

Security Architecture for Intelligent Attachment Device Specifications

– Interface for iVDR –

Version 1.22

September, 2011

- *SAFIA License Group*

Hitachi, Ltd.

PIONEER CORPORATION

SANYO Electric Co., Ltd.

SHARP CORPORATION

Preface

■ Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Hitachi, PIONEER, SANYO, and SHARP disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Some portions of this document, identified as "Draft" are in an intermediate draft form and are subject to change without notice. Adopters and other users of this Specification are cautioned these portions are preliminary, and that products based on it may not be interoperable with the final version or subsequent versions thereof.

Copyright © 2011 by Hitachi, Ltd., PIONEER CORPORATION, SANYO Electric Co., Ltd., and SHARP CORPORATION. Third-party brands and names are the property of their respective owners.

■ Intellectual Property

Implementation of this Specification requires a license from the SAFIA License Group.

■ Contact Information

Feedback on this specification should be addressed to info@safia-lb.com.

The SAFIA License Group can be contacted at info@safia-lb.com.

The URL for the SAFIA License Group web site is: <http://www.safia-lb.com>.

Table of Contents

1	General	1
1.1	Scope	1
1.2	References	1
1.3	Definitions	1
1.3.1	Definitions in iVDR/IF	1
1.3.2	Definitions in SAFIA/PDS1	2
1.3.3	Definitions in ATAPI	3
1.3.4	Additional definitions	3
1.4	Abbreviations	6
1.4.1	Abbreviations in iVDR/IF	6
1.4.2	Abbreviations in SAFIA/PDS1	6
1.4.3	Additional abbreviations	7
1.5	Conventions	7
1.5.1	Keywords	7
1.5.2	Numerical values	8
1.5.3	Bit and byte ordering	8
1.5.4	State transition diagram	8
1.5.5	Sequence example	9
1.6	Notations	9
1.6.1	Keys	9
1.6.2	Operations	10
1.6.3	Additional notations	10
2	Portion to be described in this document in the total system	11
3	Device Interface physical and electrical requirements	11
4	General operational requirements	12
4.1	Two feature sets determined in SAFIA	12
4.1.1	SAFIA UT feature set	13
4.1.1.1	READ QUALIFIED and its subcommands	13
4.1.1.2	SET QUALIFIED and its subcommands	13
4.1.1.3	WRITE QUALIFIED and its subcommands	13
4.1.2	SAFIA BT feature set	14
4.1.2.1	READ QUALIFIED and its subcommands	14
4.1.2.2	SET QUALIFIED and its subcommands	14
4.1.2.3	WRITE QUALIFIED and its subcommands	15
4.2	Write protection management on Qualified Storage	15
5	Command Block register definitions and descriptions	16
6	Subcommand descriptions	16

6.1	iVDR Qualified Access feature set subcommand.....	16
6.1.1	Normal Outputs on GET QUALIFIED ACCESS MODE.....	17
6.2	SAFIA UT feature set subcommands.....	17
6.2.1	Subcommands derived from READ QUALIFIED.....	17
6.2.1.1	GET DEVICE CLASS CERTIFICATE.....	17
6.2.1.2	GET INCEPTIVE SESSION KEY UT CONNECTION.....	20
6.2.1.3	GET INCEPTIVE SESSION KEY UT TRANSFER.....	23
6.2.1.4	GET MASKED USAGE PASS.....	25
6.2.1.5	GET PRIMAL CHALLENGE KEY UT CONNECTION.....	28
6.2.1.6	GET PRIMAL SESSION KEY UT CONNECTION.....	30
6.2.1.7	GET PRIMAL SESSION KEY UT RECONNECTION.....	33
6.2.1.8	GET SAFIA FEATURES UT.....	36
6.2.1.9	GET TRANSACTION LOG EXTERNAL.....	40
6.2.1.10	GET TRANSACTION STATUS UT RECOVERY.....	43
6.2.1.11	GET USAGE PASS.....	46
6.2.2	Subcommands derived from SET QUALIFIED.....	49
6.2.2.1	CHECK EXECUTION STATUS.....	49
6.2.2.2	ENCRYPT USAGE PASS COPY.....	52
6.2.2.3	ENCRYPT USAGE PASS MOVE.....	55
6.2.2.4	ENCRYPT USAGE PASS PLAY.....	58
6.2.2.5	READ USAGE PASS.....	61
6.2.2.6	WRITE USAGE PASS.....	64
6.2.3	Subcommands derived from WRITE QUALIFIED.....	64
6.2.3.1	CREATE INCEPTIVE SESSION KEY UT TRANSFER.....	64
6.2.3.2	PUT INCEPTIVE SESSION KEY UT CONNECTION.....	67
6.2.3.3	PUT INCEPTIVE SESSION KEY UT TRANSFER.....	70
6.2.3.4	PUT PRIMAL CHALLENGE KEY UT CONNECTION.....	73
6.2.3.5	PUT PRIMAL SESSION KEY UT CONNECTION.....	76
6.2.3.6	PUT PRIMAL SESSION KEY UT RECONNECTION.....	79
6.2.3.7	PUT USAGE PASS.....	81
6.2.3.8	SEARCH TRANSACTION LOG UT RECONNECTION.....	85
6.2.3.9	SEARCH USAGE PASS UT RECOVERY.....	88
6.2.3.10	VERIFY DEVICE CLASS CERTIFICATE.....	91
6.2.3.11	VERIFY TRANSACTION STATUS UT RECOVERY.....	94
6.3	SAFIA BT feature set subcommands.....	97
6.3.1	Subcommands derived from READ QUALIFIED.....	97
6.3.1.1	GET DEVICE CLASS CERTIFICATE.....	97
6.3.1.2	GET INCEPTIVE CHALLENGE KEY BT CONNECTION.....	98
6.3.1.3	GET INCEPTIVE SESSION KEY BT CONNECTION.....	99
6.3.1.4	GET INCEPTIVE SESSION KEY BT RECONNECTION.....	100
6.3.1.5	GET INCEPTIVE SESSION KEY BT TRANSFER.....	101
6.3.1.6	GET MASKED USAGE PASS.....	102

6.3.1.7	GET MASKED USAGE PASS WITH KEYED HASH	103
6.3.1.8	GET SAFIA FEATURES BT	104
6.3.1.9	GET TRANSACTION STATUS BT RECOVERY	107
6.3.1.10	GET USAGE PASS	108
6.3.2	Subcommands derived from SET QUALIFIED	109
6.3.2.1	CHECK EXECUTION STATUS	109
6.3.2.2	CLEAR CONNECTION LOG	111
6.3.2.3	CREATE INCEPTIVE SESSION KEY BT TRANSFER	113
6.3.2.4	ENCRYPT USAGE PASS COPY	114
6.3.2.5	ENCRYPT USAGE PASS MOVE	115
6.3.2.6	ENCRYPT USAGE PASS PLAY	116
6.3.2.7	READ USAGE PASS	117
6.3.2.8	WRITE USAGE PASS	118
6.3.3	Subcommands derived from WRITE QUALIFIED	118
6.3.3.1	PUT PRIMAL CHALLENGE KEY BT CONNECTION	118
6.3.3.2	PUT PRIMAL SESSION KEY BT CONNECTION	119
6.3.3.3	PUT PRIMAL SESSION KEY BT RECONNECTION	121
6.3.3.4	PUT PRIMAL SESSION KEY BT TRANSFER	123
6.3.3.5	PUT USAGE PASS	124
6.3.3.6	RECOVER USAGE PASS	127
6.3.3.7	SEARCH USAGE PASS BT RECOVERY	129
7	State transition diagrams.....	132
7.1	State transition diagrams on UT mode.....	133
7.1.1	State transition diagram within S _{U02}	134
7.1.2	State transition diagram within S _{U06}	135
7.1.3	State transition diagram within S _{U03}	135
7.1.4	State transition diagram within S _{U04}	136
7.1.5	State transition diagram within S _{U07}	137
7.1.6	State transition diagram within S _{U08}	138
7.1.7	State transition diagram within S _{U12}	139
7.1.8	State transition diagram within S _{U09}	139
7.1.9	State transition diagram within S _{U10}	140
7.1.10	State transition diagram within S _{U13}	140
7.2	State transition diagrams on BT mode	141
7.2.1	State transition diagram within S _{B02}	143
7.2.2	State transition diagram within S _{B07}	144
7.2.3	State transition diagram within S _{B03}	144
7.2.4	State transition diagram within S _{B04}	145
7.2.5	State transition diagram within S _{B05}	146
7.2.6	State transition diagram within S _{B08}	147
8	Sequence examples	147

