VCPS

Multi-Media Command Set (MMC) Enabling the Video Copy Protection System for the DVD+R/+RW Video Recording Format

DRAFT

Version 1.00A

November 16, 2004

PHILIPS

hp invent

Royal Philips Electronics
Intellectual Properties & Standards
Business Support
Building WAH
PO Box 220
5600 AE Eindhoven
The Netherlands

Fax: +31 - 40 - 27 32113
Internet: http://www.licensing.philips.com/
E-mail: info.licensing@philips.com

Contents

Tables

Figures

This page is intentionally blank

1 Introduction

The Video Copy Protection System (VCPS) for the DVD+R/+RW Video Recording Format defines a method to prevent unauthorized copying and/or redistribution of video data that is recorded in the DVD+R/+RW video recording format. In general, the formatting does not modify the LBA space of supported Discs and formats.

The MMC-4 command set is used as the starting point for enabling VCPS since it has been defined to operate over many different physical interfaces. This document only defines the command set, but excludes certain data structure details available only to licensees.

This document is created to match the structure of MMC-4:

1. Scope – This section
2. References – A list of documents that may be needed by the reader for the correct understanding of this document.
3. Definitions, Symbols, Abbreviations, and Conventions – A glossary of terminology in this document
4. Multi-Media Device Models – Modeling for the various media oriented behaviors that the Initiator may witness from the Logical Unit provides an overview of internal drive operation to the Application developer.
5. Commands for Multi-media Devices – Commands are described from the Initiator's point of view.
6. Mode Parameters for Multi-media Devices – Inputs required by the Logical Unit are not always a part of a command. Inputs associated with mode of operation are readable and sometimes writable.

This page is intentionally blank

2 References

[MMC-4] SCSI Multi-Media Commands – 4 (T10/1545D, Draft Revision 3a)

[SPC-2] SCSI Primary Command Set - 2 (SPC-2) (ANSI NCITS 351:2001)

[DVD+R] System Description DVD+R 4.7 Gbytes, Basic Format Specifications

[DVD+R DL] System Description DVD+R 8.5 Gbytes, Basic Format Specifications

[DVD+RW] System Description DVD+RW 4.7 Gbytes, Basic Format Specifications

[DVD+VR] System Description DVD+RW 4.7 Gbytes, Video Format Specifications

[DVD-ROM] DVD Specifications for Read-Only Disc, Part 1, Physical Specifications

[DVD-Video] DVD Specifications for Read-Only Disc, Part 3, Video Specifications.

[VCPS] System Description Video Copy Protection System for the DVD+R/+RW Video Recording Format

This page is intentionally blank

3 Definitions and Abbreviations

3.1 Definitions

3.1.1 ADIP (Address In Pre-groove)

The addressing method used on a blank Disc, either DVD+R or DVD+RW.

3.1.2 AES (Advanced Encryption Standard)

The block cipher that is used for encryption and decryption.

3.1.3 AKB (Application Key Block)

An EKB structure that is embedded in an Application for the purpose of authenticating with a Logical Unit.

3.1.4 Application

A software function or a hardware function that has the purpose of formatting or rendering Protected Video Recordings.

3.1.5 APS (Analog Protection System)

A method of embedding copy management information in an analog video signal.

3.1.6 Audio Pack

A data structure containing audible data. See [DVD-Video] and [DVD+VR].

3.1.7 Authorization Key

A cryptographic key that is carried by a leaf node of an EKB structure.

3.1.8 AV Pack

A Video Pack, an Audio Pack, a Sub-Picture Pack, or a User Defined Pack.

3.1.9 AV Sector

2048 Bytes of data according to the Protected Video Format.

3.1.10 BP (Byte Position)

The location of a byte in a sequence of bytes.

3.1.11 Buffer Zone 2

The last 512 sectors of the Lead-in on a DVD+R/+RW Disc.

3.1.12 Bus Key

A cryptographic key that is shared by an Application and a Logical Unit as a result of the Logical Unit to Application authentication protocol.

3.1.13 CBC (Cipher Block Chaining)

An encryption mode that is used for data exceeding the AES block size.

3.1.14 CCI (Copy Control Information)

A collection of status bits (such as APS, CGMS, and/or EPN) contained in video data that indicates if it is permitted to redistribute and/or make a copy of all or part of the video data.

3.1.15 CGMS (Copy Generation Management System)

A method of embedding copy management information in a digital video signal.

3.1.16 CDB (Command Descriptor Block)

A data structure that contains a SCSI Command.

3.1.17 Control Data Zone

Auxiliary information about the Disc, as defined in [DVD+RW], [DVD+R], and in [DVD+R DL].

3.1.18 Data Frame

The main data contained in a sector, extended with sector header data. See [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.19 Data Zone

An area on a DVD+R/+RW Disc that contains one or more Protected Video Recordings, and optionally other data. See [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.20 Device ID

A 40-bit binary string that identifies a Player or a Recorder.

3.1.21 Disc

A DVD+R/+RW Disc that indicates support for Protected Video Recordings. This indication is contained in the Physical Format Information.

3.1.22 Disc Key

A cryptographic key that is obtained from hashing the Root Key and the Unique ID. The Disc Key is used to protect the Unique Key.

3.1.23 DKB (Disc Key Block)

An EKB structure contained on a Disc, which authorizes Players and Recorders to record or render Protected Video Recordings.

3.1.24 ECC Block (Error Correction Code Block)

A sequence of 16 sectors for which an error correction mechanism is defined. See [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.25 EKB (Enabling Key Block)

A data structure that authorizes VCPS system components. See also AKB and DKB.

3.1.26 EPN (Encryption Plus Non-assertion)

A method of embedding redistribution control data in a broadcast digital video signal.

3.1.27 Extended Format Information

Format information pertaining to VCPS that is contained on a blank Disc. The Extended Format Information is contained in the AUX bytes of the ADIP words in the Data Zone and/or in the Initial Zone in the main data channel.

3.1.28 Initial Zone

The first part of the Lead-in on a DVD+RW Disc; the first part of the Inner Drive Area on a DVD+R Disc. See [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.29 Initialization Vector 1

A 128-bit licensed constant that is used in CBC-mode encryption and decryption of AV Packs.

3.1.30 Initialization Vector 2

A 128-bit licensed constant that is used in the Drive to Application authentication protocol.

3.1.31 Lead-in

An area on a DVD+R/+RW Disc that precedes the Data Zone. See [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.32 MAC (Message Authentication Code)

A cryptographic code that is used to detect message tampering.

3.1.33 Navigation Pack

A data structure containing presentation control information, data search information, and real-time data information. See also [DVD-Video].

3.1.34 Node Key

One of a set of secret cryptographic keys that is associated with a Device ID. A Node Key is associated with a bit position of the Device ID.

3.1.35 Physical Address

The address information in an ADIP word. See [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.36 Physical Format Information

Auxiliary information about the Disc contained in the ADIP, as defined in [DVD+RW], [DVD+R], and [DVD+R DL]. Auxiliary information about the Disc is also contained in the Control Data Zone, as defined in [DVD+RW], [DVD+R], and [DVD+R DL].

