BD CPS

Multi-Media Commands Enabling "Content Protection System for Blu-ray Disc Rewritable Specifications"

DRAFT

Version 0.82

March 8, 2005

LEGAL NOTICE

COPYRIGHT

DISCLAMER

The information contained herein is believed to be accurate as of the date of publication, however, the 3C will not be liable for any damages, including indirect or consequential, from use of *Multi-Media Commands Enabling " Content Protection System for Blu-ray Disc Rewritable Specifications"* or reliance on the accuracy of this document.

LICENSING

Application of *Multi-Media Commands Enabling " Content Protection System for Blu-ray Disc Rewritable Specifications"* in host environments is permitted and no additional written copyright license regarding *Multi-Media Commands Enabling " Content Protection System for Blu-ray Disc Rewritable Specifications"* from the 3C is required.

PURPOSE

The information contained in this document is being made available solely for the purpose of standardization. Each of the 3C grants to members of INCITS, its technical committees and their associated task groups the right to use, reproduce, or display this document solely for the purposes of INCITS standardization activities, provided this LEGAL NOTICE shall be included in any reproduction of this document:

CONTACT

For licensing information regarding *" Content Protection System for Blu-ray Disc Rewritable Specifications"* as used on media, players or recorders, please consult with:

Blu-ray Disc License Agent
Sony Corporation
Shinagawa INTERCITY C Tower 27F
2-15-3 Konan Minato-ku, Tokyo, 108-6201 Japan
E-mail: agent blu-raydisc.info
Fax: +81 3 5769 5727

For any further explanation of the contents of this document, or in case of any perceived inconsistency or ambiguity of interpretation, or for further details, please consult with:

Takaharu Ai
Matsushita Electric Industrial Co., Ltd.
E-mail : ai.takaharu@jp.panasonic.com
or
Bob IJtsma
Royal Philips Electronics
E-mail : bob.ijtsma@philips.com
or
Norichika Mine
Sony Corporation
E-mail : norichika.mine@jp.sony.com

Contents

Tables

Figures

1 Introduction

The Content Protection System (CPS) for Blu-ray Disc Rewritable Specifications, Informational Version [3C-BD-CPS-INFO] defines a method to prevent unauthorized copying and/or redistribution of data that is recorded in the BD-RE formats. In general, the formatting does not modify the LBA space of supported discs and formats.

The MMC-5 command set is used as the starting point for enabling BD CPS 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-5:

1. Introduction – This section
2. References – A list of documents that may be needed by the reader for the correct understanding of this document.
3. Definitions and Abbreviations – A glossary of terminology in this document
4. BD CPS Model – 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. BD CPS Feature - Features describe Drive capabilities.
6. BD CPS Commands – Commands are described from the Initiator's point of view.
7. Mode Pages – 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.

2 References

[MMC-5] SCSI Multi-Media Commands – 5 (T10/1675D, Draft Revision 1b)

[SPC-3] SCSI Primary Command Set - 3 (SPC-3) (INCITS T10/1416D Draft Revision 21)

[BDRE-1] System Description, Blu-ray Rewritable Format - Part 1, Basic Format Specifications

[BDR-1] System Description, Blu-ray Recordable Format - Part 1, Basic Format Specifications

[3C BD-CPS-INFO] Content Protection System for Blu-ray Disc Rewritable Specifications - Informational Version

This page is intentionally blank

3 Definitions and Abbreviations

3.1 Definitions

3.1.1 Authentication and Key Exchange (AKE)

The SAC establishment protocol that results in a shared SAC Key.

3.1.2 BD Application

A set of rules to store and process user data on a BD-RE Disc.

3.1.3 BD Drive

A PC component that is authorized to establish a SAC with a Blu-ray Disc Initiator Application. A BD Drive can write or read a BD-RE Disc.

3.1.4 Certificate

A data structure containing certified information, such as the identity and Public Key of a BD Drive or Initiator Application. It is digitally signed using the Private Key of the KIC.

3.1.5 Disc ID

A disc identifier that is unique for each disc. The data format for the Disc ID is shown in [3C-BD-CPS-INFO].

