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

DRAFT

Version 1.03

September 25, 2005

PHILIPS

hp invent

COPYRIGHT

The *Multi-Media Command Set (MMC) Enabling the Video Content Protection System for the DVD+R/+RW Video Recording Format* is published by Royal Philips Electronics (Eindhoven, The Netherlands) and has been prepared in close co-operation with Hewlett-Packard Company (Palo Alto, California). All rights are reserved. Reproduction in whole or in part is prohibited without express and prior written permission of Royal Philips Electronics.

DISCLAIMER

The information contained herein is believed to be accurate as of the date of publication; however, neither Royal Philips Electronics nor Hewlett-Packard Company will be liable for any damages, including indirect or consequential, from use of the *Multi-Media Command Set (MMC) Enabling the Video Content Protection System for the DVD+R/+RW Video Recording Format* or reliance on the accuracy of this document.

LICENSING

Application of the *Multi-Media Command Set (MMC) Enabling the Video Content Protection System for the DVD+R/+RW Video Recording Format* in both Disc and equipment products requires a separate license from Philips.

CLASSIFICATION

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

NOTICE

For any further explanation of the contents of this document, or in case of any perceived inconsistency or ambiguity of interpretation, or for any information regarding the Video Content Protection System for the DVD+R/+RW Video Recording Format patent license program, please consult:

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

This page is intentionally blank

Contents

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

Tables

Figures

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

1 Introduction

The Video Content 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 Host may witness from the Drive provides an overview of internal drive operation to the Application developer.
5. Commands for Multi-media Devices – Commands are described from the Host's point of view.
6. Mode Parameters for Multi-media Devices – Inputs required by the Drive are not always a part of a command. Inputs associated with mode of operation are readable and sometimes writable.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

This page is intentionally blank

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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, Video Format Specifications
[DVD+VRR]	System Description DVD+R, 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 Content Protection System for the DVD+R/+RW Video Recording Format, Version 1.3

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

This page is intentionally blank

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

3 Definitions and Abbreviations

3.1 Definitions

3.1.1 ADIP (Address In Pre-groove)

The addressing method used on a blank DVD+R or DVD+RW disc.

3.1.2 AES (Advanced Encryption Standard)

AES is the block cipher that is used for encryption and decryption.

3.1.3 AKB (Application Key Block)

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

3.1.4 Application

An application is 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)

APS is a method of embedding copy management information in an analog video signal.

3.1.6 Audio Pack

An audio pack is a data structure containing audible data. See [DVD-Video] and [DVD+VR].

3.1.7 Authorization Key

An Authorization Key is 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

An AV Sector is 2 048 Bytes of data according to the Protected Video Format.

3.1.10 Buffer Zone 2

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

3.1.11 Bus Key

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

3.1.12 CBC (Cipher Block Chaining)

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

3.1.13 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.

3.1.14 CGMS (Copy Generation Management System)

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

3.1.15 Control Data Zone

The Control Data Zone contains auxiliary information about the Disc, as defined in [DVD+RW], [DVD+R], and in [DVD+R DL].

3.1.16 Data Frame

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

3.1.17 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].

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

3.1.18 Device ID

The Device ID a 40-bit binary string that identifies a Player or a Recorder.

3.1.19 Disc

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

3.1.20 Disc Key

A Disc Key is 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.

3.1.21 DKB (Disc Key Block)

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

3.1.22 Drive

A Logical Unit that operates as a single MM disc accessing unit. e.g. a BD-R Drive.

3.1.23 ECC Block (Error Correction Code Block)

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

3.1.24 EKB (Enabling Key Block)

An EKB is a data structure that authorizes VCPS system components. See also AKB and DKB.

3.1.25 EPN (Encryption Plus Non-assertion)

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

3.1.26 Extended Format Information

Extended Format Information is 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.

3.1.27 Host

A Host is a SCSI device with the characteristics of a primary computing device, typically a personal computer, workstation, minicomputer, mainframe computer, or auxiliary computing device or server. A Host includes one or more SCSI initiator devices.

3.1.28 Initial Zone

The Initial Zone is 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)

MAC is 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.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

3.1.35 Physical Address

The address information in an ADIP word is the physical address. 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 Drive/Application combination.