3.1.37 Physical Sector Number.

Bit 0 through 23 of the ID field of a Data Frame. See [DVD+RW], [DVD+R], and [DVD+R DL]

3.1.38 Player

A DVD+R/+RW video Playback function capable of rendering video stored according to the Protected Video Format. A Player may consist of a Logical Unit/Application combination.

3.1.39 Program Key

A cryptographic key that is used to compute the Sector Keys of a Protected Video Recording. Multiple Program Keys may be used within a single Protected Video Recording.

3.1.40 Protected Video Format

The data structures specified in [DVD-Video] plus [DVD+VRW] plus this System Description VCPS. Alternatively, the data structures specified in [DVD-Video] plus this System Description VCPS.

3.1.41 Protected Video Recording

A recording of moving pictures, which is structured according to the Protected Video Format.

3.1.42 Recorder

A DVD+R/+RW video recording function capable of storing video according to the Protected Video Format. A Recorder is also a Player. A Recorder may consist of a Logical Unit/Application combination.

3.1.43 Root Key

A cryptographic key, which is contained in an EKB structure in an encrypted form.

3.1.44 Sector Key

A cryptographic key that is used to encrypt the content of an individual sector that contains part of a Protected Video Recording.

3.1.45 Sub-picture Pack

A data structure containing still picture data. See also [DVD-Video].

3.1.46 Unique ID

A 40-bit binary string that identifies a Disc.

3.1.47 Unique Key

A cryptographic key that is used to protect the Program Key.

3.1.48 User Defined Pack

A data structure containing under defined data. See also [DVD+VR].

3.1.49 Video Pack

A data structure containing moving picture data. See also [DVD-Video].

3.1.50 VCPS

The Video Copy Protection System for the DVD+R/+RW Video Recording Format as described in [VCPS].

3.1.51 VCPS Capable

A DVD+R/+RW Disc is VCPS Capable if the Current bit in the VCPS Feature Descriptor (see 5, The VCPS Feature) is set to 1. A Logical Unit is VCPS Capable if it returns the VCPS Feature Descriptor in response to the appropriate GET CONFIGURATION command.

3.1.52 VOB (Video Object)

See [DVD-Video].

3.2 Abbreviations

ADIP	Address in pre-groove
AES	Advanced Encryption Standard
AKB	Application Key Block
APS	Analog Protection System
AV	Audio/Video
CCI	Copy Control Information
DKB	Drive Key Block
EKB	Enabling Key Block
IV1	Initialization Vector 1
IV2	Initialization Vector 2
KA	Authorization Key
KB	Bus Key
KD	Drive Key
KN	Node Key
KP	Program Key
KR	Root Key
KS	Sector Key
KU	Unique Key
VOB	Video Object

4 The VCPS Model

4.1 Overview

4.1.1 General

This is a general description of the Video Copy Protection System (VCPS). Consult [VCPS] for a detailed description.

VCPS defines a method for preventing unauthorized copying and/or redistribution of video data that is recorded in the DVD+R/+RW video recording format. For the purposes of VCPS, the DVD+R/+RW video recording format may either consist of the data structures specified in [DVD-Video] plus [DVD+VR], which are optimized for real-time recording on DVD+R/+RW media, or consist of the data structures specified in [DVD-Video], which are more suitable for off-line recording (e.g., through a large buffer on a hard disk).

In a computer environment, VCPS has three components: a software Application operating as or through the Initiator, a DVD+R/+RW Logical Unit acting as the Logical Unit, and a VCPS Capable Disc. Each component possesses a collection of secrets necessary for recording and rendering VCPS protected sectors.

The software Application collects Logical Unit and Disc secrets during an Authorization process, combining with its own secrets to determine the keys necessary to encrypt/decrypt protected sectors.

4.1.2 Playback

For the purposes of rendering video data, all decryption is performed by the software Application. Consequently, given sector X, the software Application is required to know the encryption status of sector X: encrypted or not. If X is encrypted, the software Application is required to possess the keys and other information necessary to render the clear text from X.

4.1.3 Recording

VCPS protected recording is possible only when the correct components are present:

1. A VCPS Capable Disc in a
2. VCPS Capable Logical Unit, and operating under control of a
3. VCPS licensed Application.

4.2 The Protection Mechanisms

4.2.1 Protection Components

VCPS has a number of components designed to protect both video data and the key generation secrets. The primary VCPS components as described in Table 1.

Table 1 – VCPS Primary Components

Component	Abbr	Description
Application Key Block	AKB	An EKB structure that is embedded in an Application for the purpose of authenticating with a Logical Unit.
Device ID	-	Each VCPS Capable Player, Recorder, and Logical Unit has a 40-bit Device ID.
Disc Key	KD	A cryptographic key that is obtained from hashing the Root Key and the Unique ID. The Disc Key is used to protect the Unique Key.
Disc Key Block	DKB	An EKB structure contained on a Disc that authorizes Recorders to record or render Protected Video Recordings and Players to render Protected Video Recordings.
Enabling Key Block	EKB	A data structure that authorizes VCPS system components. See also AKB and DKB.
Initialization Vector 1	IV1	This is a 128-bit licensed constant that is used in cipher block chaining mode encryption and decryption of AV Packs.
Initialization Vector 2	IV2	This is a 128-bit licensed constant that is used in the Logical Unit to Application authentication protocol.
Node Key	KN	One of a set of cryptographic keys that is associated with a Device ID. A Node Key is associated with a bit position of the Device ID.
Program Key	KP	A cryptographic key that is used to compute the Sector Keys of a Protected Video Recording. Multiple Program Keys may be used within a single Protected Video Recording.
Sector Key	KS	A cryptographic key that is used to encrypt the content of an individual sector that contains part of a Protected Video Recording.
Unique ID	-	Each VCPS Capable Recorder has the ability to generate a 40-bit ID for each mounted Disc.
Unique Key	KU	A cryptographic key that is used to protect the Program Key.

4.2.2 Authorization

If a Disc contains VCPS protected data, the Application and Logical Unit shall first authorize each other for access to VCPS protected sectors:

1. The Application shall request the Device ID of the Logical Unit.
2. The Application shall use the Logical Unit's Device ID to parse its embedded AKB to locate the appropriate Authorization Key. If no valid key is found, the Application shall abort the Authorization process.
3. If the Authorization process is permitted to continue, the Application shall send the Logical Unit an appropriately large random number, the Application's Authorization Key, and a search reference index.
4. The Logical Unit shall locate the Node Key that is associated with the search reference and combine it with the Application's Authorization Key to create the Logical Unit's Root Key. The Logical Unit shall generate an appropriately large random number and combine the Root Key, both random numbers, the Logical Unit's key contribution, and a licensed constant into a single structure. The Application should request this structure.