8.1	Sequence example for Storage Device recognition	147
8.2	Sequence examples for the transaction on UT mode and BT mode.....	149
8.2.1	Abbreviations used in the figures in this section.....	149
8.2.1.1	Key names and others.....	149
8.2.1.2	Wait time for completing the cryptographic operations in the Storage Device.....	149
8.2.2	Channel management.....	150
8.2.2.1	Channel opening	150
8.2.2.2	Channel closing.....	150
8.2.3	Masked Usage Pass transfer	150
8.2.4	Subcommand belonging to SAFIA feature set execution status transfer.....	151
8.2.5	A Usage Pass relocation in the drive.....	151
8.2.6	The sequence examples for Usage Pass transfer in UT mode	151
8.2.6.1	Transfer of External Log portion of Transaction Log.....	151
8.2.6.2	Connection Stage	153
8.2.6.3	Reconnection Stage	154
8.2.6.4	Transfer Stage.....	155
8.2.6.5	Recovery Stage	156
8.2.7	The sequence examples for Usage Pass transfer under BT mode	156
8.2.7.1	Connection Stage	156
8.2.7.2	Reconnection Stage	158
8.2.7.3	Transfer Stage.....	159
8.2.7.4	Recovery Stage.....	161
Annex A	Composition of an HIFU	163

1 General

1.1 Scope

This document describes the architecture of Device Interface other than physical and electrical characteristics. The architecture is constructed completely based on iVDR/IF, therefore the Storage Device has the characteristics that normal data writing to the Device and reading from the Device is realized by the standard of AT Attachment with Packet Interface; here normal data means the data other than Device Class Certificates, various keys and Usage Pass which are described in SAFIA/PDS1. In the sense, the architecture is affinitive to standard AT Attachment architecture.

1.2 References

- 1) ANSI NCITS 361-2002
Information Technology – AT Attachment with Packet Interface – 6 [ATAPI]
- 2) ISO/IEC 646, Information technology, ISO 7-bit coded character set for information interchange, 1991 [ISO/IEC646]
- 3) iVDR Hard Disk Drive Consortium,
File System Specification, Version 2.1, April 2006 [iVDR/FS]
- 4) iVDR Hard Disk Drive Consortium,
Interface Specification, Version 2.0, April 2006 [iVDR/IF]
- 5) Security Architecture for Intelligent Attachment Device Specifications;
Protocol and Data Structure Volume 1 [SAFIA/PDS1]
- 6) Security Architecture for Intelligent Attachment Device Specifications;
Protocol and Data Structure Volume 2 [SAFIA/PDS2]
- 7) Serial ATA International Organization;
Serial ATA Revision 2.6, 15-February-2007 [SATA]

1.3 Definitions

1.3.1 Definitions in iVDR/IF

The following terms used in this document are defined in iVDR/IF:

- BP
- Channel
- Channel Identifier
- LBAQ
- Qualified Access mode
- Subcommand

- Qualified Space

1.3.2 Definitions in SAFIA/PDS1

The following terms used in this document are defined in section 1.3.2 of SAFIA/PDS1.

- Access Condition
- Access Condition for Storage Module (This term was defined as Access Condition for Storage Device in version 1.0.)
- Bidirectional Transfer
- Challenge Key
- Cipher Information of Content
- Data concatenation
- Destination
- Device
- Device Class
- Device Class Certificate
- Device Class Private Key
- Device Class Public Key
- Device Private Key
- Device Public Key
- Domicile
- ECDH Shared Key
- Entry Pointer
- Inceptive
- Interface Module
- Interface Unit
- Masked Usage Pass
- Message Version
- Open Storage
- Primal
- Qualified Storage
- Qualified Storage Controller
- Revoked Device Class List

- SAFIA Content
- SAFIA Terminal
- Session
- Session Key
- Session Status
- Source
- Storage Module (This term was defined as Security Management Module in version 1.0.)
- Transaction
- Transaction Status
- Unidirectional Transfer
- Usage Pass
- Usage Pass Copy
- Usage Pass Identifier
- Usage Pass Move
- Usage Pass Play
- Usage Pass Status
- Usage Pass Transfer
- Usage Pass Transfer Unit

1.3.3 Definitions in ATAPI

The following terms used in this document are defined in ATAPI:

- ATA (AT Attachment)
- command aborted
- Command Block registers
- command completion
- LBA (Logical Block Address)
- PIO (programmed input/output)

1.3.4 Additional definitions

The following terms used in this document are defined in this section.

- Buf.UPTU
Buf.UPTU is a buffer placed in Usage Pass Transfer Unit (see chapter 2) in the Storage Module. This buffer is used for the following purpose:

- to place a received data like Device Class Certificate, encrypted keys, encrypted Usage Passes and so forth. If the received data is encrypted, the data is decrypted according to the description provided in SAFIA/PDS1 and SAFIA/PDS2, and the structure is verified in this buffer. Moreover, comparison of Acceptable Usage Pass Type in the Device Class Certificate sent from other Device and Usage Pass Type of the Usage Pass to be transferred is executed. Usage Pass Transfer Unit determines whether it outputs the Usage Pass or not by the result.
- to place a data like Device Class Certificate, keys and Usage Passes which will be output to other Device. If the encryption of the data is necessary, the process is executed in this buffer.
- **Buf.QSTC**

Buf.QSTC is a buffer placed in Qualified Storage Controller (see chapter 2). This buffer is used for the following purpose:

 - to modify the value of COUNT in AC_s. The Usage Pass of which AC_s is modified is whether sent to Buf.UPTU in order to transfer to the other Device or written into Qualified Storage in order to record by Qualified Storage Controller. When the Usage Pass is written into Qualified Storage, Qualified Storage Controller verifies the COUNT in AC_s and determines to write or not according to the description provided in the section 7.3 of SAFIA/PDS1.
 - to verify the structure of the Usage Pass fetched from the Qualified Storage.
- **Device Interface**

Device Interface is the one defined in SAFIA/PDS1. Moreover, its physical characteristics are Serial ATA compatible and logical characteristics comply with the description provided in iVDR/IF.
- **Device Interface bus**

Device Interface bus is an physical electric wires on which command codes, parameters attributive to each command and actual data flow between the Host Interface Unit and the Storage Interface Unit.
- **Device Interface commands**

Device Interface commands are the commands and subcommands described only in iVDR/IF and this document.
- **Host Device**

Host Device is the one defined in SAFIA/PDS1. However, it includes at least one Host Interface Module described in this section.
- **Host Interface Module**

Host Interface Module is the one defined in SAFIA/PDS1. However, it comprises at least one Host Interface Unit described in this section.
- **Host Interface Unit**

Host Interface Unit is the one defined in SAFIA/PDS1. However, the Unit has the features and function described in only iVDR/IF and this document, which means that this unit has the following functions

 - to set subcommands with parameters described in this document, commands described in iVDR/IF and data into the Command Block registers equipped in Storage Interface Unit.