3.1.39 Program Key

A Program Key is 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+VR] plus optionally [DVD+VRR] 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 Protected Video Recording is 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 Drive/Application combination.

3.1.43 Root Key

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

3.1.44 Sector Key

A Sector Key is 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 Content Protection System for the DVD+R/+RW Video Recording Format as described in [VCPS].

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 Drive 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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

4 The VCPS Model

4.1 Overview

4.1.1 General

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, there are two forms of the DVD+R/+RW video recording format. The first form consists of the data structures specified in [DVD-Video] plus [DVD+VR] plus optionally [DVD+VRR], which are optimized for real-time recording on DVD+R/+RW media. The second form consists 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). Examples of video data that require the use of the VCPS copy protection features are the following:

1. Video data asserting that only one generation of copies is permitted. Such video data typically reaches a Recorder through a protected channel, such as DTCP (Digital Transmission Content Protection; for more information see http://www.dtcp.com).
2. Publicly broadcast television signals asserting that redistribution is not authorized.

Usage of the VCPS copy protection features requires special DVD+R/+RW discs. Such special discs are fully compatible with DVD+R/+RW players and recorders that do not implement VCPS.

In a computer environment, a Player/Recorder consists of a Drive and a software Application. In this combination, the software Application calculates the Sector Keys and handles decryption/ encryption of the video data. For this purpose, the software Application contains a set of Node Keys KN_H. Unlike stand-alone Players/Recorders, individual installations of a software Application may contain the same set of Node Keys KN_H. Additionally, the software Application handles the integrity protection of the Copy Control Information (CCI) provided by the encrypted copy of the CCI in the Navigation Packs.

The Drive generates a Unique ID and stores that Unique ID on the Disc. In addition, a Drive that has recording functionality reads the DKB hash value from the ADIP, and writes the DKB to a location that is accessible for a Drive that has playback-only functionality (Buffer Zone 2 in the Lead-in).

4.1.2 The Software Application

In order to calculate the Sector Keys, the software Application must retrieve both the Unique ID and the DKB hash value after authenticating the Drive. For this purpose, software Applications contain a built-in Application Key Block (AKB) and its Root Key KR_{AUTH}, while Drives contain a set of Node Keys KN_D. As part of the authentication protocol, the Drive decodes the Root Key KR_{AUTH} from the AKB using its Node Keys KN_D. Only if both the Application and the Drive are authorized, the authentication protocol results in a so-called Bus Key KB. The Bus Key KB is used to encrypt the Unique ID and the DKB hash value, over the interface between the Drive and the software Application. This ensures that the software Application obtains the Unique ID and the DKB hash value from the physical media, i.e. the Disc. The significance thereof is that the software Application ensures that encrypted video data is bound to that particular Disc.

4.1.3 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.

4.1.4 Recording

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

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

4.2 The Protection Mechanisms

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 Drive.
Device ID	-	Each VCPS Capable Player, Recorder, and Drive 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 Drive 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.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

4.3 Using VCPS

4.3.1 Overview

The following descriptions are included to provide Host Application developers with an overview of VCPS operations. Drive implementers should refer to [VCPS] for implementation details.

4.3.2 Authentication with a Drive

For the Host application, the authentication sequence proceeds as follows:

1. The Host should issue a REPORT KEY command requesting Device ID in order to obtain the Device ID.
2. The Host should retrieve the Authorization Key (AKx) from the AKB built into the Host. In addition, the Host should generate a random number (RA). The Host should issue a SEND KEY command, requesting Authorization Key in order to send this information to the Drive.
3. The Host should issue a REPORT KEY command, requesting Key Contribution in order to obtain the key contribution (QD) of the Drive. Prior to accepting the key contribution QD of the Drive, the Host should verify that the Drive has returned the correct random number (RA).
4. The Host should issue a SEND KEY command, requesting Key Contribution in order to send its own key contribution (QA) to the Drive. With its key contribution QA, the Host should include the random number RD it has received from the Drive.
5. The Host should issue a REPORT KEY command, requesting DKB Hash and Unique ID in order to retrieve the DKB hash value and Unique ID from the Drive. This information will be used to calculate the Unique Key KU for Protected Video Recordings on the Disc.

If any of the commands issued during authentication results in an error, the Host should retry the authentication protocol.