5. The Application shall deconstruct the structure into its components. If the deconstructed value of the Application's random number does not match the original value sent, the Application shall abort the authentication process.
6. If the Authorization process is permitted to continue, the Application shall generate its random key contribution. The Application shall create a structure that contains a combination of the Application's random key contribution, both random numbers, the Application's Root Key, and the deconstructed licensed constant. This structure is sent to the Logical Unit.
7. The Logical Unit shall deconstruct the received structure into its components. If the deconstructed value of the Logical Unit's random number does not match the original value sent, the Logical Unit shall abort the authentication process. If the Authorization process is permitted to continue, the Logical Unit shall calculate the Bus Key using the a hash with both key contributions.
8. The Application shall request the Logical Unit to return an encryption of the Bus Key, the Logical Unit's licensed constant, the DKB hash (from Disc ADIP), and the Unique ID. If the Logical Unit has read-only capability, the DKB hash field shall be all zeros.

4.3 Using VCPS

4.3.1 Disc Initialization - Read-only Devices

Read-only devices are capable of reading only Discs with at least one closed session. As a part of the spin-up initialization process, the read-only device should read the Physical Format Information from the Control Data Zone. The VCPS bit in the Physical Format Information identifies the Disc's VCPS capability.

If an Application starts the Authorization process and the Disc is VCPS Capable, the read-only device shall read Buffer Zone 2 in order to retrieve the DKB.

4.3.2 Disc Initialization - Recorder Devices

4.3.2.1 A Blank VCPS Disc

A blank VCPS Capable Disc has the DKB either pre-recorded in the Initial Zone or in the Data Zone ADIP. Both may be present on the Disc. If both are present, the Initial Zone copy is should be read since it is possible to read written data much faster than ADIP data.

The DKB may not be written into Buffer Zone 2 until an Authorization sequence has successfully concluded and the DKB has been requested. The writing of Buffer Zone 2 shall also be deferred until appropriate for the mounted medium:

- If the Disc is DVD+RW, writing the DKB may occur only after the format process has begun recording the Lead-in area.
- If the Disc is DVD+R, writing the DKB is deferred until the first session is closed.

Note: If it is necessary to retrieve the DKB from ADIP, it is preferred to collect the DKB into the Logical Unit's buffer memory beginning during the spin-up process and continuing as a low priority background function. Reading the DKB from ADIP may require as much as 30 seconds.

4.3.2.2 A Written VCPS Disc

A non-blank Disc that is VCPS Capable may already be initialized for VCPS operations.

If a non-blank Disc is DVD+R (either SL or DL) and the first session is closed, then the VCPS capability status of the Disc is already specified and is not possible to change.

If a non-blank Disc is DVD+R and the first session is not closed, it is still possible to initialize the Disc for VCPS operations.

If the non-blank Disc is DVD+RW and the Disc has not been initialized for VCPS operations, then initialization shall be performed as described in 4.3.2.1.

4.3.3 Playback

The Logical Unit has no involvement in decoding/decryption of VCPS protected sectors. During authentication the Application receives sufficient information to decrypt/decode VCPS protected

sectors. Consequently, once Authorization has been performed, the Logical Unit 's involvement in reading protected data is to simply execute READ commands as sent by the Application through the Initiator.

4.3.4 Recording

4.3.4.1 Initialization and Self Authorization

If an authorized Application requests the DKB, the Logical Unit shall ensure that Buffer Zone 2 contains a valid copy of the DKB. If necessary, the Logical Unit shall record Buffer Zone 2 with a copy from either the Data Zone ADIP or the Initial Zone.

The Logical Unit shall ensure that Buffer Zone 2 contains a valid Unique ID. If the Disc has no Unique ID (blank) it shall generate a non-zero 40-bit Unique ID using a random number generator. The Logical Unit shall store the generated Unique ID in all Data Frames in Buffer Zone 2 that contain the DKB.

4.3.4.2 Video Data Protection

During authentication, the Application receives sufficient information necessary to encrypt video data. Actual encryption is performed by the Application. Consequently, once Authorization has been performed, the Logical Unit 's involvement in recording protected data is to simply execute WRITE commands as sent by the Application through the Initiator.

5 The VCPS Feature

The VCPS feature specifies that the Logical Unit is capable of processing the data structures on a Disc that are specified in the System Description VCPS. The VCPS feature descriptor is shown in Table 2.

Table 2 – The VCPS Feature Descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Feature Code (0110h)							
1								(LSB)
2	Reserved			Version = 0000b			Persistent	Current
3	Additional Length = 04h							
4	Reserved							
5	Reserved							
6	Reserved							
7	Reserved							

The Feature Code shall be set to 0110h.

The Version field shall be set to 0h.

The Persistent bit shall be set to zero, indicating that this Feature may change its current status.

When the Current bit is set to zero this Feature is not currently active and certain Feature Dependent Data may not be valid. When the Current bit is set to one, a Disc is present and ready that is either formatted for VCPS or is capable of being formatted for VCPS. When the Current bit is set to one, the Feature Dependent Data is valid.

Bit 6 of byte 16 of the Physical Format Information found in the Control Data Zone (or the ADIP) of DVD+R/+RW is the VCPS bit. If the VCPS bit is set to one, then the Disc is VCPS Capable. Otherwise, the Disc is not VCPS Capable. shows the state of the Current for various Disc status.

Table 3 – Currency of the VCPS Feature

Currently Mounted Disc	Disc Format Status	VCPS bit	Current bit
DVD+RW	Blank,	0	0
	DVD+RW Basic format - format completed, or DVD+RW Basic format - background format in progress	1	1
DVD+R	Session 1 is not closed	0	0
		1	1
DVD+R	Session 1 is closed and Buffer Zone 2 contains no VCPS initialization data	0	0
		1	0
DVD+R	Session 1 is closed and Buffer Zone 2 contains VCPS initialization data	-	1
All other media	-	-	0

Note: Read-only devices are typically unable to decode ADIP. These devices should determine the VCPS bit status by reading the Physical Format Information in the Control Data Zone of the Disc.

The Additional Length field shall be set to 04h.

A Logical Unit reporting the VCPS Feature shall support the commands shown in Table 4.

Table 4 – Commands required by the Secure Channels Feature

Op Code	Command Name	Reference
A4h	REPORT KEY	6.1
A3h	SEND KEY	6.2

6 Commands

The commands that have unique behavior defined when the VCPS Feature is current are listed in Table 5.

Table 5 – Commands for the VCPS Feature

Command	Op Code	Reference
REPORT KEY	A4h	6.1
SEND KEY	A5h	6.2

6.1 REPORT KEY Command

6.1.1 General

The REPORT KEY command provides a general mechanism for transferring Authorization information from the Logical Unit to the Initiator. The general form of the command is shown in Table 6.

Table 6 – REPORT KEY Command Descriptor Block, General Form

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code (A4h)							
1	Reserved			Key Class Dependent Definition				
2	Key Class Dependent Definition							
3	Key Class Dependent Definition							
4	Key Class Dependent Definition							
5	Key Class Dependent Definition							
6	Key Class Dependent Definition							
7	Key Class							
8	Key Class Dependent Definition							
9	Key Class Dependent Definition							
10	Key Class Dependent Definition							
11	Control							

The Key Class field selects the security system and defines the meaning of Key Class Dependent parameters of the CDB. Valid values for Key Class are listed in Table 7.