- to capture response parameters described in this document and data set in the Command Block registers equipped in Storage Interface Unit.
- to send/receive data hold in itself from/to Import Module, Export Module and Transmit Module.
- Destination Module
 - As for Usage Pass transfer from Import Module or Transmit Module to Storage Module, Storage Module is Destination Module. If the Usage Pass transfer is executed in either UT mode or BT mode, a Device including Import Module or Transmit Module which outputs the Usage Passes is Primal Device and Storage Device including the Storage Module is Inceptive Device.
 - Similarly, as for Usage Pass transfer from Storage Module to Export Module or Transmit Module, Export Module or Transmit Module is Destination Module. If the Usage Pass transfer is executed in UT mode, a Device including Export Module or Transmit Module which receives the Usage Passes is Inceptive Device and Storage Device including the Storage Module is Primal Device. On the contrary, if the Usage Pass transfer is executed in BT mode, a Device including Export Module or Transmit Module which receives the Usage Passes is Primal Device and Storage Device including the Storage Module is Inceptive Device.
- Serial ATA compatible
 - Serial ATA compatible is a state of interface, where physical characteristics other than the shape of connector and logical characteristics other than the command set which Host Interface Unit issues to Storage Interface Unit to access Open Storage and Qualified Storage comply with SATA.
- Source Module
 - As for Usage Pass transfer from Import Module or Transmit Module to Storage Module, Import Module or Transmit Module is Source Module. If the Usage Pass transfer is executed in either UT mode or BT mode, a Device including Import Module or Transmit Module which outputs the Usage Passes is Primal Device and Storage Device including the Storage Module is Inceptive Device.
 - Similarly, as for Usage Pass transfer from Storage Module to Export Module or Transmit Module, Storage Module is Source Module. If the Usage Pass transfer is executed in UT mode, a Device including Export Module or Transmit Module which receives the Usage Passes is Inceptive Device and Storage Device including the Storage Module is Primal Device. On the contrary, if the Usage Pass transfer is executed in BT mode, a Device including Export Module or Transmit Module which receives the Usage Passes is Primal Device and Storage Device including the Storage Module is Inceptive Device.
- Status
 - Status is data set of “Session Status || Usage Pass Status” in a Transaction Log in this document. “Session Status” and “Usage Pass Status” are defined in SAFIA/PDS1.
- Storage Device
 - Storage Device is the one defined in SAFIA/PDS1. However, it includes at least one Storage Interface Module described in this section.
- Storage Interface Module

Storage Interface Module is the one defined in SAFIA/PDS1. However, it comprises at least one Storage Interface Unit described in this section.

- **Storage Interface Unit**

Storage Interface Unit is the one defined in SAFIA/PDS1. However, the Unit has the features and function described only in iVDR/IF and this document, which means that this unit has the following functions

- to interpret subcommands with parameters described in this document, commands described in iVDR/IF and data which are set in the Command Block registers equipped in itself.
- to set response parameters described in this document and data into the Command Block registers equipped in itself.
- to send/receive data hold in itself from/to Storage Module and Open Storage.

- **Transaction Log**

Transaction Log is defined in SAFIA/PDS1. However, address of the Qualified Storage where the objective Usage Pass is recorded into and sector size of the Usage Pass are added.

1.4 Abbreviations

1.4.1 Abbreviations in iVDR/IF

The following abbreviations are described in iVDR/IF.

- CHID

1.4.2 Abbreviations in SAFIA/PDS1

The following abbreviations are described in section 1.4 of SAFIA/PDS1.

- AC_s
- BT
- CIC
- CL
- HIFU
- OST
- QST
- QSTC
- RDCL
- SAFIA
- SIFU
- SS

- TL
- TS
- UP
- UPID
- UPL
- UPS
- UPTU
- UT

1.4.3 Additional abbreviations

- AI Action Indicator
- CBR Command Block Register
- CKS Checksum
- EP Entry Pointer
- MUP Masked Usage Pass
- MVB_[X] Message Version (in BT mode, X is P or I)
- MVU_[X] Message Version (in UT mode, X is P or I)
- ms milli second
- PDS Primal Device Specifier
- RAPDI Recovery-Allowed Primal Device Indicator
- RPI Recovery Permission Indicator
- SN_[P] Serial Number of Device Class Certificate embedded in Primal Device
- STTS Status
- TM Type Map
- na not applicable

1.5 Conventions

1.5.1 Keywords

Words of mandatory, may, reserved, shall, should follow the description provided in section 1.5.1 of SAFIA/PDS1. A word “obsolete” follows the description provided in ATAPI. A word “na” appeared in registers indicates the content of a bit or field is not applicable to the particular subcommand.

1.5.2 Numerical values

Conventions for description of numerical values including decimal numbers, hexadecimal numbers and binary numbers follow the description provided in section 1.5.2 of SAFIA/PDS1.

1.5.3 Bit and byte ordering

Conventions for bit and byte ordering follow the description provided in section 1.5.3 of SAFIA/PDS1.

1.5.4 State transition diagram

Usage Pass Transfer is achieved by using subcommands derived from iVDR Qualified Access feature set. Obligations as to the order of the subcommand execution are described as state transition in chapter 7. In this section, convention for the diagram for state transition is described.

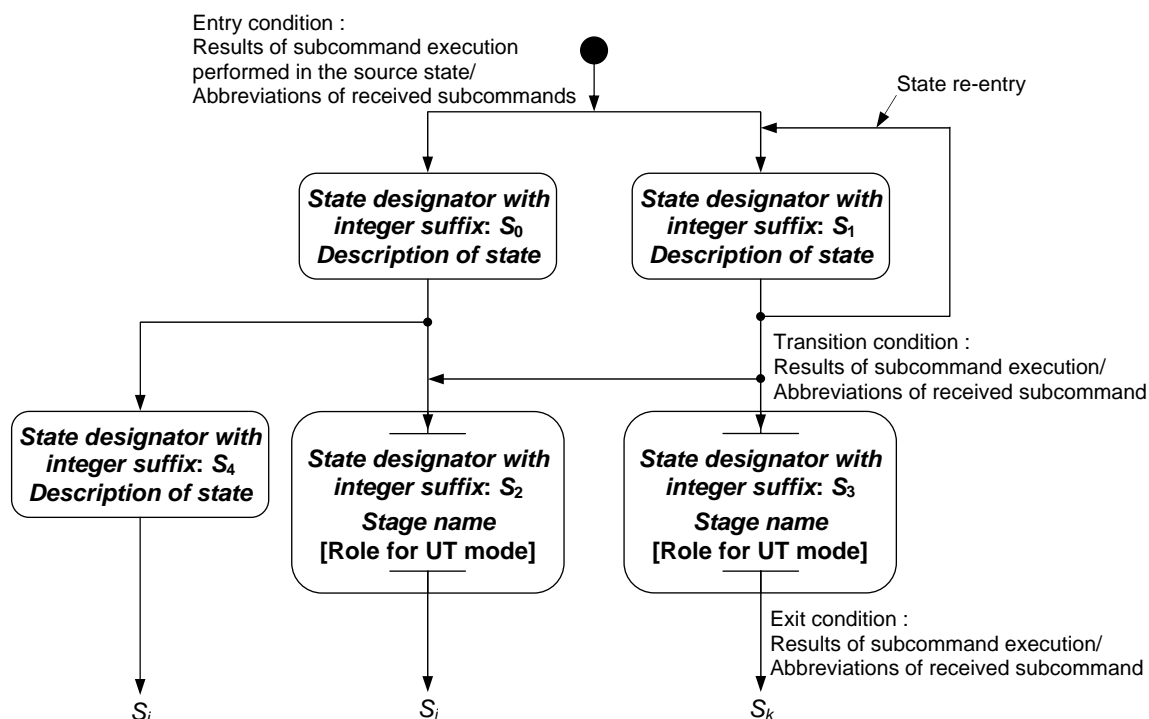


Figure 1.1 Convention as to state transition diagram

A big circle that is blacked out is not a normal state but is just a start point. Similarly, a mere big circle indicates just a start point in each diagram.

Each state is identified by a state designator and a description of the state. The state designator is unique among all states in all state diagrams in this document. The state designator consists of an italic capitalized letter with suffix, like S_{U000}. First suffix indicates the initial letter of mode ("U" is for UT mode, "B" is for BT mode). Next two digits indicate the number that is assigned to each state. The third digits are assigned to substates to identify them. Description of substate is a brief description of the completed results executed in the source state. But there are some exceptions for this notation rule if readers may not confuse.