3.1.6 Disc Key

A secret cryptographic key that shall vary at least with every release of the RKB. A Disc Key is denoted as k_d. It is contained in the RKB Record, encrypted with the Media Key.

3.1.7 Initiator Application

A PC application that is authorized to establish a SAC with a Blu-ray Disc Drive. For example, an Initiator Application is a software program that implements one or more BD Applications and is running on an open, general-purpose computing platform.

3.1.8 Key Issuing Center (KIC)

A first function of the KIC is to provide Device IDs, Device Keys, RKBs and Public/Private Key pairs. A second function of the KIC is to manage Application identifiers. A third function of the KIC is to provide authentication information for the SAC.

3.1.9 Public Key

The key of an asymmetric cryptographic system that is made public. It is used to verify signatures.

3.1.10 Private Key

The key of an asymmetric cryptographic system that is kept secret. It is used to generate signatures.

3.1.11 SAC

Secure Authenticated Channel. A communications channel between an Initiator Application and a BD Drive, which provides authenticity and confidentiality. A SAC Key is denoted as k_{sac}.

3.1.12 SAC Key

The cryptographic key that is used to encrypt a Disc ID and a Disc Key.

3.2 Abbreviations

AKE	Authentication and Key Exchange
AV	Audio Visual
BCA	Burst Cutting Area
BD-RE	Blu-ray Disc Rewritable
CDB	Command Descriptor Block
KIC	Key Issuing Center
lsb	Least Significant Bit
msb	Most Significant Bit
PC	Personal Computer
PIC	Permanent Information & Control data
PKC	Public Key Certificate
SAC	Secure Authenticated Channel

4 BD CPS Model

4.1 Overview

4.1.1 General

This is a general description of the [3C-BD-CPS-INFO].

[3C-BD-CPS-INFO] defines a method for preventing unauthorized copying and/or redistribution of content that is written in BD recording format.

In a computer environment, [3C-BD-CPS-INFO] has three components: an Application operating as or through the Initiator, a BD Drive acting as the Logical Unit, and a BD Disc with CPS structures in the PIC area and the BCA. Each component possesses a collection of secrets necessary for recording and rendering data protected with [3C-BD-CPS-INFO].

The Initiator Application collects Logical Unit and disc secrets during an authentication process, combining these with its own secrets to determine the keys necessary to encrypt/decrypt protected sectors.

4.1.2 Playback

For the purposes of decrypting and decoding data, all decryption and decoding is performed by the 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 sector X.

4.1.3 Recording

Similarly, for the purposes of encoding and encrypting data, all encoding and encryption is performed by the application.

Protected recording in [3C-BD-CPS-INFO] is possible only when the correct components that conform to [3C-BD-CPS-INFO] are present:

1. A CPS licensed BD-RE disc in a
2. licensed logical unit, and operating under control of a
3. licensed application.

4.1.4 Protection Mechanisms

See [3C-BD-CPS-INFO].

4.1.5 Authentication

In order to play or record data protected according to [3C BD-CPS-INFO], the Application and Logical Unit shall first authenticate each other to allow secure exchange of necessary cryptographic material. The authentication is a modified form of a standard certificated-based challenge-response authentication and Diffie-Hellman key exchange (AKE) as shown in Figure 1.