Table 7 – Key Class Field

Key Class	Authentication Type
00h	DVD CSS/CPPM or CPRM
01h	ReWritable Security Service – A
02h - 1Fh	Reserved
20h	VCPS
21h - FFh	Reserved

Key Class = 00h is for authentication services for DVD Video (CSS, CPRM). For specific descriptions, please refer to [MMC-4].

Key Class = 20h is defined for secure functions unique to VCPS Logical Units.

6.1.2 The VCPS Key Class

6.1.2.1 The REPORT KEY CDB for the VCPS Key Class

Key Class = 20h is used for authentication services associated with the VCPS Feature. The CDB has the format shown in Table 8.

Table 8 – Report Key Command Descriptor Block, VCPS Form

Byte \ Bit	7	6	5	4	3	2	1	0
0	Operation Code (A4h)							
1	Reserved							
2	(MSB)							
3	Starting Offset							
4								
5								(LSB)
6	VCPS Function Code							
7	Key Class = VCPS (20h)							
8	(MSB)			Allocation Length				
9								(LSB)
10	Reserved							
11	Control							

The VCPS CDB form is identified when the Key Class field = 20h.

The Starting Offset field specifies the byte offset from which the information structure transfer shall begin. Typically, Starting Offset is zero, however, when the structure is larger than 65 535 bytes, the entire structure may be delivered during the execution of several REPORT KEY commands.

The Allocation Length field specifies the maximum length in bytes of REPORT KEY response data that shall be transferred from the Logical Unit to the Initiator. An Allocation Length of zero indicates that no data shall be transferred. This condition shall not be considered an error.

Data shall be returned in response to the request specified in the command. The general format of that returned data is shown in Table 9.

Table 9 – Report Key Returned Data Format

Byte \ Bit	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB)			Data Length = N				
3	(Number of bytes available following this field)							(LSB)
Additional Data								
0	Report Key Data							
...								
N-1								

The VCPS Function code specifies the VCPS function to be performed. VCPS Functions are listed in Table 10. If the VCPS Function code is a reserved value, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ values shall be set to ILLEGAL REQUEST/INVALID PARAMETER IN CDB.

Table 10 – VCPS Functions for REPORT KEY

VCPS Function Code	VCPS Function
00h	Reserved
01	DKB
02	Device ID
03	Key Contribution
04	DKB Hash & Unique ID
05	DKB Information
06 - FFh	Reserved

If CDB is validated, but the Disc is not VCPS Capable, the Logical Unit shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE.

6.1.2.2 VCPS Function Code = 01h, DKB

When the VCPS function is 01h, the REPORT KEY command shall return the DKB.

If the Logical Unit represents a read-only device, the DKB shall be returned from Buffer Zone 2.

If the Logical Unit represents a Recorder device, the command execution shall proceed as follows:

1. If the DKB is contained in Buffer Zone 2, the Logical Unit, the DKB structure shall be returned to the Initiator and the command shall be terminated with GOOD status.
2. If no DKB is found in Buffer Zone 2, but the DKB is contained in the Initial Zone, the Logical Unit shall generate a new Unique ID. The Logical Unit shall either write or schedule the write of the DKB and the Unique ID into Buffer Zone 2. If an unrecoverable error occurs during this process, the Logical Unit shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE. Otherwise, the Logical Unit shall return the DKB, and terminate with GOOD status.
3. If no DKB is found in either Buffer Zone 2 or the Initial Zone, the DKB is contained in the ADIP. The Logical Unit shall completely retrieve the DKB from the DKB region in the ADIP, the Logical Unit shall generate a new Unique ID. The Logical Unit shall either write or schedule the write of the DKB and the Unique ID in Buffer Zone 2. If an unrecoverable error occurs during this process, the Logical Unit shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE. Otherwise, the Logical Unit shall return the DKB, and terminate with GOOD status.
4. If a DKB is not found on the Disc, the Logical Unit shall terminate the command with CHECK CONDITION status. In addition the Logical Unit shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE.

The format of the returned data is defined in Table 11.

Table 11 – VCPS Key Class REPORT KEY returned data, DKB

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length							
3	(LSB)							
DKB data								
0	(MSB) DKB							
...								
L-1	(LSB)							
...	P Zero Padding bytes							
N-1								

The Data Length (= N) contains the length of the structure not including the Data Length field.

The DKB field contains the EKB structure.

If L is not a multiple of 4, then P = 1, 2 or 3 zero padding bytes shall be appended in order that N is an integral multiple of 4. Consequently, the structure data length is N = L+P.

6.1.2.3 VCPS Function Code = 02h, Device ID

When the VCPS function is 02h, the REPORT KEY command shall return Device ID_d of the Logical Unit. This assists the functionality of step 1 in the authentication protocol (see A.3). The Logical Unit shall return Device ID_d and terminate with GOOD status. If a previous execution of the authentication protocol is in progress, the Logical Unit shall abort that previous execution of the authentication protocol. The format of the returned data is defined in Table 12.

Table 12 – VCPS Key Class REPORT KEY returned data, Device ID

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length = 0024h							
3								(LSB)
Device ID data								
0	Reserved							
...								
30								
31	(MSB) Device ID							
...								
35								(LSB)

The Data Length field shall contain 36 (24h).

Each byte of the reserved field shall be set to zero (00h).

The Device ID field contains the Device ID of the VCPS Capable Logical Unit.

6.1.2.4 VCPS Function Code = 03h, Key Contribution

When the VCPS function is 03h, the REPORT KEY command shall return the key contribution QD of the Logical Unit. This assists the functionality of step 4 in the authentication protocol (see A.3). The command execution shall proceed as follows:

1. If the authentication sequence has been violated, the Logical Unit shall terminate the command with CHECK CONDITION status. In addition the Logical Unit shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR. A retry of the authentication protocol shall start from step 1.
2. Otherwise, the Logical Unit shall return its key contribution QD and terminate with GOOD status.

The format of the returned data is defined in Table 13.

Table 13 – VCPS Key Class REPORT KEY returned data, Key Contribution

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length = 0024h							
3	(LSB)							
Key Contribution data								
0	Reserved							
...								
3								
4	(MSB) Encrypted Random Numbers 1							
...								
19	(LSB)							
20	(MSB) Encrypted Logical Unit Key Contribution							
...								
35	(LSB)							

The Data Length field shall contain 36 (24h).

Each byte of the reserved field shall be set to zero (00h).

The Encrypted Random Numbers 1 field contains the random number (RA) of the Application, the random number (RD) of the Logical Unit combined with IV2 and encrypted using the Root Key KR_{auth}. IV2 is a 128-bit licensed constant.)

The Encrypted Logical Unit Key Contribution field contains the key contribution (QD) of the Logical Unit, encrypted using the Root Key KR_{auth} and combined with Encrypted Random numbers 1.