The Host may execute the authentication protocol multiple times. The Drive will always accept a REPORT KEY Device ID. The Drive interprets this command as a start of (a new execution of) the authentication protocol, i.e. the Drive will reset its internal authentication state. If another execution of the authentication protocol was in progress, that execution will be abandoned.

A more detailed description of the authentication sequence is presented in A.3.2.

4.3.3 First Protected Video Recording on DVD+R/+RW media

The Host should issue a GET CONFIGURATION command to check that the Drive and media support Protected Video Recordings (i.e. the VCPS feature is current).

The Host should issue a REPORT KEY DKB Information command to verify that the DKB is already available. If the Drive is required to retrieve the DKB from the DKB region in the ADIP, the Drive returns the number of bytes of the DKB that has been retrieved so far. This enables the Host to estimate after how much time the DKB will be available.

The Host may start recording a Protected Video Recording, while the Drive still is collecting the DKB.

In the meantime, the Host may poll the Drive using a REPORT KEY DKB Information command to check on the availability of the DKB.

The Host should issue a REPORT KEY DKB command to retrieve the DKB from the Disc. This will cause the Drive to write the DKB in Buffer Zone 2.

> Note: If the media is DVD+R, the drive also writes the first ECC block of the data zone (LBA 0, 1, 2 …, 15) in order to protect the content of Buffer Zone 2.

The Host should authenticate with the Drive (4.3.2).

The Host should verify that the DKB is consistent with the DKB Hash obtained in the final step of the authentication sequence. If the DKB is not consistent with the DKB Hash, the Host should refrain from making Protected Video Recordings.

The Host should use the DKB and the Unique ID to calculate the Disc Key KD of the Disc, and store the encrypted Unique Key KU on the Disc.

The Host may continue or start to record a new Protected Video Recording.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

4.3.4 Additional Protected Video Recordings

The Host should parse the file VIDEO_RM.IFO (or VIDEO_RK.IFO) to determine that the Disc contains Protected Video Recordings. See also [DVD+VR], and optionally [DVD+VRR].

The Host should issue a GET CONFIGURATION command to check that the Drive supports Protected Video Recordings (i.e. the VCPS feature is current).

The Host should issue a REPORT KEY DKB command to retrieve the DKB from the Disc.

The Host should authenticate with the Drive (4.3.2).

The Host should verify that the DKB is consistent with the DKB Hash obtained in the final step of the authentication sequence. If the DKB is not consistent with the DKB Hash, the Host should refrain from making Protected Video Recordings.

The Host should use the DKB and the Unique ID to calculate the Disc Key KD of the Disc, and retrieve the encrypted Unique Key KU from the Disc.

The Host may start to record a new Protected Video Recording.

4.3.5 Playback of Protected Video Recordings

The Host should parse the file VIDEO_RM.IFO (or VIDEO_RK.IFO) to determine that the Disc contains Protected Video Recordings. See also [DVD+VR], and optionally [DVD+VRR].

The Host should issue a GET CONFIGURATION command to check that the Drive supports Protected Video Recordings (i.e. the VCPS feature is current).

The Host should authenticate with the Drive (4.3.2).

The Host should issue a REPORT KEY DKB command to retrieve the DKB from the Disc.

The Host should authenticate with the Drive (4.3.2).

The Host should use the DKB and the Unique ID to calculate the Disc Key KD of the Disc, and retrieve the encrypted Unique Key KU from the Disc.

The Host may start to render a Protected Video Recording.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

5 The VCPS Feature

The VCPS feature specifies that the Drive 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 0000b.

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, the currently mounted disc has no VCPS capability. 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.

On DVD+R/+RW discs, bits 5 and 6 of byte 16 of the Physical Format Information found in the lead-in ADIP specify VCPS capability of the disc. Bit 5 is set to zero while bit 6 identifies the presence/absence of VCPS related information in the Extended Format Information. When bit 6 is set to zero, the Extended Format Information does not contain VCPS related information and Current is set to zero. When bit 6 is set to one, the Extended Format Information contains VCPS related information and Current is set to one.