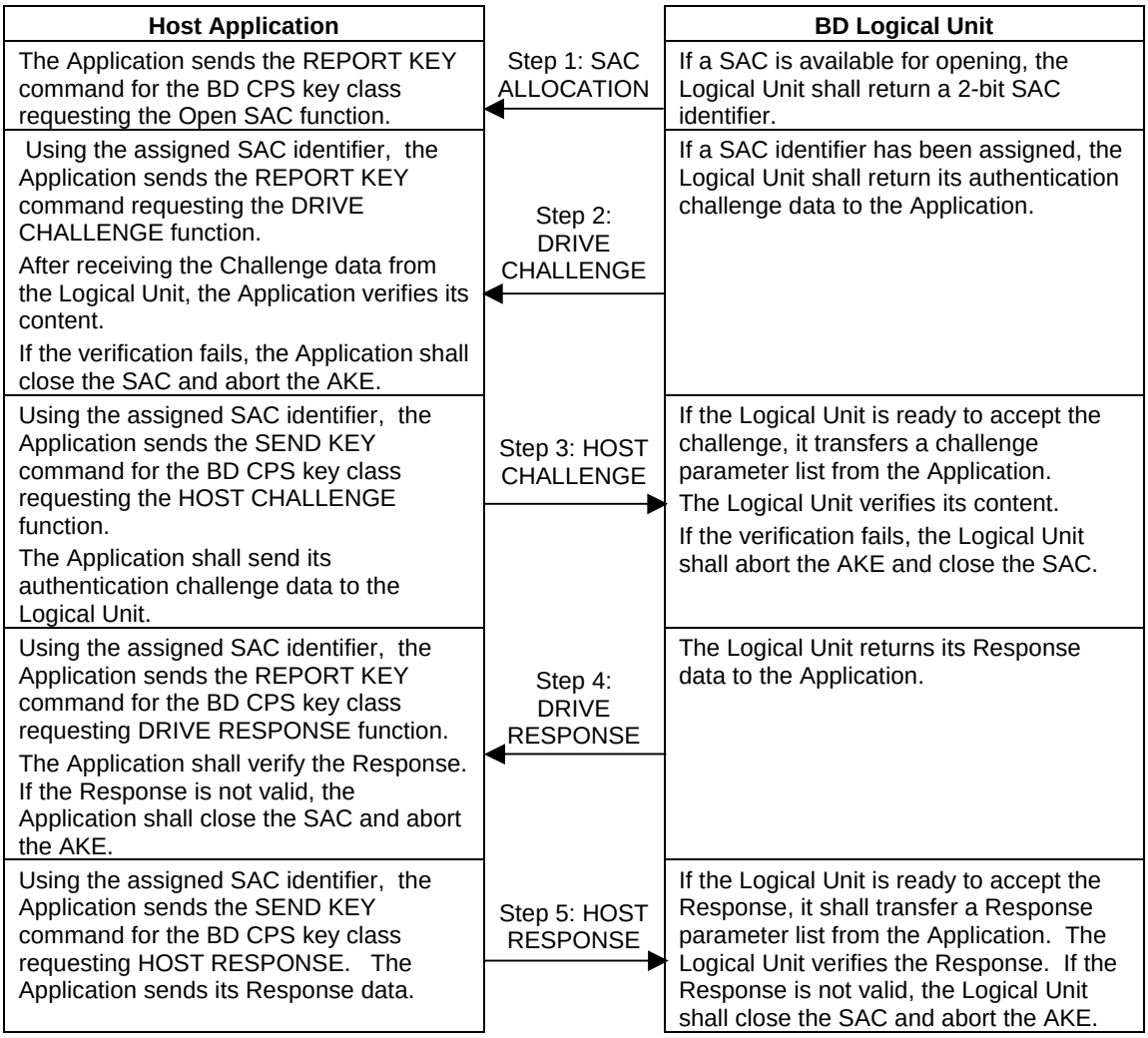

Figure 1 — BD CPS Authentication

If the entire AKE succeeds, the Application and Logical Unit shall each use the information passed during the key exchange to calculate a SAC key.

Next, the Application sends the REPORT KEY command requesting the DISC KEY & DISC ID function. The Logical Unit sends the Disc Key and Disc ID, encrypted by the SAC Key. Once the data has been transfered, the Logical Unit shall automatically close the SAC.

5 BD CPS Feature

The presence of the BD CPS Feature indicates that the device is capable of mounting and executing the BD CPS AKE for BD-RE discs that contain data structures which conform to [3C-BD-CPS-INFO].

The BD CPS Feature Descriptor is shown in Table 1.

Table 1 – BD CPS Feature Descriptor

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB) Feature Code (0120h)							
1								(LSB)
2	Reserved			Version			Persistent	Current
3	Additional Length = 04h							
4	Reserved							
5	BD CPS Version							
	Major Version Number				Minor Version Number			
6	Reserved							Maximum Number of Simultaneously Opened SACs
7	Reserved							

The Feature Code shall be set to 0120h.

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.

The Current bit; when cleared to zero indicates that this Feature is not currently active and certain Feature Dependent Data may not be valid. When set to one, this Feature is currently active and the Feature Dependent Data is valid.