6.1.2.5 VCPS Function Code = 04h, DKB Hash and Unique ID

When the VCPS function is 04h, the REPORT KEY command shall return the DKB hash value and Unique ID. This assists the functionality of step 8 in the authentication protocol.

The command execution shall proceed as follows:

1. If the Logical Unit has aborted the authentication protocol in a previous step, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR. The Application may retry authntication beginning with step 1 (see A.3) of the authentication sequence.
2. Otherwise, the Logical Unit shall return the DKB Hash and Unique ID, and terminate with GOOD status. The format of the returned data is defined in Table 14.

Table 14 – VCPS Key Class REPORT KEY returned data, DKB Hash & Unique ID

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length = 0024h							
3								(LSB)
Key Contribution data								
0	Reserved							
...								
3								
4	(MSB) Encrypted DKB Hash							
...								
19								(LSB)
20	(MSB) Encrypted Unique ID							
...								
35								(LSB)

The Data Length field shall contain 36 (24h).

Each byte of the reserved field shall be set to zero (00h).

The Encrypted DKB Hash field contains the DKB Hash value combined with IV2, encrypted using the Bus Key KB. IV2 is a 128-bit licensed constant.

A Logical Unit that has playback-only functionality shall set the DKB Hash field to all zeros, prior to encryption. A Logical Unit that has recording functionality shall retrieve the DKB hash value from the hash region contained in the ADIP.

The Encrypted Unique ID field contains the Unique ID, encrypted using the Bus Key KB and combined with the encrypted DKB Hash.

If the mounted medium is read-only (i.e.without ADIP structures), the Logical Unit shall set the DKB Hash field to all zeros, prior to encryption.

6.1.2.6 VCPS Function Code = 05h, DKB Information

When the VCPS function is 05h, the REPORT KEY command shall return the information with respect to the DKB. The format of the returned data is shown in Table 15.

Table 15 – VCPS Key Class REPORT KEY returned data, DKB Hash & Unique ID

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length = 000Ch							
3								(LSB)
Key Contribution data								
0	DKB size							
...								
3								
4	DKB bytes collected							
...								
7								
8	Reserved					DKB_AD	DKB_IZ	DKB_BZ
9	Reserved							
...								
11								

The Data Length field shall be set to 12 (0Ch).

The DKB size field contains the size in bytes of the DKB.

The DKB bytes collected is the number of DKB bytes that the Logical Unit has collected so far. If the Logical Unit is required to retrieve the DKB from the DKB region in the ADIP, DKB Bytes Collected may be less than DKB Size. If the Logical Unit is able to retrieve the DKB from the Initial Zone, DKB Bytes Collected shall be equal to DKB Size. If the Logical Unit is able to retrieve the DKB from Buffer Zone 2, DKB Bytes Collected shall be equal to DKB Size.

The bit flags in byte 8 of the Key Contribution data specifies the DKB locations:

If DKB_AD = 1, the Disc contains a DKB in the DKB region in the ADIP, otherwise no DKB was found in the DKB region in the ADIP.

If DKB_IZ = 1, the Disc contains an DKB in the Initial Zone, otherwise no DKB was found in the Initial Zone.

If DKB_BZ = 1, the Disc contains a DKB in Buffer Zone 2, otherwise no DKB was found in Buffer Zone 2.

6.2 SEND KEY Command

6.2.1 General

The SEND KEY command provides a general mechanism for transferring Authorization information from the Initiator to the device. The general form of the command is shown in Table 16.

Table 16 – SEND KEY Command Descriptor Block, General Form

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code (A3h)							
1	Reserved			Key Class Dependent Definition				
2	Key Class Dependent Definition							
3	Key Class Dependent Definition							
4	Key Class Dependent Definition							
5	Key Class Dependent Definition							
6	Key Class Dependent Definition							
7	Key Class							
8	(MSB) Parameter List Length							
9	(LSB)							
10	Key Class Dependent Definition							
11	Control							

The Key Class field selects the security system and defines the meaning of Key Class Dependent parameters of the CDB. Valid values for Key Class are listed in Table 17.

The Parameter List Length field specifies the number of SEND KEY parameter bytes that shall be transferred from the Initiator to the Logical Unit.

Table 17 – Key Class Field

Key Class	Authentication Type
00h	DVD CSS/CPPM or CPRM
01h	ReWritable Security Service – A
02h - 1Fh	Reserved
20h	VCPS
21h - FFh	Reserved

Key Class = 00h is for authentication services for DVD Video (CSS, CPRM). For specific descriptions, please refer to [MMC-4].

Key Class = 20h is defined for secure functions unique to VCPS Logical Units.

6.2.2 The VCPS Key Class

6.2.2.1 The SEND KEY CDB for the VCPS Key Class

Key Class = 20h is used for authentication services associated with the VCPS Feature. The CDB has the format shown in Table 18.

Table 18 – SEND KEY Command Descriptor Block, VCPS Form

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code (A3h)							
1	Reserved							
2	Reserved							
3	Reserved							
4	Reserved							
5	Reserved							
6	VCPS Function							
7	Key Class = VCPS (20h)							
8	(MSB) Parameter List Length							
9	(LSB)							
10	Reserved							
11	Control							

The VCPS CDB form is identified when the Key Class field = 20h.

The VCPS Function code specifies the VCPS function to be performed. VCPS Functions are listed in Table 10. If the VCPS Function code is a reserved value, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ values shall be set to ILLEGAL REQUEST/INVALID PARAMETER IN CDB.

Table 19 – VCPS Functions for SEND KEY

VCPS Function Code	VCPS Function Code
00h	Reserved
01h	Authorization Key
02h	Key Contribution
03-FFh	Reserved

The Parameter List Length field contains the number of bytes that shall be transferred after the CDB has been received and decoded by the Logical Unit.

During command execution, the Initiator shall send parameter data to the Logical Unit. The general format of that parameter data is shown in Table 20.

Table 20 – Send Key Parameter List Format

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Send Key Data Length (N)							
3								(LSB)
Send Key Parameter Data								
0	Send Key Data							
1								
N-1								

6.2.2.2 VCPS Function Code = 01h, Authorization Key

When the VCPS function code is 01h, the SEND KEY command sends the Authorization Key K*A* of the Logical Unit. This function of the SEND KEY command provides the functionality of step 2 in the authentication protocol. The command execution shall proceed as follows:

1. If the authentication sequence has been violated, the Logical Unit shall terminate the command with CHECK CONDITION status. In addition the Logical Unit shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR. A retry of the authentication protocol shall start from step 1.
2. Otherwise, the Logical Unit shall accept the Authorization Key and terminate with GOOD status.

The format of the parameter data is defined in Table 21.

Table 21 – VCPS Key Class SEND KEY parameter list, Authorization Key

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length = 0020h							
3	(LSB)							
Authorization Key Information								
0	Reserved							
...								
6								
7	Node Key Number							
8	(MSB) Initiator's Random Number							
...								
15	(LSB)							
16	(MSB) Authorization Key KA_X							
...								
31	(LSB)							

The Reserved field shall contain 7 bytes, each set to 00h.