Typically, the Control Data Zone is recorded to include this information. However, the Control Data Zone may be recorded by a recorder that is not VCPS capable. Consequently, the Physical Format Information in the Control Data Zone may not correctly match the ADIP version. A VCPS read-only Drive should determine disc capability by inspecting Buffer Zone 2. In the Physical Format Information of the Control Data Zone on a VCPS DVD-ROM disc, bit 6 is set to zero, while bit 5 identifies the presence/absence of VCPS information in Buffer Zone 2. When bit 5 is set to zero, Buffer Zone 2 does not contain VCPS related information. When bit 5 is set to one, the Buffer Zone 2 contains VCPS related information. If there is an indication that VCPS related information is present, then Current is set to one. Otherwise, the Disc is not VCPS Capable and Current is set to zero.

The Additional Length field shall be set to 04h.

A Drive reporting the VCPS Feature shall support the commands shown in Table 3.

Table 3 — Commands required by the Secure Channels Feature

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

This page is intentionally blank

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

6 Commands

The commands that have unique behavior defined when the VCPS Feature is current are listed in Table 4.

Table 4 — Commands for the VCPS Feature

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

6.1 REPORT KEY Command

6.1.1 General

The REPORT KEY command provides a general mechanism for transferring Authorization information from the Drive to the Host. The general form of the command is shown in Table 5.

Table 5 — 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 6.

Table 6 — 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 Drives.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 7.

Table 7 — Report Key Command Descriptor Block, VCPS Form

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code (A4h)							
1	Reserved							
2	(MSB) Starting Offset							
3								
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 Drive to the Host. 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 8.

Table 8 — Report Key Returned Data Format

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

The VCPS Function code specifies the VCPS function to be performed. VCPS Functions are listed in Table 9. 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 9 — 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 Drive shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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

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

1. If the DKB is contained in Buffer Zone 2, the Drive, the DKB structure shall be returned to the Host and the command shall be terminated with GOOD status.

   If no DKB is found in Buffer Zone 2, but the DKB is contained in the Initial Zone, the Drive shall generate a new Unique ID. The Drive shall write the DKB and the Unique ID into Buffer Zone 2. If an unrecoverable error occurs during this process, the Drive shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE. Otherwise, the Drive shall return the DKB, write the DKB into Buffer Zone 2, and terminate with GOOD status. If the media is DVD+R, the drive shall also zero-fill write the first ECC block of the data zone (LBA 0, 1, 2 …, 15).

2. If no DKB is found in either Buffer Zone 2 or the Initial Zone, the DKB is contained in the ADIP. The Drive shall completely retrieve the DKB from the DKB region in the ADIP; the Drive shall generate a new Unique ID. The Drive shall write the DKB and the Unique ID in Buffer Zone 2. If an unrecoverable error occurs during this process, the Drive shall terminate the command with CHECK CONDITION status and set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE. Otherwise, the Drive shall return the DKB, write the DKB into Buffer Zone 2, and terminate with GOOD status. If the media is DVD+R, the drive shall also zero-fill write the first ECC block of the data zone (LBA 0, 1, 2 …, 15).

3. If a DKB is not found on the Disc, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE.

The format of the returned data is defined in Table 10.

Table 10 — VCPS Key Class REPORT KEY returned data, DKB

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Data Length = N+2				
1								(LSB)
2	Reserved							
3	Reserved							
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.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 Drive. This assists the functionality of step 1 in the authentication protocol (see A.3.2). The Drive shall return Device ID_d and terminate with GOOD status. If a previous execution of the authentication protocol is in progress, the Drive shall abort that previous execution of the authentication protocol. The format of the returned data is defined in Table 11.

Table 11 — VCPS Key Class REPORT KEY returned data, Device ID

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Data Length = 26h				
1								(LSB)
2	Reserved							
3	Reserved							
	Device ID data							
0	Reserved							
...								
30								
31	(MSB)							
...	Device ID							
35								(LSB)

The Data Length field shall contain 38 (26h).

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

The Device ID field contains the Device ID of the VCPS Capable Drive.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 Drive. This assists the functionality of step 4 in the authentication protocol (see A.3.2). The command execution shall proceed as follows:

1. If the authentication sequence has been violated, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive 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 Drive shall return its key contribution QD and terminate with GOOD status.

The format of the returned data is defined in Table 12.