States which has bar internally have “substates” inside. Substates are described in terms of states. For only UT mode, information to indicate whether the state is in terms of Primal or Inceptive is written as “Role for UT mode” under the stage name.

The transition condition is described on the arrows emitted from each state. The condition is described in terms of the result of subcommand execution. The state of result of subcommand execution is described as “done” or “failed”, and executed subcommands are listed as abbreviation after “/”. These description rules are applied for every state to enter, exit and re-enter.

An arrow which emits from a dot located on a base arrow means that the transition which follows the direction is allowed. This means that only state transitions which follow direction of arrow is allowed and transition like S_1 to S_4 is not allowed because the direction of arrow between S_0 and S_2 is “ S_0 to S_2 ”, not vice versa.

1.5.5 Sequence example

In this section, convention for the diagram as to subcommand execution is described.



Figure 1.2 Convention for subcommand and data flow

A term on the arrow means the followings from the left:

N: Number of subcommand executed in the sequence

SC: Subcommand name

ILC: Initial letter of the command name defined in iVDR Qualified Access feature set, namely, “R” means READ QUALIFIED, “W” means WRITE QUALIFIED, and “S” means SET QUALIFIED. The subcommands are descendent from these three commands.

An arrow of full line means a flow of subcommand from the Host Interface Unit to the Storage Interface Unit and dashed line means a flow of data to be actually transferred. In the above example, data is transferred from the Storage Interface Unit to the Host Interface Unit. Note that for returning some information to the Host Interface Unit by setting them in the Command Block register on the response from the Storage Interface Unit, no arrows are described.

1.6 Notations

1.6.1 Keys

The following notations of keys follow the description provided in section 1.6.1 of SAFIA/PDS1.

- K_c
- K_r
- KP_r
- K_{dc}
- KP_{dc}

- K_d
- KP_d
- K_s
- K_{ch}
- $K_{x[I]}$
- $K_{x[P]}$
- $K_{s[x]CL}$
- $K_{s[x]TL}$
- $*KP_x$
- $RDCL_{[x]}$
- AC_{sTL}

1.6.2 Operations

The following notations of operations follow the description provided in section 1.6.2 of SAFIA/PDS1.

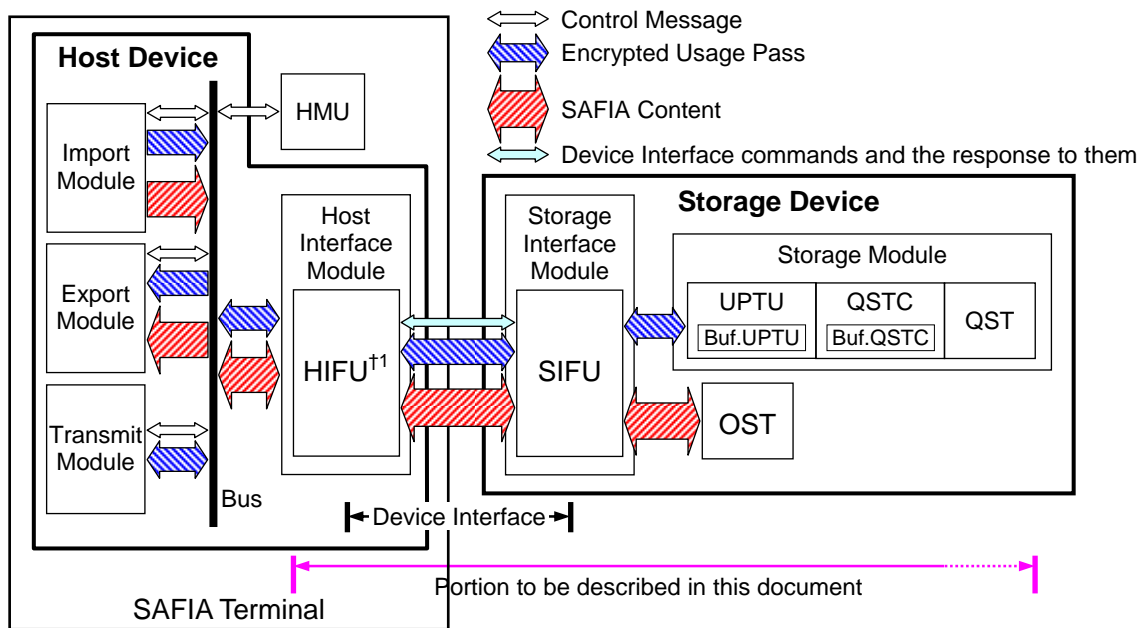
- \parallel
- $C(K_r, KP_x)$
- $E(K, D)$

1.6.3 Additional notations

- $D(x, y)$ The result of the decryption of data y with a key x .
- $*K_{d[x]}$ Shared symmetric key through ECDH key exchange with $KP_{d[x]}$ and $K_{d[x]}$. The key is ECDH Shared Key which is equal to $*KP_{d[x]}$ described in SAFIA/PDS1. However, $*K_{d[x]}$ is not calculated with $KP_{d[x]}$ but calculated with $K_{d[x]}$.
- $SectorNumber(x)$ The result of the operation is a quotient of $(x + 511) / 512$.

2 Portion to be described in this document in the total system

The scope of this document in the total system is shown in Figure 2.1.



†1 There may be cases where a part of HIFU not related to Connection Log and Transaction Log is not in Host Device. Details are described in Annex A.

Figure 2.1 Described part

3 Device Interface physical and electrical requirements

Physical and electrical requirements for Device Interface are the interface which is Serial ATA compatible.

4 General operational requirements

The following articles follow the description provided in iVDR/IF.

- Command delivery
- Register delivered data transfer command sector addressing
- Interrupts
- Multiword DMA
- General feature set
- Ultra DMA feature set
- Packet command feature set
- Overlapped feature set
- Queued feature set
- Power Management feature set
- Advanced Power Management feature set
- Security Mode feature set
- Self-monitoring, analysis, and reporting technology feature set
- Host Protected Area feature set
- CFA feature set
- Removable Media Status Notification and Removable Media feature sets
- Power-Up in Standby feature set

4.1 Two feature sets determined in SAFIA

SAFIA UT and BT feature set, which are determined as to UT mode and BT mode respectively, provides the subcommand set to realize Usage Pass transfer on Device Interface, on the basis of the particulars described in SAFIA/PDS1. These feature sets are described by use of the following three iVDR Qualified Access feature set commands specified in iVDR/IF.

- READ QUALIFIED
- SET QUALIFIED
- WRITE QUALIFIED

When the above three commands are issued from the Host Interface Unit to the Storage Interface Unit, the Host Interface Unit sets particular parameters to Command Block registers. The Storage Interface Unit interprets received command and a set of parameters as a subcommand, and executes it.

When SAFIA UT feature set is implemented on a Host Interface Unit and a Storage Interface Unit, all subcommands described in sections of 4.1.1.1, 4.1.1.2 and 4.1.1.3 shall be implemented

in the Units as far as no exceptional clause is provided. Similarly, SAFIA BT feature set is implemented in the Units, all subcommands described in sections of 4.1.2.1, 4.1.2.2 and 4.1.2.3 shall be implemented in the Units as far as no exceptional clause is provided.

4.1.1 SAFIA UT feature set

4.1.1.1 READ QUALIFIED and its subcommands

READ QUALIFIED is the command wherein after command is transferred from the Host Interface Unit to the Storage Interface Unit, data transfer is actually executed from the Storage Interface Unit to the Host Interface Unit. Subcommands derived from this command by setting particular parameters to the Command Block registers are shown in Table 4.1.