The Node Key Number field is the Node Key (KN_j) from the set of Node Keys (KN_d) that the Logical Unit shall use to obtain the Root Key (KR_{auth}) from the Authorization Key (KA_X). For this purpose, the Node Key Number field contains the bit position of the Device ID_D bit that the Application has last processed in the EKB search algorithm.

The Initiator's Random Number field contains a 64-bit random number.

The Authorization Key field contains KA_X that the Application has retrieved from the Application Key Block AKB that is built-in to the Application, based on the Device ID_D the Application has obtained from the Logical Unit.

6.2.2.3 VCPS Function Code = 02h, Key Contribution

When the VCPS function is 02h, the SEND KEY command sends the Bus Key contribution of the Application. This function of the SEND KEY command provides the functionality of steps 6 and 7 in the authentication protocol (see A.3). The command execution shall proceed as follows:

1. If the authentication sequence has been violated, the Logical Unit shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR. A retry of the authentication protocol shall start from step 1.
2. If the random number RD of the Logical Unit is not equal to the random number RD that the Logical Unit has sent to the Application in the previous REPORT KEY Contribution command, the Logical Unit shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE — AUTHENTICATION FAILURE. A retry of the authentication protocol shall start from step 1 (see A.3).
3. Otherwise, the Logical Unit shall accept the Application Bus Key contribution and terminate with GOOD status.

The format of the parameter data is defined in Table 22.

Table 22 – VCPS Key Class SEND KEY parameter list, Key Contribution

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							
2	(MSB) Data Length = 0024h							
3								(LSB)
Key Contribution data								
0	Reserved							
...								
3								
4	(MSB) Encrypted Random Numbers 2							
...								
19								(LSB)
20	(MSB) Encrypted Application Key Contribution							
...								
35								(LSB)

The Reserved field contains 4 bytes, each set to 00h.

The Encrypted Random Numbers 2 field contains the random number RD of the Logical Unit and the random number RA of the Application, encrypted using the Root Key KR_{auth}.

Encrypted Random Numbers 2 is determined by an encryption using KR_{auth}, IV2 , RD, and RA, where IV2 is a 128-bit licensed constant.

The Encrypted Application Key Contribution field contains the key contribution QA of the Application, encrypted using the Root Key KR_{auth} and combined with Encrypted Random numbers 2.

7 Mode Parameters

The VCPS Feature is able to become current (and useful) only for Logical Units that are able to report a current DVD+RW Profile, a current DVD+R Profile, or a Double Layer DVD+R Profile. Each of those profiles has a nonempty list of mandatory mode pages.

If the VCPS Feature is present and current, no additional mode pages are mandatory.

Annex A Using VCPS

A.1 Disc Recognition

If the Logical Unit has a Disc mounted and ready, the Initiator is able to recognize VCPS capability only by inspecting the feature list of the Logical Unit. If the VCPS Feature Descriptor is present and current, then it is possible to read/record VCPS Capable Discs.

A.2 Initializing a Disc for VCPS Operations

If it is possible to initialize a VCPS Capable Disc, then initialization occurs automatically once the DKB has been read. If it is necessary to retrieve the DKB from ADIP, it is preferred to collect the DKB into the Logical Unit's buffer memory beginning during the spin-up process and continuing as a low priority background function. Reading the DKB from ADIP may require as much as 30 seconds.

A.3 Authorization

A.3.1 Function Definitions

A.3.1.1 AESEncrypt

The AESEncrypt function is c = AESEncrypt(k, m), where k is a 128-bit key, and m is the 128-bit plain text block to be encrypted. The result, c, is a 128-bit cipher block.

A.3.1.2 AESCBCEncrypt

Cipher Block Chaining (CBC) mode encryption is a method of multiple plain text blocks [see VCPS]. CBC-mode encryption is denoted as c = AESCBCEncrypt(k, iv, m), where k is a 128-bit key, iv is a 128-bit initialization vector, and m is a sequence of two or more consecutive 128-bit plain text blocks m_i, i = 1..last. The result is a sequence c of consecutive cipher text blocks c_i, i = 1..last, which shall be calculated from the equations:

$c_0 = iv;$

$c_i = AESEncrypt(k, m_i \oplus c_{i-1})$, i = 1,..last.

A.3.1.3 AESDecrypt

The AESDecrypt function is m = AESDecrypt(k, c), where k is a 128-bit key, and c is the 128-bit cipher text block to be decrypted. The result is a 128-bit plain text block m.

A.3.1.4 AESCBCDecrypt

CBC-mode decryption is denoted as m = AESCBCDecrypt(k, iv, c), where k is a 128-bit key, iv is a 128-bit initialization vector, and c is a sequence of two or more consecutive 128-bit cipher text blocks c_i, i = 1..last. The result is a sequence m of consecutive plain text block m_i, i = 1..last, which shall be calculated from the equations:

$c_0 = iv;$

$m_i = AESDecrypt(k, c_i) \oplus c_{i-1}$, i = 1..last.

A.3.1.5 AESHash

The AESHash function is given by h = AESHash(m), where m is a sequence of 17 or more bytes. The sequence m shall be padded at the end by the shortest amount of zeros (bytes of value 0x00), such that m consists of two or more consecutive 128-bit blocks m_i, i = 0..last. The result is a single 128-bit value h, which shall be calculated from the equations:

$h_1 = AESEncrypt(m_0, m_1) \oplus m_1;$

$h_i = AESEncrypt(h_i - 1, m_i) \oplus m_i$, i = 2..last – 1;

$h = AESEncrypt(h_{last} - 1, m_{last}) \oplus m_{last}.$

All intermediate values h_i shall be discarded.

A.3.2 Authorization Sequence

The Authorization sequence is illustrated in Figure 1, Figure 2, and Figure 3, according to the following steps:

Step 1

The Application shall request the Logical Unit to return the Device ID_d. This is done by sending the REPORT KEY command for the VCPS Key Class requesting the Device ID function (see 6.1.2.3).

Step 2

The Application shall use Device ID_d to locate the Authorization Key KA_x for the Logical Unit in the built-in Application Key Block (AKB). If the Logical Unit is not authorized, the Application shall abort the authentication protocol.

Otherwise, the Application shall generate a 64-bit random number RA . The Application shall use the SEND KEY command requesting the Authorization Key function (see 6.2.2.2).

Step 3

The Logical Unit shall obtain KR_{auth} with the calculation: KR_{auth} = AESEncrypt(KN_j, KA_x). Here KN_j is the key in the set of Node Keys KN_d that is associated with bit position j of Device ID_d.

Step 4

The Logical Unit shall generate a 64-bit random number RD as well as a 128-bit random key contribution QD. The Application shall request the Logical Unit to return the following encrypted message:

(RA || RD || QD)KR_{auth} = AESCBCEncrypt(KR_{auth}, IV2, RA || RD || QD).

The initialization vector IV2 is a 128-bit licensed constant.