Table 12 — VCPS Key Class REPORT KEY returned data, Key Contribution

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Data Length = 26h							
1								(LSB)
2	Reserved							
3	Reserved							
Key Contribution data								
0	Reserved							
...								
3								
4	(MSB) Encrypted Random Numbers 1							
...								
19								(LSB)
20	(MSB) Encrypted Drive Key Contribution							
...								
35								(LSB)

The Data Length field shall contain 38 (26h).

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 Drive combined with IV2 and encrypted using the Root Key KR_{auth}. IV2 is a 128-bit licensed constant.)

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 (see A.3.2).

The command execution shall proceed as follows:

1. If the Drive 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 authentication beginning with step 1 (see 4.3.2) of the authentication sequence.
2. If the Host has not retrieved the DKB and Unique ID during this authentication sequence, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR.
3. Otherwise, the Drive shall return the DKB Hash and Unique ID, 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, DKB Hash & Unique ID

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Data Length = 26h				
1								(LSB)
2	Reserved							
3	Reserved							
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 38 (26h).

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 Drive that has playback-only functionality shall set the DKB Hash field to all zeros, prior to encryption. A Drive 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 Drive shall set the DKB Hash field to all zeros, prior to encryption.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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. This information may be required for step 8 of the authentication protocol (see A.3.2). The format of the returned data is shown 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	(MSB)			Data Length = 000Eh				
1								(LSB)
2	Reserved							
3	Reserved							
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 14 (000Eh).

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

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

6.2 SEND KEY Command

6.2.1 General

The SEND KEY command provides a general mechanism for transferring Authorization information from the Host to the device. The general form of the command is shown in Table 15.

Table 15 — SEND KEY Command Descriptor Block, General Form

Byte \ Bit	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 16.

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

Table 16 — 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 Drives.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 17.

Table 17 — 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 9. 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 18 — 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 Drive.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

During command execution, the Host shall send parameter data to the Drive. The general format of that parameter data is shown in Table 19.

Table 19 — Send Key Parameter List Format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Send Key Data Length (N+2)							
1	(Number of bytes available following this field) (LSB)							
2	Reserved							
3	Reserved							
Send Key Parameter Data								
0	Send Key Data							
1								
N-1								

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 Drive. This function of the SEND KEY command provides the functionality of step 2 in the authentication protocol (see A.3.2). The command execution shall proceed as follows:

1. If the authentication sequence has been violated, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive 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 Drive shall accept the Authorization Key and terminate with GOOD status.

The format of the parameter data is defined in Table 20.

Table 20 — VCPS Key Class SEND KEY parameter list, Authorization Key

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Send Key Data Length (0022h)							
1								(LSB)
2	Reserved							
3	Reserved							
Authorization Key Information								
0	Reserved							
...								
6								
7	Node Key Number							
8	(MSB) Host's Random Number							
...								
15								(LSB)
16	(MSB) Authorization Key KA_X							
...								
31								(LSB)

The Send Key Data Length is 34 bytes (0022h).

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 Drive 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 Host'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 Drive.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

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 in step 6 of the authentication protocol (see A.3.2). The command execution shall proceed as follows:

1. If the authentication sequence has been violated, the Drive 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 Drive is not equal to the random number RD that the Drive has sent to the Application in the previous REPORT KEY Contribution command, the Drive 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 4.3.2).
3. Otherwise, the Drive shall accept the Application Bus Key contribution 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, Key Contribution

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Send Key Data Length (0026h)							
1								(LSB)
2	Reserved							
3	Reserved							
Key Contribution data								
0	Reserved							
...								
3								
4	(MSB) Encrypted Random Numbers 2							
...								
19								(LSB)
20	(MSB) Encrypted Application Key Contribution							
...								
35								(LSB)

The Send Key Data Length is 38 bytes (0026h).

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

The Encrypted Random Numbers 2 field contains the random number RD of the Drive 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.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

7 Mode Parameters

The VCPS Feature is able to become current (and useful) only for Drives that are able to report a current DVD-ROM Profile.

Each of those profiles has a nonempty list of mandatory mode pages. Refer to MMC-4.

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

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

This page is intentionally blank

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

Annex A Authentication

A.1 Disc Recognition

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

A.2 Initializing for VCPS Operations

If a VCPS Capable Disc is mounted, then preparation for VCPS operations involves reading the DKB prior to it being needed. If the DKB is only available from ADIP, the DKB may be read into the Drive's internal memory beginning during the spin-up process and continuing as a background function. This permits collecting a copy of the DKB while giving priority to Host commands.