Table 4.1 Subcommands derived from READ QUALIFIED

No.	Subcommand name	Abbreviation
1	GET DEVICE CLASS CERTIFICATE	GC_U
2	GET INCEPTIVE SESSION KEY UT CONNECTION	GIS_UCN
3	GET INCEPTIVE SESSION KEY UT TRANSFER	GIS_UTR
4	GET PRIMAL CHALLENGE KEY UT CONNECTION	GPC_U
5	GET PRIMAL SESSION KEY UT CONNECTION	GPS_UCN
6	GET PRIMAL SESSION KEY UT RECONNECTION	GPS_URCN
7	GET MASKED USAGE PASS	GMUP_U
8	GET SAFIA FEATURES UT	GSF_U
9	GET TRANSACTION LOG EXTERNAL	GTL
10	GET TRANSACTION STATUS UT RECOVERY	GTS_U
11	GET USAGE PASS	GUP_U

Descriptions on the subcommands listed above are provided in section 6.2.1.

4.1.1.2 SET QUALIFIED and its subcommands

SET QUALIFIED is the command wherein actual data transfer is not executed when the command is received. Subcommands derived from this command by setting particular parameters to the Command Block registers are shown in Table 4.2.

Table 4.2 Subcommands derived from SET QUALIFIED

No.	Subcommand name	Abbreviation
12	CHECK EXECUTION STATUS	CES_U
13	ENCRYPT USAGE PASS COPY	EUPC_U
14	ENCRYPT USAGE PASS MOVE	EUPM_U
15	ENCRYPT USAGE PASS PLAY	EUPP_U
16	READ USAGE PASS	RUP_U

Descriptions on the subcommands listed above are provided in section 6.2.2.

4.1.1.3 WRITE QUALIFIED and its subcommands

WRITE QUALIFIED is the command wherein after command is transferred from the Host

Interface Unit to the Storage Interface Unit, data transfer is actually executed from the Host Interface Unit to the Storage Interface Unit. Subcommands derived from this command by setting particular parameters to the Command Block registers are shown in Table 4.3.

Table 4.3 Subcommands derived from WRITE QUALIFIED

No.	Subcommand name	Abbreviation
17	CREATE INCEPTIVE SESSION KEY UT TRANSFER	CIS_UTR
18	PUT INCEPTIVE SESSION KEY UT CONNECTION	PIS_UCN
19	PUT INCEPTIVE SESSION KEY UT TRANSFER	PIS_UTR
20	PUT PRIMAL CHALLENGE KEY UT CONNECTION	PPC_U
21	PUT PRIMAL SESSION KEY UT CONNECTION	PPS_UCN
22	PUT PRIMAL SESSION KEY UT RECONNECTION	PPS_URCN
23	PUT USAGE PASS	PUP_U
24	SEARCH TRANSACTION LOG UT RECONNECTION	STL_U
25	SEARCH USAGE PASS UT RECOVERY	SUP_U
26	VERIFY DEVICE CLASS CERTIFICATE	VC_U
27	VERIFY TRANSACTION STATUS UT RECOVERY	VTS_U

Descriptions on the subcommands listed above are provided in section 6.2.3.

4.1.2 SAFIA BT feature set

4.1.2.1 READ QUALIFIED and its subcommands

READ QUALIFIED is the command wherein after command is transferred from the Host Interface Unit to the Storage Interface Unit, data transfer is actually executed from the Storage Interface Unit to the Host Interface Unit. Subcommands derived from this command by setting particular parameters to the Command Block registers are shown in Table 4.4.

Table 4.4 Subcommands derived from READ QUALIFEID

No.	Subcommand name	Abbreviation
1	GET DEVICE CLASS CERTIFICATE	GC_B
2	GET INCEPTIVE CHALLENGE KEY BT CONNECTION	GIC_B
3	GET INCEPTIVE SESSION KEY BT CONNECTION	GIS_BCN
4	GET INCEPTIVE SESSION KEY BT RECONNECTION	GIS_BRCN
5	GET INCEPTIVE SESSION KEY BT TRANSFER	GIS_BTR
6	GET MASKED USAGE PASS	GMUP_B
7	GET MASKED USAGE PASS WITH KEYED HASH	GMUPH
8	GET SAFIA FEATURES BT	GSF_B
9	GET TRANSACTION STATUS BT RECOVERY	GTS_B
10	GET USAGE PASS	GUP_B

Descriptions on the subcommands listed above are provided in section 6.3.1.

4.1.2.2 SET QUALIFIED and its subcommands

SET QUALIFIED is the command wherein actual data transfer is not executed when command is received. Subcommands derived from this command by setting particular parameters to the

Command Block registers are shown in Table 4.5.

Table 4.5 Subcommands derived from SET QUALIFIED

No.	Subcommand name	Abbreviation
11	CHECK EXECUTION STATUS	CES_B
12	CLEAR CONNECTION LOG	CCL_B
13	CREATE INCEPTIVE SESSION KEY BT TRANSFER	CIS_BTR
14	ENCRYPT USAGE PASS COPY	EUPC_B
15	ENCRYPT USAGE PASS MOVE	EUPM_B
16	ENCRYPT USAGE PASS PLAY	EUPP_B
17	READ USAGE PASS	RUP_B

Descriptions on the subcommands listed above are provided in section 6.3.2.

4.1.2.3 WRITE QUALIFIED and its subcommands

WRITE QUALIFIED is the command wherein after command is transferred from the Host Interface Unit to the Storage Interface Unit, data transfer is actually executed from the Host Interface Unit to the Storage Interface Unit. Subcommands derived from this command by setting particular parameters to the Command Block registers are shown in Table 4.6.

Table 4.6 Subcommands derived from WRITE QUALIFIED

No.	Subcommand name	Abbreviation
18	PUT PRIMAL CHALLENGE KEY BT CONNECTION	PPC_B
19	PUT PRIMAL SESSION KEY BT CONNECTION	PPS_BCN
20	PUT PRIMAL SESSION KEY BT RECONNECTION	PPS_BRCN
21	PUT PRIMAL SESSION KEY BT TRANSFER	PPS_BTR
22	PUT USAGE PASS	PUP_B
23	RECOVER USAGE PASS	RCVUP_B
24	SEARCH USAGE PASS BT RECOVERY	SUP_B

Descriptions on the subcommands listed above are provided in section 6.3.3.

4.2 Write protection management on Qualified Storage

When the Host Interface Unit issues DISABLE WRITE QUALIFIED SPACE to the Storage Interface Unit, modification of the information recorded in Qualified Storage is prohibited (cf. iVDR/IF). After reception of this subcommand, the Storage Interface Unit, the Usage Pass Transfer Unit and the Qualified Storage Controller abort the execution of seven subcommands according to the rules described in Table 4.7 in UT and BT mode.

Table 4.7 Subcommands to be aborted

Subcommand	Rules for abort
PUT USAGE PASS	Always
CLEAR CONNECTION LOG	Always
RECOVER USAGE PASS	Always (defined only in BT mode)
VERIFY TRANSACTION STATUS UT RECOVERY	Always (defined only in UT mode)
ENCRYPT USAGE PASS COPY	In the case when bit 2 of Features register is set to one for DISABLE WRITE QUALIFIED SPACE
ENCRYPT USAGE PASS MOVE	In the case when bit 1 of Features register is set to one for DISABLE WRITE QUALIFIED SPACE
ENCRYPT USAGE PASS PLAY	In the case when bit 0 of Features register is set to one for DISABLE WRITE QUALIFIED SPACE

5 Command Block register definitions and descriptions

Definitions and descriptions on Command Block register follow the description provided in chapter 4 of iVDR/IF.

6 Subcommand descriptions

In this chapter, description for every subcommand for Usage Pass Transfer is provided. Data to be transferred are briefly described for each PIO data in and PIO data out subcommand. Detailed data structure is provided in SAFIA/PDS1 and SAFIA/PDS2. In this chapter, the following points are noted:

- (1) Some parts occupied with “fz” in the Command Block registers, fields and variables shall be filled with zero in this chapter.
- (2) Abort conditions are described in the section of “Error outputs” and “Description”. The conditions described in “Error outputs” section are mainly related to parameters set in the Command Block registers. Meanwhile, the conditions described in “Description” are related to the detailed process which shall be executed on the Storage Device after the reception of each subcommand. If one of the conditions is satisfied, the execution of the subcommand shall be aborted, ABRT in Error register and ERR in Status register shall be set to one by the Storage Interface Unit.