This is done by sending the REPORT KEY command for the VCPS Key Class requesting the Key Contribution function (03h).

Step 5

The Application shall decrypt the message received from the Logical Unit as follows:

RA || RD || QD = AESCBCDecrypt(KR_{auth}, IV2, (RA || RD || QD)KR_{auth}).

If RA is not identical to the value that the Application has sent to the Logical Unit in step 2, the Application shall abort the authentication protocol.

Otherwise, the Application shall continue with step 6.

Step 6

The Application shall generate a 128-bit random key contribution QA. The Application shall send the following message to the Logical Unit:

(RD || RA || QA)KR_{auth} = AESCBCEncrypt(KR_{auth}, IV2, RD || RA || QA).

The Application shall calculate the Bus Key KB as follows:

KB = AESHash(QD || QA).

This is done by sending the SEND KEY command for the VCPS Key Class requesting the Key Contribution function (02h).

Step 7

The Logical Unit shall encrypt the message received from the Application as follows:

RD || RA || QA = AESCBCDecrypt(KR_{auth}, IV2, (RD || RA || QA)KR_{auth}).

If RD is not identical to the value that the Logical Unit has sent to the Application in step 4, the Logical Unit shall abort the authentication protocol.

Otherwise, the Logical Unit shall calculate the Bus Key KB as follows:

KB = AESHash(QD || QA).

Step 8

The Application shall request the Logical Unit to return the following message:

(DKB Hash || Reserved || Unique ID)KB =

AESCBCEncrypt(KB, IV2, DKB Hash || Reserved || Unique ID).

To assemble this message, a Logical Unit that has playback-only functionality shall set the DKB Hash field to all zeros; a Logical Unit that has recording functionality shall read the DKB hash value from the hash region contained in the ADIP. The bit string Reserved consists of 88 bits that are set to '0'.