The Additional Length field shall be set to 04h.

The BD CPS Version shall be set to the version licensed for the device. e.g Version 1.0 is encoded with major version = 0001b and minor version = 0000b.

The Maximum Number of Simultaneously Opened SACs (N) represents the maximum number of Initiator entities that may concurrently use this feature. The maximum value for N is 3. Each opened SAC is assigned a non-zero SAC ID (1, 2, or 3).

A device reporting the BD CPS Feature shall support the commands shown in Table 2.

Table 2 – Commands required by the Secure Channels Feature

Operation Code	Command Name	Reference
A3h	SEND KEY, Key Class 30h	6.3
A4h	REPORT KEY, Key Class 30h	6.2

6 BD CPS Commands

6.1 General

The commands listed in Table 3 are mandatory when the BD CPS Feature is current.

Table 3 – Commands for the BD CPS Features

Command	Op Code	Reference
REPORT KEY, Key Class 30h	A4h	6.2
SEND KEY, Key Class 30h	A3h	6.3

6.2 REPORT KEY Command

The REPORT KEY command provides a general mechanism for transferring authentication information from the Logical Unit to the Initiator Application. The general form of the command is shown in Table 4.

Table 4 – 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 5.

Table 5 – Key Class Field

Key Class	Authentication Type
00h	DVD CSS/CPPM or CPRM
01h	ReWritable Security Service - A
02h - 1Fh	Reserved
20h	VCPS for DVD+R/+RW
21h - 2Fh	Reserved
30h	BD CPS
31h - FFh	Reserved

Key Class = 00h is for authentication services for DVD Video (CSS, CPRM). For specific descriptions, please refer to [MMC-5].

Key Class = 01h is for ReWritable Security Service - A, please refer to [MMC-5].

Key Class = 20h is defined for VCPS for DVD+R/+RW. See [MMC-5].

Key Class = 30h is defined for security functions unique to BD Drives which conform to [3C-BD-CPS-INFO]. The CDB format and functions associated with this Key Class are described in 6.2.1.

6.2.1 The BD CPS Key Class

6.2.1.1 The REPORT KEY CDB for BD CPS Key Class

Key Class = 30h is used for authentication services associated with the BD CPS Feature. The CDB has the format shown in Table 6.

Table 6 – Report Key Command Descriptor Block, BD CPS Form

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code (A4h)							
1	Reserved							
2	Reserved							
3	Reserved							
4	Reserved							
5	Reserved							
6	Reserved							
7	Key Class = BD CPS (30h)							
8	(MSB) Allocation Length							
9								(LSB)
10	SAC Identifier		BD CPS Function					
11	Control							

When the REPORT KEY command is to be used for BD CPS functions, the Key Class shall be set to 30h.

The Allocation Length field specifies the maximum length in bytes of the 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.

The SAC Identifier field identifies the SAC assigned during the Open SAC function. When the BD CPS Function is Open SAC, the Logical Unit ignores this field.

The BD CPS Function code specifies the function to be performed. BD CPS Functions are shown in Table 7.

Table 7 – BD CPS Functions for REPORT KEY

BD CPS Function code	BD CPS Function
00h	Open SAC
01h	Reserved
02h	DRIVE CHALLENGE
03h	DRIVE RESPONSE
04h	DISC KEY & DISC ID
06h – 3Eh	Reserved
3Fh	Close SAC

6.2.1.2 Command Execution

6.2.1.2.1 General

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								(LSB)
2	Reserved							
3	Reserved							
Report Key Data								
0	Report Key Data – N bytes (possibly encrypted)							
1								
...								
N-1								

Data Length is a 16-bit representation of the number of bytes of Additional Data that are available. In the case of key class = BD CPS, when data is passed through the SAC, the 4-byte header shall not be encrypted.

6.2.1.2.2 Open SAC (00h)

When the function field is 00h, a SAC is to be opened for secure access. Authentication may proceed only after the application has opened a SAC. The Report Key data is shown in Table 9.