6.1 iVDR Qualified Access feature set subcommand

As specified in section 5.2.1.3.6 of iVDR/IF, Qualified Access modes implemented on the Storage Device is notified to the Host Device in Normal Outputs on GET QUALIFIED ACCESS MODE. The configuration of the Normal Outputs is described in the next subsection.

6.1.1 Normal Outputs on GET QUALIFIED ACCESS MODE

Register	7	6	5	4	3	2	1	0
Error	Specified in iVDR/IF							
Sector Count	M1	MCN_M1			M0	MCN_M0		
LBA Low	Specified in iVDR/IF							
LBA Mid	Specified in iVDR/IF							
LBA High	Specified in iVDR/IF							
Device	Specified in iVDR/IF							
Status	Specified in iVDR/IF							

Sector Count register -

M0 shall be set to 1b if functions related to UT mode are implemented in this Storage Device. MCN_M0 shall be set to the number of Channels which this Storage Device can open in parallel.

M1 shall be set to 1b if functions related to BT mode are implemented in this Storage Device. MCN_M1 shall be always set to 000b, which means that only one Channel is allowed to open when a Channel is opened in BT mode.

6.2 SAFIA UT feature set subcommands

In the following section, detail of subcommand included in SAFIA UT feature set is described. The subcommands included in the feature set are executable only when a Channel is opened in UT mode.

This feature set is subordinate feature set of iVDR Qualified Access feature set in the sense that the feature set cannot be implemented unless iVDR Qualified Access feature set is implemented in the Storage Device.

6.2.1 Subcommands derived from READ QUALIFIED

Protocol is PIO data in.

6.2.1.1 GET DEVICE CLASS CERTIFICATE

6.2.1.1.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz				DCCN			
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit6 shall be set to 1b. Bit7, bit5, bit4 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

LBA Low register -

DCCN shall be set to the number of Device Class Certificate to be transferred to the Host Interface Unit. The number is specified with a value from 000b to 111b. If DCCN is set to 000b by the Host Interface Unit, a Device Class Certificate identified by IDCC1 in Installed Device Class List of GET SAFIA FEATURES UT information is transferred to the Host Interface Unit. The parameter value 001b corresponds to IDCC2 in Installed Device Class List of GET SAFIA FEATURES UT information, and the others correspond similarly.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.1.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.1.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the

execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) A valid Device Class Certificate is not installed in an area pointed by the number which the Host Interface Unit specified as DCCN.
- 6) Transferred Sector Count specified by the Host Interface Unit differs from 01h.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.1.4 Data to be transferred to the Host Device

GET DEVICE CLASS CERTIFICATE information of which size is one sector is set into the Data register. The structure is shown in Table 6.1. In the information, a Device Class Certificate installed in the Storage Device is included; $C(K_r, KP_{dc[l]})$. The structure of the data is described as Open_Connection in SAFIA/PDS2.

Table 6.1 GET DEVICE CLASS CERTIFICATE information

BP	Length	Descriptions
0	N (from 326 to 390)	Open_Connection
N	$512 - N$	Filled with zeros

6.2.1.1.5 Prerequisites

DRDY set to 1b.

6.2.1.1.6 Description

After receiving this subcommand, the Storage Interface Unit sets the Device Class Certificate $C(K_r, KP_{dc[l]})$ installed in the Storage Device into the Data register.

This subcommand is allowed to execute for the Storage Device in any state if a Channel specified with the Channel Identifier has been opened in UT mode. If the Storage Interface Unit

receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Connection Stage. After that, the Storage Device turns to Inceptive Device until the Storage Interface Unit receives one of the following subcommands in the Channel, namely VERIFY DEVICE CLASS CERTIFICATE or SEARCH TRANSACTION LOG UT RECONNECTION and the Storage Module completes the processes related to the subcommands.

6.2.1.2 GET INCEPTIVE SESSION KEY UT CONNECTION

6.2.1.2.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	0	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	Transferred Sector Number							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			TSU
Command	ABh							

Feature register -

Bit7 and bit3 shall be set to 1b. Bit6 to bit4 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred.

LBA Low register -

Transferred Sector Number shall be set to a number of the sector to be transferred. When TSU is set to 1b and this subcommand is issued iteratively in order to transfer all objective data, Transferred Sector Number shall be set to i or $i + 1$, where i is set into this register on the previous issuance by the Host Interface Unit. Moreover, initial value of i is set to 00h in this case. When TSU is set to 0b, Transferred Sector Number shall be set to 00h.

Device register -

DEV shall specify the selected Storage Device.

TSU shall be set to 1b if the unit of sectors to be transferred is one. On the other hand, TSU shall be set to 0b if the whole data is transferred all at once.

6.2.1.2.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.2.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	ISC	ITSN	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ISC shall be set to 1b if Transferred Sector Count is illegal.

ITSN shall be set to 1b if Transferred Sector Number is illegal.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Number specified by the Host Interface Unit is not appropriate.
- 6) Transferred Sector Count specified by the Host Interface Unit differs from whether the size of the data prepared in Buf.UPTU if TSU is set to 1b or one if TSU is set to 0b. The length of the data prepared in Buf.UPTU depends on the length of RDCL_[i]. The length of RDCL_[i] is noticed to the Host Interface Unit in GET SAFIA FEATURES UT information.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.2.4 Data to be transferred to the Host Device

GET INCEPTIVE SESSION KEY UT CONNECTION information of which size is SectorNumber(N) sectors or one sector is set into the Data register. The size is determined in accordance with the values of TSU. The structure is shown in Table 6.2. In the information, a Session Key generated in the Storage Module on Connection Stage is included; $E(K_{ch}, E(KP_{dc[P]}, K_{s[l]} || KP_{d[l]} || MVU_{[l]} || RDCL_{[l]}))$. The structure of the data is described as Inceptive_Session in SAFIA/PDS2.

Table 6.2 GET INCEPTIVE SESSION KEY UT CONNECTION information

BP	Length	Descriptions
0	N	Inceptive_Session
N	$512 \times \text{SectorNumber}(N) - N$	Filled with zeros

6.2.1.2.5 Prerequisites

DRDY set to 1b.

6.2.1.2.6 Description

After receiving this subcommand, the Usage Pass Transfer Unit in the Storage Device prepares SectorNumber(N) sectors data including a Session Key $K_{s[l]}$, generated in the Storage Module, Device Public Key $KP_{d[l]}$ and Revoked Device Class List $RDCL_{[l]}$ which are installed or recorded in the Storage Device. If TSU is set to 0b, the prepared data is set into Data register all at once. If TSU is set to 1b, the prepared data is set into Data register one sector at a time. $K_{s[l]}$ and $KP_{d[l]}$ are doubly encrypted with $K_{ch[P]}$ and $KP_{dc[P]}$, meanwhile, the Revoked Device Class List is encrypted with $K_{ch[P]}$ only. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating a Session Key $K_{s[l]}$, which is shared in Connection Stage.
- (2) Concatenating $K_{s[l]}$ with $KP_{d[l]}$ installed in itself.
- (3) Encrypting the concatenated data with $KP_{dc[P]}$.
- (4) Concatenating $RDCL_{[l]}$ recorded in the Storage Device with the encrypted data $E(KP_{dc[P]}, K_{s[l]} || KP_{d[l]} || MVU_{[l]})$.
- (5) Encrypting the concatenated data $E(KP_{dc[P]}, K_{s[l]} || KP_{d[l]} || MVU_{[l]} || RDCL_{[l]})$ with $K_{ch[P]}$.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) after PUT PRIMAL CHALLENGE KEY UT CONNECTION or GET INCEPTIVE SESSION KEY UT CONNECTION (this subcommand itself) was executed on

Connection Stage in the Channel.