A.3 Authentication

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.

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

A.3.2 Authentication Protocol

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

Step 1

The Application shall request the Drive 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 Drive in the built-in Application Key Block (AKB). If the Drive 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 Drive 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 Drive shall generate a 64-bit random number RD as well as a 128-bit random key contribution QD. The Application shall request the Drive 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 Drive 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 Drive 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 Drive:

(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 Drive 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 Drive has sent to the Application in step 4, the Drive shall abort the authentication protocol.

Otherwise, the Drive shall calculate the Bus Key KB as follows:

KB = AESHash(QD || QA).

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

Step 8

The Application shall request the Drive to return the following message:

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

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

To assemble this message, a Drive that has playback-only functionality shall set the DKB Hash field to all zeros; a Drive 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'.

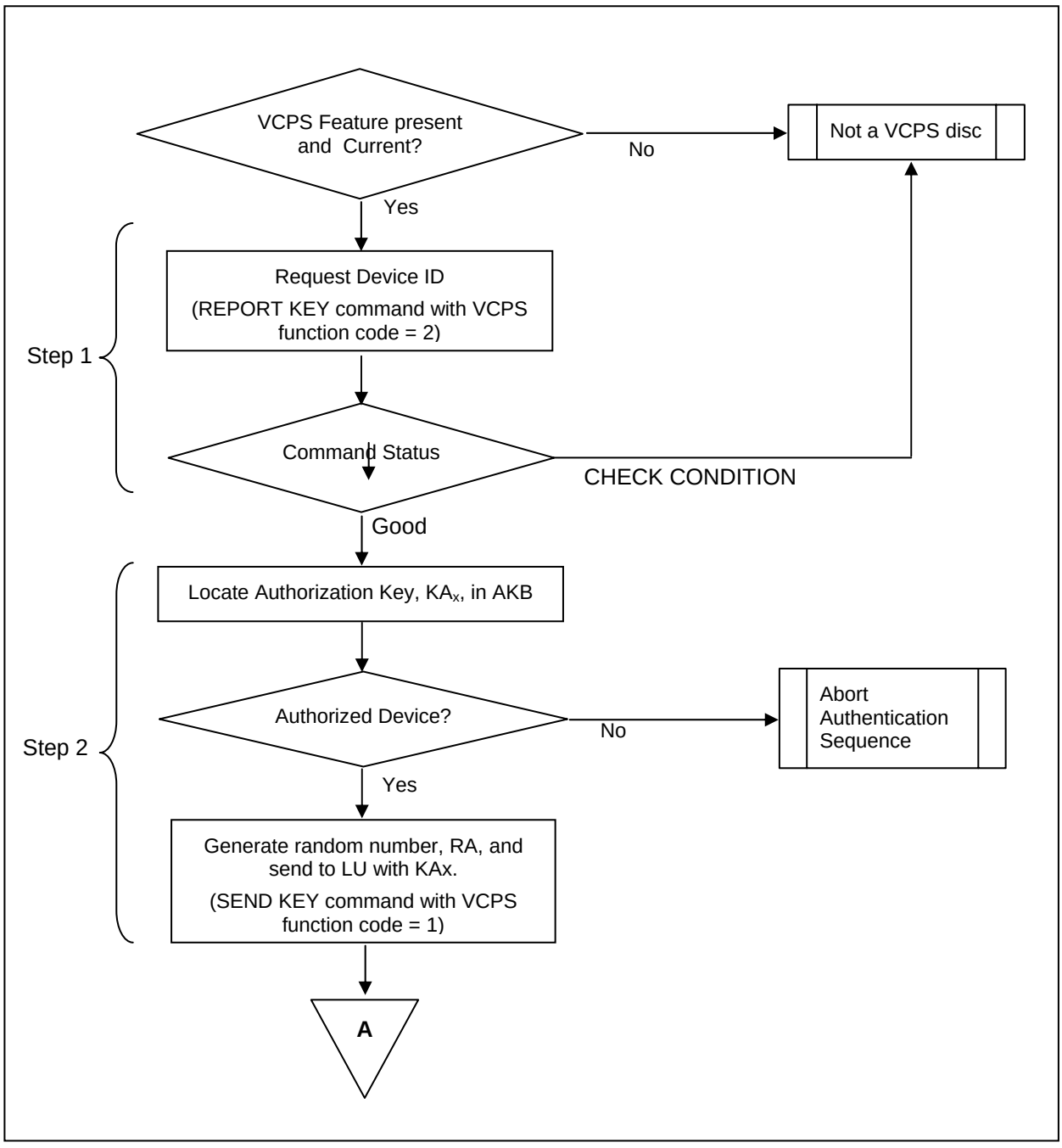

Figure 1 – Authentication Sequence, part 1

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

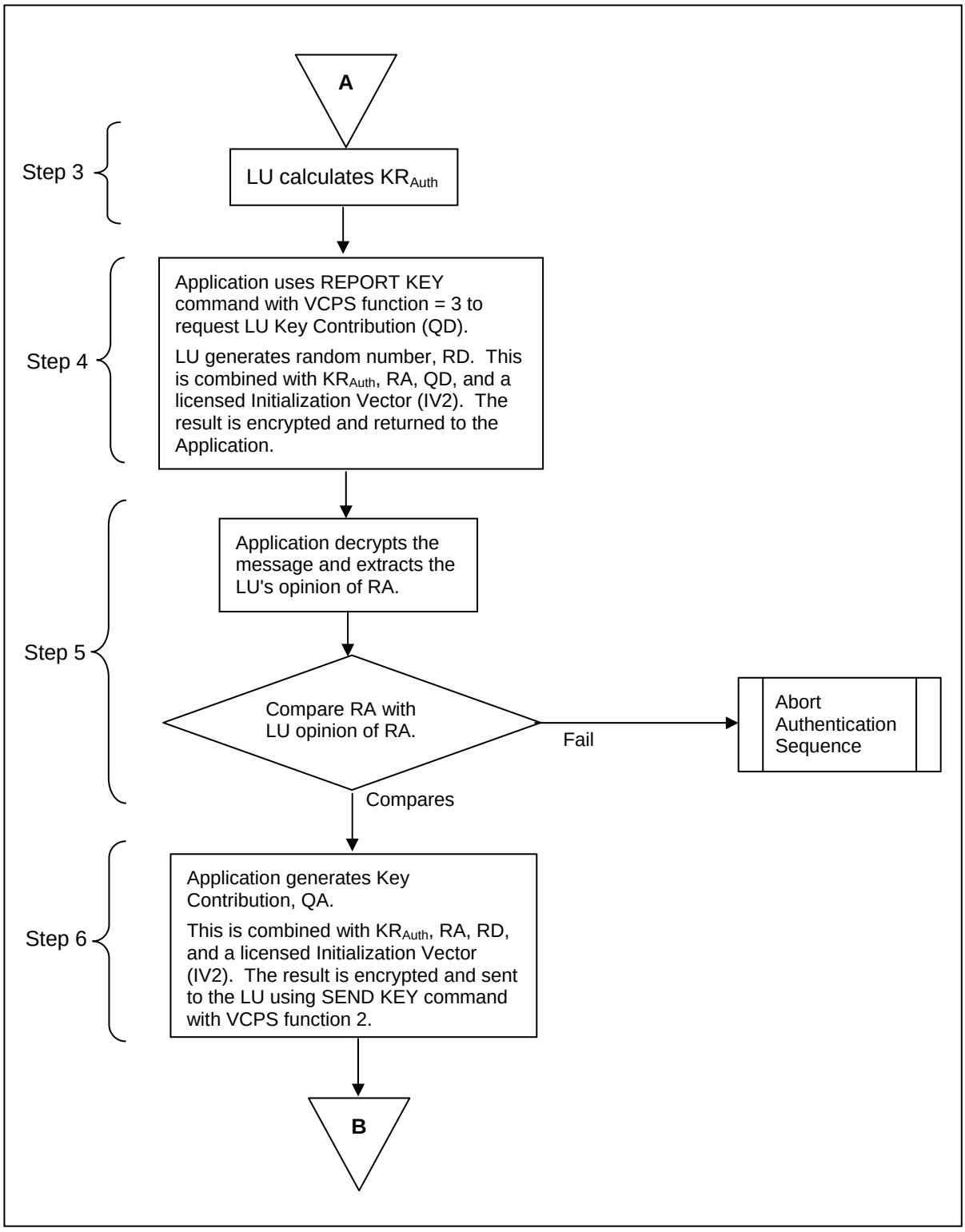

Figure 2 – Authentication Sequence, part 2

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

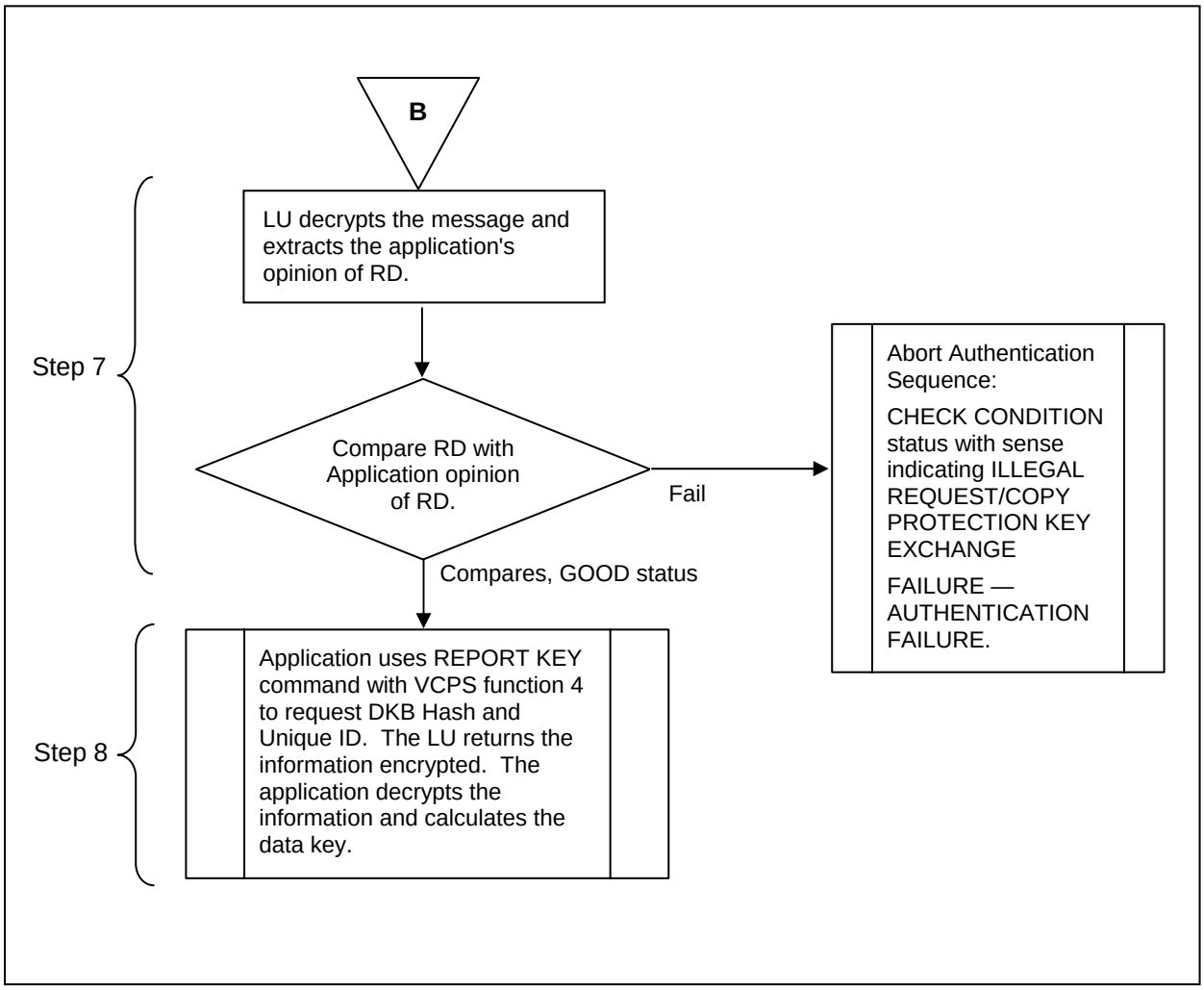

Figure 3 – Authentication Sequence, part 3

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company

END

© 2004, 2005 Royal Philips Electronics and Hewlett-Packard Company