Table 9 – REPORT KEY Data Format for Open a SAC

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Data Length = 0006h				
1								(LSB)
2	Reserved							
1	Reserved							
Additional Data								
0	Reserved							
1	Reserved							
2	Reserved							
3	SAC Identifier		Reserved					

Data Length shall be 6.

If there is no SAC available, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE.

6.2.1.2.3 Drive Challenge (02h)

In step 2 of the authentication process (see 4.1.5), an application operating through the Initiator shall request a Challenge from the Logical Unit.

If the SAC identifier in the CDB does not represent an opened SAC, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/ COMMAND SEQUENCE ERROR.

Table 10 – Drive Challenge Returned Data Format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Data Length = 0076h				
1								(LSB)
2	Reserved							
3	Reserved							
Drive Challenge Data								
0	Random Number (R_Drv)							
...								
15								
16	Certificate Data (PKC_Drv)							
...								
115								

Data Length shall be 118.

In order that authentication may proceed, the Initiator should receive all of the available returned data. Consequently, the CDB Allocation length field should be at least 120.

The Random Number field contains a random number that is generated by the Logical Unit. For each challenge that the Logical Unit sends to the Initiator Application, a new random number shall be generated.

The Certificate Data field contains the Public Key Certificate of the Logical Unit (see [3C-BD-CPS-INFO]).

6.2.1.2.4 Drive Response (03h)

In step 4 of the authentication process (see 4.1.5), an application operating through the Initiator shall request a Response from the Logical Unit.

If the authentication process has already failed or if the authentication sequence has been violated, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR. Otherwise, the device shall return the appropriate Response data structure and terminate with GOOD status. The format for this returned data is shown in Table 11.

Table 11 – Drive Response Data Format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Data Length = 0052h							
1								(LSB)
2	Reserved							
3	Reserved							
Drive Response Data								
0	Drv_X1							
...								
39								
40	Drive Response Signature							
...								
79								

Data Length shall be 82.

In order that authentication may proceed, the Initiator should receive all of the available returned data. Consequently, the CDB Allocation length field should be at least 84.

The Drv_X1 field consists of two 20-byte values representing the vector: k_Drv***G**, where _Drv is the random number generated by the Logical Unit for the Diffie-Hellman key exchange, and **G** is the vector representing the base point of the Elliptic Curve.

The Drive Response Signature field consists of two 20-byte values representing the signature associated with this step in the authentication (see [3C-BD-CPS-INFO]).

6.2.1.2.5 Disc Key and Disc ID (04h)

After successful authentication (see 4.1.5), an application operating through the Initiator shall request the Disc Key and Disc ID from the Logical Unit.

If the authentication process has already failed or if the authentication sequence has been violated, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR. Otherwise, the device shall return the appropriate Disc Key and Disc ID data structure, close the SAC, and terminate with GOOD status. The format for this returned data is shown in Table 12.

Table 12 – Disc Key and Disc ID Data Format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Data Length = 0022h							
1								(LSB)
2	Reserved							
3	Reserved							
Disc Key and Disc ID								
0	Disc Key							
...								
15								
16	Disc ID							
...								
31								

Data Length shall be 34.

In order to have a usable disc key and disc ID, the Initiator should receive all of the available returned data. Consequently, the CDB Allocation length field should be at least 36.

The Disc Key and Disc ID data is encrypted with the SAC Key.

6.2.1.2.6 Close SAC (3Fh)

The device shall return no data in response to this SAC Function.

The Logical Unit shall terminate operation of the current SAC and make the SAC resource available for allocation.

6.3 SEND KEY Command

The SEND KEY command provides a general mechanism for transferring authentication information from the Host to the Logical Unit. The general form of the command is shown in Table 13.

Table 13 – 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 14.

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 14 – Key Class Field

Key Class	Authentication Type
00h	DVD CSS/CPPM or CPRM
01h	ReWritable Security Service – A
02h - 1Fhh	Reserved
20h	VCPS for DVD+R/+RW
21h - 2Fh	Reserved
30h	BD CPS
31h - FFh	Reserved

Key Class = 00h is for authentication services for DVD Video (CSS, CPRM). For specific descriptions, please refer to [MMC-5].

Key Class = 01h is for ReWritable Security Service - A, please refer to [MMC-5].