6.2.1.3 GET INCEPTIVE SESSION KEY UT TRANSFER

6.2.1.3.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	1	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit7 and bit5 shall be set to 1b. Bit6, bit4 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.3.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.3.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.3.4 Data to be transferred to the Host Device

GET INCEPTIVE SESSION KEY UT TRANSFER information of which size is one sector is set into the Data register. The structure is shown in Table 6.3. In the information, a Session Key generated in the Storage Module on Transfer Stage is included; UPID || E(K_{s[P]}, E(K_{s[|]n}, K_{s[|]n+1})), where K_{s[|]n} is the Session Key generated in the Storage Module most recently. The structure of the data is described as Transfer_Session in SAFIA/PDS2.

Table 6.3 GET INCEPTIVE SESSION KEY UT TRANSFER information

BP	Length	Descriptions
0	86	Transfer_Session
86	426	Filled with zeros

6.2.1.3.5 Prerequisites

DRDY set to 1b.

6.2.1.3.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Session Key $K_{s[[]]n+1}$ generated in the Storage Module into the Data register. $K_{s[[]]n+1}$ is doubly encrypted with $K_{s[[]]n}$ and $K_{s[P]}$.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) after CREATE INCEPTIVE DEVICE SESSION KEY UT TRANSFER or GET INCEPTIVE SESSION KEY UT TRANSFER (this subcommand itself) was executed on Transfer Stage in the Channel.

6.2.1.4 GET MASKED USAGE PASS

6.2.1.4.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	1	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit6 and bit4 shall be set to 1b. Bit7, bit5 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred. A value of 00h specifies that 256 sectors are to be transferred.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.4.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating the subcommand completion.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.4.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from the number of sectors for the objective Usage Passes existing in Buf.UPTU.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.4.4 Data to be transferred to the Host Device

GET MASKED USAGE PASS information of which size is N sectors is set into the Data register. The structure is shown in Table 6.4. In the information, Usage Passes are included and CIC in the Usage Pass is filled with zeros. The structure of a Usage Pass is described as Masked_UsagePass in SAFIA/PDS2.

Table 6.4 GET MASKED USAGE PASS information

BP	Length	Descriptions
0	345	Masked_UsagePass (1)
345	167	Filled with zeros
512	345	Masked_UsagePass (2)
857	167	Filled with zeros
		Repetition of 1 sector unit where Masked_UsagePass are Included

6.2.1.4.5 Prerequisites

DRDY set to 1b.

6.2.1.4.6 Description

After receiving this subcommand, the Storage Interface Unit sets the information of the Usage Pass that exists in the Buf.UPTU as the GET MASKED USAGE PASS information into the Data register.

If the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS to Buf.QSTC is “Not Exist” or “Invalid”, up_masked field of Masked_UsagePass is filled with zeros.

If the Host Interface Unit sets N into Sector Count register when N Usage Passes exist in Buf.UPTU, N sector data is transferred to the Host Interface Unit.

This subcommand is allowed for the Storage Device to execute after READ USAGE PASS is executed on UP Inquiry Stage in the Channel, then the Storage Device may be whether Primal Device or Inceptive Device.

6.2.1.5 GET PRIMAL CHALLENGE KEY UT CONNECTION

6.2.1.5.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz				DCCN			
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit7 shall be set to 1b. Bit6 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

LBA Low register -

DCCN shall be set to the number of Device Class Certificate to be transferred to the Host Interface Unit. The number is specified with a value from 000b to 111b. If DCCN is set to 000b by the Host Interface Unit, a Device Class Certificate identified by IDCC1 in Installed Device Certificate List of GET SAFIA FEATURES UT information is transferred to the Host Device. The parameter value 001b corresponds to IDCC2 in Installed Device Class List of GET SAFIA FEATURES UT information, and the others correspond similarly.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.5.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.5.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) A valid Device Class Certificate is not installed in an area pointed by the number which the Host Interface Unit specified as DCCN.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.5.4 Data to be transferred to the Host Device

GET PRIMAL CHALLENGE KEY UT CONNECTION information of which size is 512-byte is set into the Data register. The structure is shown in Table 6.5. In the information, a Challenge Key generated in the Storage Device on Connection Stage is included; $E(KP_{dc[P]}, K_{ch[P]}) || C(K_r, KP_{dc[P]})$. The structure of the data is described as Primal_Challenge in SAFIA/PDS2.

Table 6.5 GET PRIMAL CHALLENGE KEY UT CONNECTION information

BP	Length	Descriptions
0	N (from 428 to 492)	Primal_Challenge
N	$512 - N$	Filled with zeros

6.2.1.5.5 Prerequisites

DRDY set to 1b.

6.2.1.5.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Challenge Key $K_{ch[P]}$ generated in the Storage Device with Device Class Certificate $C(K_r, KP_{dc[P]})$ installed in the Storage Device into the Data register. $K_{ch[P]}$ is encrypted with $KP_{dc[I]}$ only. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating a Challenge Key $K_{ch[P]}$.
- (2) Encrypting the data with $KP_{dc[I]}$.
- (3) Concatenating the encrypted data $E(KP_{dc[I]}, K_{ch[P]})$ with $C(K_r, KP_{dc[P]})$.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after VERIFY DEVICE CLASS CERTIFICATE or GET PRIMAL CHALLENGE KEY UT CONNECTION (this subcommand itself) was executed on Connection Stage in the Channel.

6.2.1.6 GET PRIMAL SESSION KEY UT CONNECTION

6.2.1.6.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	1	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	Transferred Sector Number							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			TSU
Command	ABh							

Feature register -

Bit7 and bit4 shall be set to 1b. Bit6, bit5 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred.

LBA Low register -

Transferred Sector Number shall be set to a number of the sector to be transferred. When TSU is set to 1b and this subcommand is issued iteratively in order to transfer all objective data, Transferred Sector Number shall be set to i or $i + 1$, where i is set into this register on

the previous issuance by the Host Interface Unit. Moreover, initial value of *i* is set to 00h in this case. When TSU is set to 0b, Transferred Sector Number shall be set to 00h.

Device register -

DEV shall specify the selected Storage Device.

TSU shall be set to 1b if the unit of sectors to be transferred is one. On the other hand, TSU shall be set to 0b if the whole data is transferred all at once.

6.2.1.6.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.6.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	ISC	ITSN	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ISC shall be set to 1b if Transferred Sector Count is illegal.

ITSN shall be set to 1b if Transferred Sector Number is illegal.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Number specified by the Host Interface Unit is not appropriate.
- 6) Transferred Sector Count specified by the Host Interface Unit differs from whether the size of the data prepared in Buf.UPTU if TSU is set to 1b or one if TSU is set to 0b. The length of the data prepared in Buf.UPTU depends on the length of RDCL_[P]. The length of RDCL_[P] is noticed to the Host Device in GET SAFIA FEATURES UT information.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.6.4 Data to be transferred to the Host Device

GET PRIMAL SESSION KEY UT CONNECTION information of which size is SectorNumber(*N*) sectors or one sector is set into the Data register. The size is determined in accordance with the values of TSU. The structure is shown in Table 6.6. In the information, a Session Key generated the Storage Module on Connection Stage is included; $E(KP_{d[I]})$, $E(K_{s[I]})$, $K_{s[P]} \parallel MVU_{[P]} \parallel RDCL_{[P]}$. The structure of the data is described as Primal_Session in SAFIA/PDS2.

Table 6.6 GET PRIMAL SESSION KEY UT CONNECTION information

BP	Length	Descriptions
0	<i>N</i>	Primal_Session
<i>N</i>	$512 \times \text{SectorNumber}(N) - N$	Filled with zeros

6.2.1.6.5 Prerequisites

DRDY set to 1b.

