of Standards and Technology (NIST), Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38A, December 2001

8 “Orange Book”, System Description Recordable Compact Disc Systems, part II: CD-R Volume 1 (1x,2x,4x), 1998-12

9 “Orange Book”, System Description Recordable Compact Disc Systems, part II: CD-R Volume 2: Multi-Speed (16x-48x), 2002-04

10 “Orange Book”, System Description Recordable Compact Disc Systems, part III: Volume 1 (1x,2x,4x) CD-RW, 1998-08

11 “Orange Book”, System Description Recordable Compact Disc Systems, part III: Volume 2 High-Speed (4x-10x) CD-RW, 2001-06

12 “Orange Book”, System Description Recordable Compact Disc Systems, part III: Volume 3 Ultra-Speed (8x-32x) CD-RW , 2003-07

13 OMG, Object Constraint Language, Version 2.0, May 2006.

14 T10 Multi-Media Commands – 6 (MMC-6), Revision 0, 2006-11-14

15 TCG Storage Architecture Core Specification Version 1.0, Revision 0.9 – draft, 2006-11-28

Appendix A: MMC References

MMC-6[15] includes essential information that is required to implement an TPer as defined by the Optical SSC.

Table 13. MMC References

Topic	Reference	Description

Appendix B. Trusted Optical Disc Authority

The “Trusted Optical Disc Authority” licenses cryptographic parameters and algorithms, copyrighted items, and intellectual property to ensure media interchange and the ability to execute enforcement actions against circumvention tools and software. The cryptographic algorithms deployed in the Optical SSC are public and fully disclosed. Certain input parameters to cryptographic algorithms are licensed, copyrighted, and shall be treated as highly confidential as described in the license agreement. The parameters and algorithms licensed by the Trusted Optical Disc Authority include:

1) TPer Certificates
2) Host Certificates
3) Initialization Vector (IV) for on-disc user data encryption.
4) Constants for DeriveKey(), MakeEAC(), and CheckEAC()
5) Registration of Host Defined fields

Providing and offering to the public a technology, product, service, device, component, or part thereof that is primarily designed, produced, or marketed for the purpose of circumventing the technological protection measures afforded by the “Trusted Optical Disc Authority” constitutes a violation of the anti-circumvention provisions of the Digital Millennium Copyright Act (the "DMCA"), 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1). Any other such offering that is primarily designed or produced to circumvent protection measures, or which has only limited commercial significant purpose other than to circumvent, or which are offered to the public with knowledge that it is for use in circumventing, violates the rights of “Trusted Optical Disc Authority” and any others harmed as well. See §§ 1201(a)(2), 1201(b)(1), and 1203.

Appendix C. SA Core Tables

Table 14 Admin SP tables referenced from SA Core

Table	Template	Section	Comment
MethodID	Base	SWG 5.3.3.6	
Method	Base	SWG 5.3.3.7	
SPInfo	Base	SWG 5.3.3.1	
SP	Admin	SWG 5.4.2.6	
TPerInfo	Admin	SWG 5.4.2.1	

Tables that are included in the Admin template and the Base template of the SA Core, but are not listed in Table 14 are optional and shall be reported as NOT_AUTHORIZED when they are not present on the TPer.

SPInfo Table (Admin SP)

This table contains information that the Admin SP publishes about itself.

Row Number	UID	SPID	Name	Size	Size In Use	SP Session Timeout	Enabled
1	77 77 77 01 77 00 00 00	00 00 02 05 00 00 00 01	Admin			0	true

SP Table (Admin SP)

This table publishes information about the Security Providers on the TPer. The Admin SP and the Optical SP are created at manufacturing time.

UID	Name	ORG	Effective Auth	Date Of Issue	Bytes	Life Cycle State	Frozen
00 00 02 05 00 00 00 01	Admin					0	false
00 00 02 05 77 77 00 01	Optical					0	false

Table 15 Optical SP tables referenced from SA Core

Table	Template	Section	Comment
ACE	Base	SWG 5.3.3.8	Formed by TPer and not on disc
Authority	Base	SWG 5.3.3.9	Formed by TPer and not on disc
C_EC_163	Base	SWG 5.3.3.23	Formed by TPer and not on disc
MethodID	Base	SWG 5.3.3.6	Formed by TPer and not on disc
Method	Base	SWG 5.3.3.7	Formed by TPer and not on disc
SPInfo	Base	SWG 5.3.3.1	Formed by TPer and not on disc

Tables included in the Base template of the SA Core, but are not listed in, are optional and shall be reported as NOT_AUTHORIZED when they are not present on the TPer.

SPInfo Table (Optical SP)

This table contains information about the Optical SP.

Row Number	UID	SPID	Name	Size	Size In Use	SP Session Timeout	Enabled
1	77 77 77 01 00 00 00 00	00 00 02 05 77 77 00 01	Optical				true

Appendix D: Document Management

- 2007-09-20, OSSCR, version 0.4, Hines
  - Permissions
  - PSA construction reference
- 2007-09-20, OSSCR, version 0.3, Hines
  - added Anchor table invariants
  - added SA Core tables
  - added ISO9660 cleartext volume table
  - added anchor table sequence
  - changed n-factor bracket functions
- 2007-08-08, OSSCR, version 0.2, Hines
  - moved material to MMC proposal
  - moved RBAC to Host Defined
  - All tables synched with MMC
  - Anchor table improvement
  - DiscInfo improvement
  - C_User improvement
  - N-factor
- 2007-06-28, version 0.4, Hines
  - removed comments
- 2007-06-14, version 0.3, Hines
  - added improvements from Jason Cox
  - moved definitions to Section 1.2
  - assigned default values and provided invariants to on-disc tables
  - Authorities section improved
  - Added Compact Disc and DVD- references
- 2007-06-05, version 0.2, Hines, Lee, Gurkowski, McFerrin
  - initial external release

Contact: OSSCR@dataplay.com

Issues List

- version r0.3
  - Properties table
  - Failed state
  - Personalization
  - PSA construction
  - pass thru 2X
- Drive session closing, rather than host (mechanical disc removal, reset)
- Review Checklist:
  - Editorial
  - SWG compliance
  - MMC conformance
  - Security
  - System
  - Completeness
  - Repetition