Key Class = 20h is defined for VCPS for DVD+R/+RW. See [MMC-5].

Key Class = 30h is defined for security functions unique to BD Drives which conform to [3C-BD-CPS-INFO]. The CDB format and functions associated with this Key Class are described in 6.3.1.

6.3.1 The BD CPS Key Class

6.3.1.1 The SEND KEY CDB for the BD CPS Key Class

Key Class = 30h is used for authentication services associated with the BD CPS Feature. The CDB has the format shown in Table 15.

Table 15 – SEND KEY Command Descriptor Block, BD CPS 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	Reserved							
7	Key Class = BD CPS (30h)							
8	(MSB) Parameter List Length							
9	(LSB)							
10	SAC Identifier		BD CPS Function					
11	Control							

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

The SAC Identifier field identifies the SAC assigned during the (REPORT KEY) Open SAC function.

The BD CPS Function code specifies the BD CPS Function to be performed.

Table 16 – BD CPS Functions for SEND KEY

BD CPS Function code	BD CPS Function
00h	Reserved
01h	Reserved
02h	HOST CHALLENGE
03h	HOST RESPONSE
04h-3Fh	Reserved

6.3.1.2 Command Execution

6.3.1.2.1 General

Parameter list data shall be sent according BD CPS Function specified in the command. The general format of that parameter list is shown in Table 17.

Table 17 – Send Key Parameter List Format

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

The Data Header contains only Data Length. Data Length is a 16-bit representation of the number of bytes of Send Key Parameter Data that are sent.

6.3.1.2.2 Host Challenge (02h)

In step 3 of the authentication process (see 4.1.5), an application operating through the Initiator shall send a Challenge to the Logical Unit.

If the SAC identified in the CDB is not open, 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 format for the Host Challenge Parameter List is shown in Table 18.

Table 18 – Host Challenge Parameter List Format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Data Length = 0076h							
1								(LSB)
2	Reserved							
3	Reserved							
Host Challenge Data								
0	Random Number (R_Host)							
...								
15								
16	Certificate Data (PKC_Host)							
...								
115								

Data Length shall be set to 118.

In order that authentication proceed, it is necessary that the Logical Unit receive all of the defined parameter list data. Consequently, the CDB Parameter List Length field shall be equal to 120.

The Random Number field contains a random number that is generated by the Initiator's Application. For each challenge that the Application sends to the Logical Unit, a new random number shall be generated.

The Certificate Data field contains the Public Key Certificate of the Application (see [3C BD-CPS-INFO]).

The Logical Unit shall validate the Host Application's PKC. If the validation fails, the SAC shall be closed, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE - AUTHENTICATION FAILURE.

6.3.1.2.3 Host Response (03h)

In step 5 of the authentication process (see 4.1.5), an application operating through the Initiator shall send a Response to the Logical Unit.

If the authentication process has already failed or if the authentication sequence has been violated, 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 format for the Host Response Parameter List is shown in Table 19.

Table 19 – Host Response Parameter List Format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB) Data Length = 0052h							
1								(LSB)
2	Reserved							
3	Reserved							
Host Response Data								
0	Host_X1							
...								
39								
40	Host Response Signature							
…								
79								

Data Length shall be 82.

In order that authentication proceed, it is necessary that the Logical Unit receive all of the defined parameter list data. Consequently, the CDB Parameter List Length field shall be equal to 84.

The Host_X1 field consists of two 20-byte values representing the vector k_Host***G**, where k_Host is the random number generated by the Initiator's Application for the Diffie-Hellman key exchange, and **G** is the vector representing the base point of the Elliptic Curve.

The Host Response Signature field consists of two 20-byte values representing the signature associated with this step in the authentication (see[3C-BD-CPS-INFO]).

The Logical Unit shall validate the Host Response Signature. If the validation fails, the SAC shall be closed, the command shall be terminated with CHECK CONDITION status and sense bytes SK/ASC/ASCQ shall be set to ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE - AUTHENTICATION FAILURE.

7 Mode Pages

The BD CPS Feature is able to become current (and useful) only for Logical Units that are able to report a current BD-RE Profile. That profile has a nonempty list of mandatory mode pages.

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

END