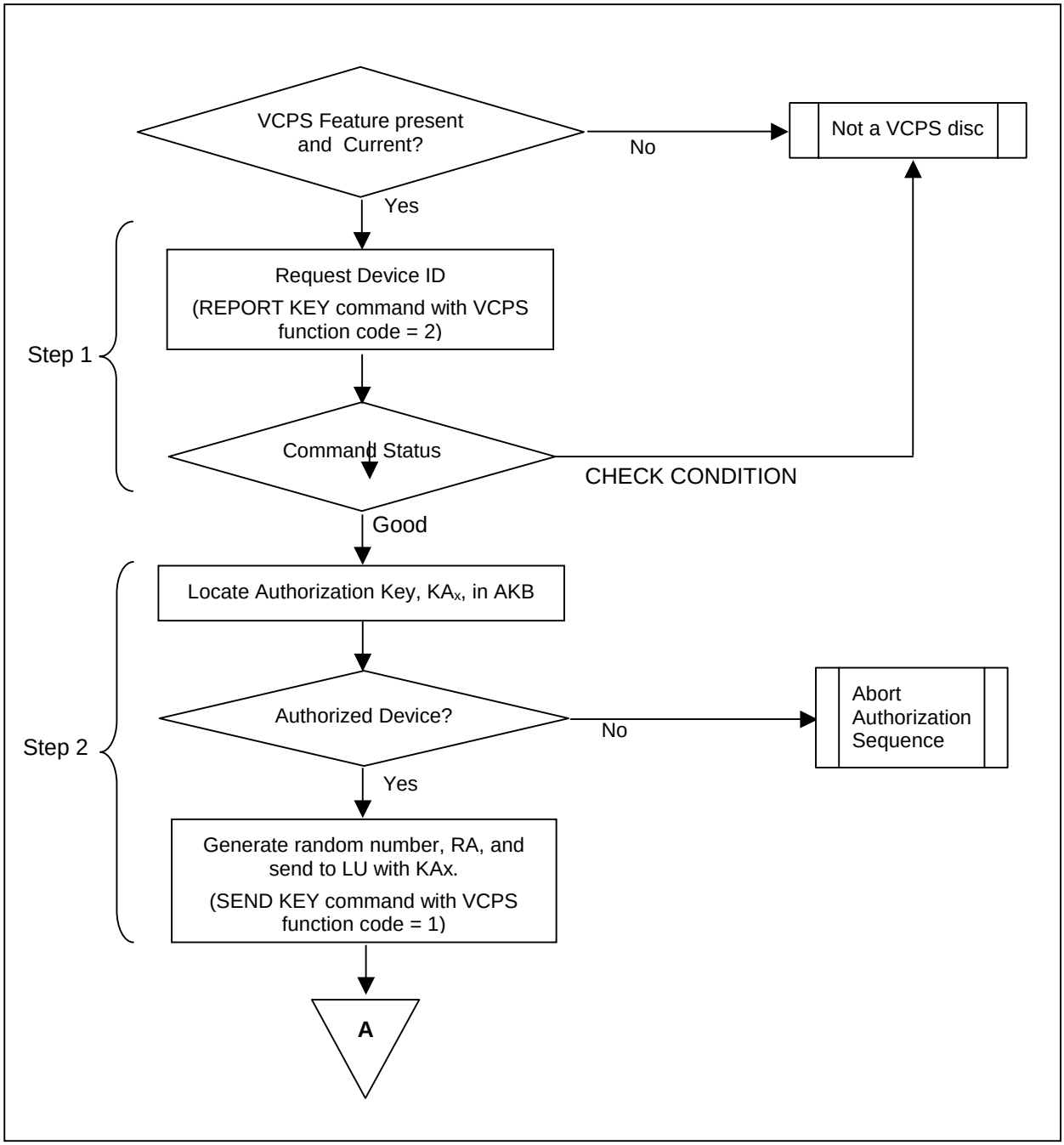

Figure 1 – Authorization Sequence, part 1

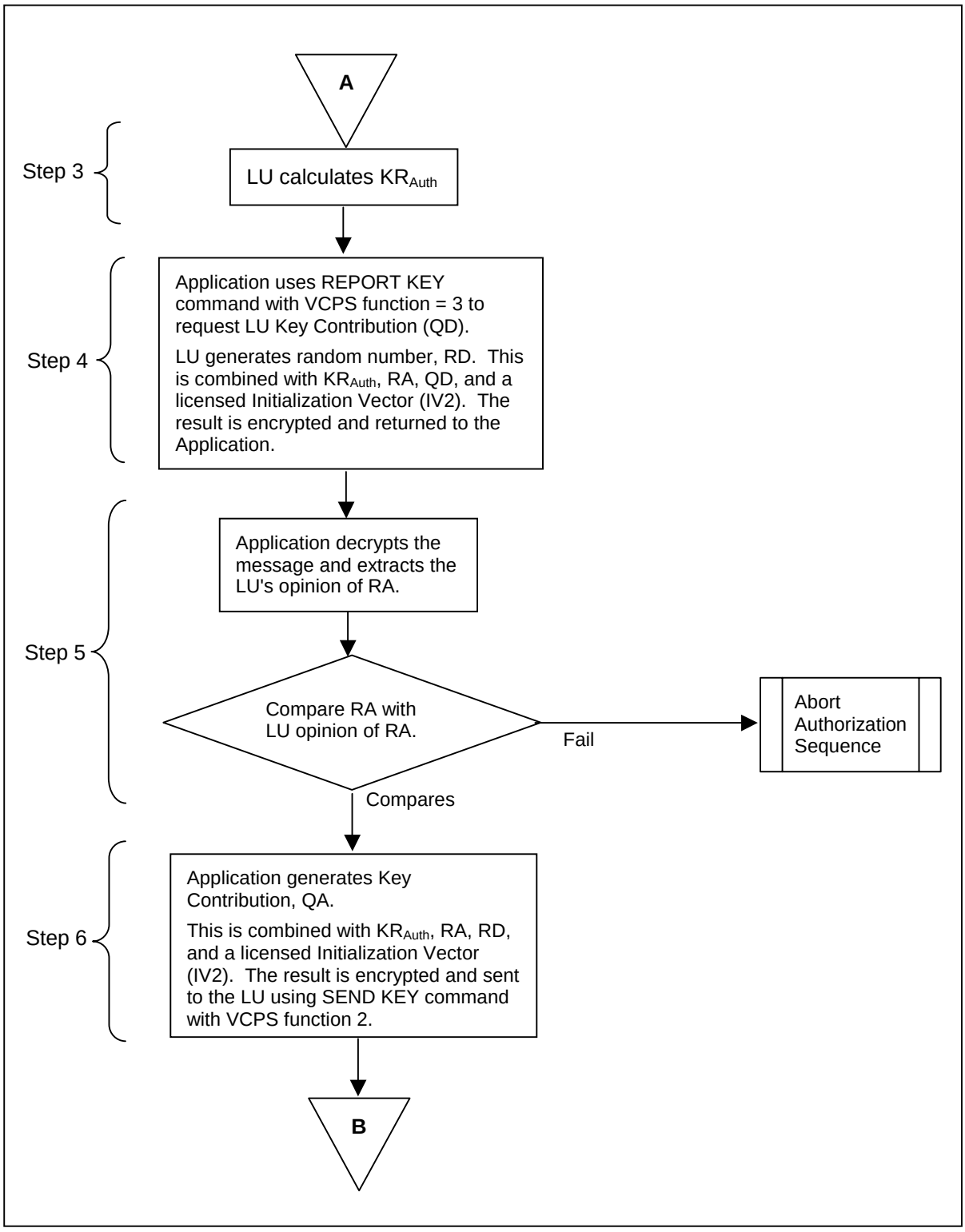

Figure 2 – Authorization Sequence, part 2

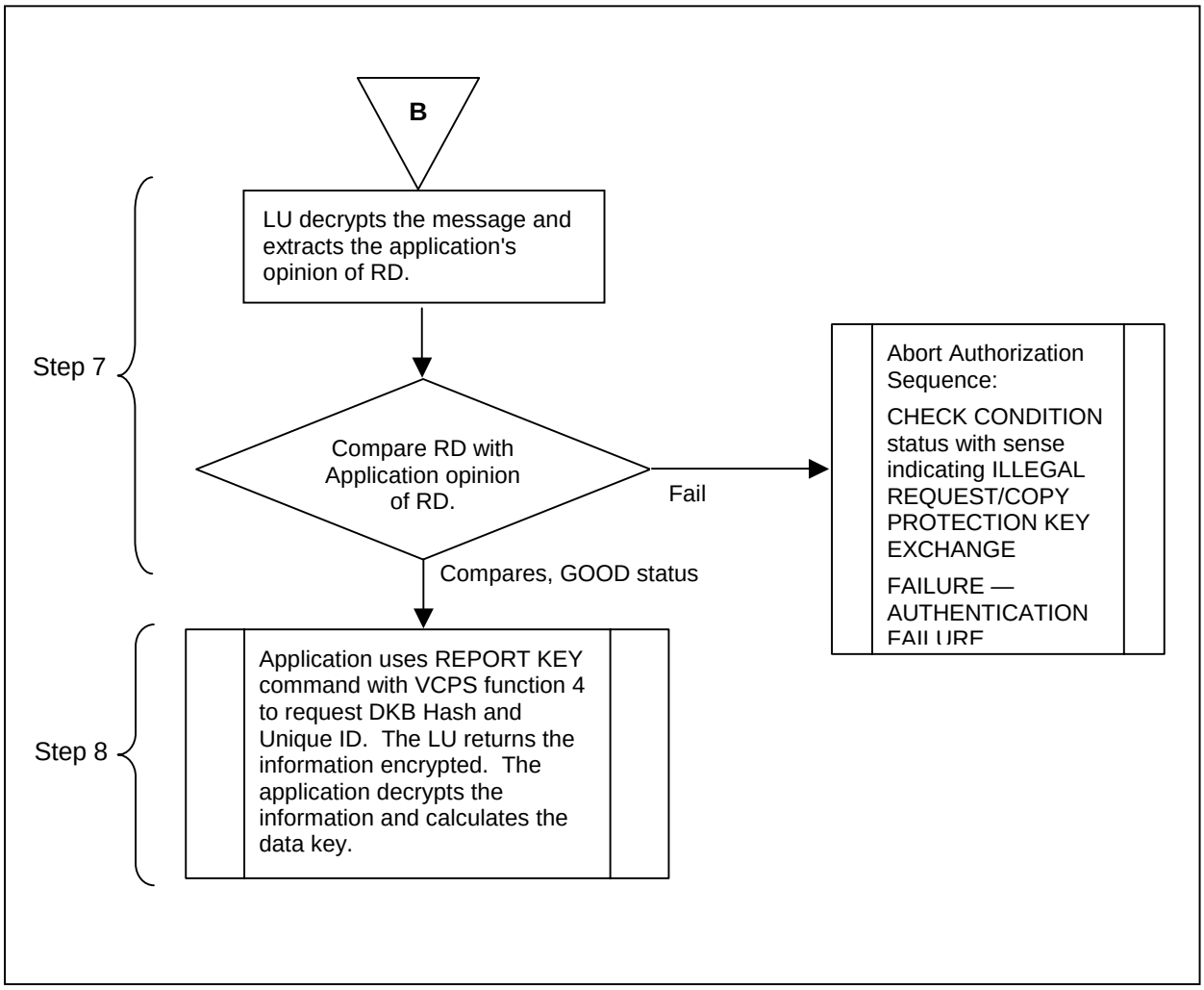

Figure 3 – Authorization Sequence, part 3

A.4 Reading a VCPS Disc

All decryption and decoding of VCPS protected data shall be performed by the Application. Consequently, once the Authorization process has completed, the Logical Unit has no further responsibility in the VCPS protection.

A.5 Recording a VCPS Disc

All encryption and encoding for VCPS protection shall be performed by the Application. Consequently, once the Authorization process has completed, the Logical Unit has no further responsibility in the VCPS protection.

This page is intentionally blank