6.2.1.6.6 Description

After receiving this subcommand, the Usage Pass Transfer Unit in the Storage Device prepares SectorNumber(*N*) sectors data including a Session Key $K_{s[P]}$ generated in the Storage Module with Revoked Device Class List recorded RDCL_[P] recorded in the Storage Device. If TSU is set to 0b, the prepared data is set into Data register all at once. If TSU is set to 1b, the prepared data is set

into Data register 1b sector at a time. Then, the $RDCL_{[P]}$ is concatenated if the issue date of $RDCL_{[I]}$ sent from the Inceptive Device is older than that recorded in the Storage Device. $K_{s[P]}$ is doubly encrypted with $K_{s[I]}$ and $KP_{d[I]}$, meanwhile, the $RDCL_{[P]}$ is encrypted with $KP_{d[I]}$ only. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating a Session Key $K_{s[P]}$, which is shared in Connection Stage.
- (2) Encrypting the $K_{s[P]}$ with $K_{s[I]}$.
- (3) Concatenate $RDCL_{[P]}$ with the encrypted data $E(K_{s[I]}, K_{s[P]} || MVU_{[P]})$ if $RDCL_{[I]}$ has already been verified and the issue date of $RDCL_{[I]}$ is older than the issue date of $RDCL_{[P]}$.
- (4) Encrypting the concatenated data $E(K_{s[I]}, K_{s[P]} || MVU_{[P]} || RDCL_{[P]})$ with $KP_{d[I]}$.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after PUT INCEPTIVE SESSION KEY UT CONNECTION or GET PRIMAL SESSION KEY UT CONNECTION (this subcommand itself) was executed on Connection Stage in the Channel.

6.2.1.7 GET PRIMAL SESSION KEY UT RECONNECTION

6.2.1.7.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	1	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit7, bit4 and bit3 shall be set to 1b. Bit6 and bit5 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.7.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.7.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.7.4 Data to be transferred to the Host Device

GET PRIMAL SESSION KEY UT RECONNECTION information of which size is one sector is set into the Data register. The structure is shown in Table 6.7. In the information, a Session Key generated in the Storage Module on Reconnection Stage is included; UPID || E(KP_{d[I]TL}, E(K_{s[I]TL}, K_{s[P]})). The structure of the data is described as Recovery_Connection in SAFIA/PDS2.

Table 6.7 GET PRIMAL SESSION KEY UT RECONNECTION information

BP	Length	Descriptions
0	151	Recovery_Connection
151	361	Filled with zeros

6.2.1.7.5 Prerequisites

DRDY set to 1b.

6.2.1.7.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Session Key K_{s[P]} generated in the Storage Module into the Data register. K_{s[P]} is doubly encrypted with K_{s[I]TL} and KP_{d[I]TL} which are fetched from Transaction Log in the Usage Pass Transfer Unit in the Storage Device. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating K_{s[P]} which is shared in Reconnection Stage.
- (2) Encrypting K_{s[P]} with the retrieved K_{s[I]TL} and KP_{d[I]TL} as the result of the execution of SEARCH TRANSACTION LOG UT RECONNECTION.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after SEARCH TRANSACTION LOG UT RECONNECTION or GET PRIMAL SESSION KEY UT RECONNECTION (this subcommand itself) was executed on Reconnection Stage in the Channel.

6.2.1.8 GET SAFIA FEATURES UT

6.2.1.8.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	0	0	0	0	CHID		
Sector Count	fz							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit7 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.8.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.8.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.8.4 Data to be transferred to the Host Device

GET SAFIA FEATURES UT information of which size is one sector is set into the Data register.
 The structure is shown in Table 6.8.

Table 6.8 GET SAFIA FEATURES UT information

BP	Length	Descriptions
0	64	Installed Device Class Certificate List
64	1	SAFIA Device Interface Version
65	2	Reference Completion Time [GET DEVICE CLASS CERTIFICATE]
67	2	Reference Completion Time [GET INCEPTIVE SESSION KEY UT CONNECTION]
69	2	Reference Completion Time [GET INCEPTIVE SESSION KEY UT TRANSFER]
71	2	Reference Completion Time [GET PRIMAL CHALLENGE KEY UT CONNECTION]
73	2	Reference Completion Time [GET PRIMAL SESSION KEY UT CONNECTION]
75	2	Reference Completion Time [GET PRIMAL SESSION KEY UT RECONNECTION]
77	2	Reference Completion Time [GET MASKED USAGE PASS for one Usage Pass]
79	2	Reference Completion Time [GET TRANSACTION LOG EXTERNAL]
81	2	Reference Completion Time [GET TRANSACTION STATUS UT RECOVERY]
83	2	Reference Completion Time [GET USAGE PASS]
85	2	Reference Completion Time [ENCRYPT USAGE PASS COPY]
87	2	Reference Completion Time [ENCRYPT USAGE PASS MOVE]
89	2	Reference Completion Time [ENCRYPT USAGE PASS PLAY]
91	2	Reference Completion Time [READ USAGE PASS (for one Usage Pass)]
93	2	Filled with zeros (0000h)
95	2	Reference Completion Time [CREATE INCEPTIVE SESSION KEY UT TRANSFER]
97	2	Reference Completion Time [PUT INCEPTIVE SESSION KEY UT CONNECTION]
99	2	Reference Completion Time [PUT INCEPTIVE SESSION KEY UT TRANSFER]
101	2	Reference Completion Time [PUT PRIMAL CHALLENGE KEY UT CONNECTION]
103	2	Reference Completion Time [PUT PRIMAL SESSION KEY UT CONNECTION]
105	2	Reference Completion Time [PUT PRIMAL SESSION KEY UT RECONNECTION]
107	2	Reference Completion Time [PUT USAGE PASS]
109	2	Reference Completion Time [SEARCH TRANSACTION LOG UT RECONNECTION]

111	2	Reference Completion Time [SEARCH USAGE PASS UT RECOVERY]
113	2	Reference Completion Time [VERIFY DEVICE CLASS CERTIFICATE]
115	2	Reference Completion Time [VERIFY TRANSACTION STATUS UT RECOVERY]
117	6	Start LBAQ of Qualified Storage
123	6	End LBAQ of Qualified Storage
129	1	Recordable Entry Number of Transaction Log
130	2	Recorded Size of Revoked Device Class List
132	2	Maximum Transferred Sector Count
134	378	Filled with zeros

- Installed Device Class Certificate List

Installed Device Class Certificate List indicates the information of Device Class Certificates installed in the Storage Device. Installed Device Class Certificate List consists of eight entries where the size of one entry is eight bytes. The structure of Installed Device Class Certificate is described in Table 6.9

Table 6.9 Structure of Installed Device Class Certificate List

BP EN	0	1	2	3	4	5	6	7
1	IDCC1							
2	IDCC2							
...	...							
8	IDCC8							

EN: Entry Number

IDCC1 shall be set to 44 52 56 00 00 00 00 00h, which is DRV in the character defined in ISO/IEC646. IDCC2 to IDCC8 shall be set to 00 00 00 00 00 00 00 00h.

- SAFIA Device Interface Version

Table 6.10 Structure of SAFIA Device Interface Version

7	6	5	4	3	2	1	0
Version							

SAFIA Device Interface Version shall be set to 13h by the Storage Device.

- Reference Completion Time (BP 65 to 116)

Reference Completion Time indicates the reference time in mili second unit to complete the subcommand described in the following bracket. If a Reference Completion Time is 0000h, Reference Completion Time is invalid.

- Start LBAQ of Qualified Storage

Start LBAQ of Qualified Storage indicates a LBAQ to designate the first sector of Qualified Storage.

- End LBAQ of Qualified Storage

End LBAQ of Qualified Storage indicates a LBAQ to designate the final sector of Qualified Storage.

- Recordable Entry Number of Transaction Log
 Recordable Entry Number of Transaction Log indicates a maximum number of entries of Transaction Log which the Storage Device can record.
- Recorded Size of Revoked Device Class List
 Recorded Size of Revoked Device Class List indicates the size of total area where Revoked Device Class List is actually recorded in the Storage Device in byte unit. If the recorded Revoked Device Class List is updated, the value shall be modified to correspond to the length in the Storage Device.
- Maximum Transferred Sector Count
 Maximum Transferred Sector Count indicates a number of sectors which the Storage Device can process as reception of one READ USAGE PASS and one PUT USAGE PASS.

6.2.1.8.5 Prerequisites

DRDY set to one.

6.2.1.8.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data in which various parameters are included as described in Table 6.8 into the Data register.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in UT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit remain unchanged.

6.2.1.9 GET TRANSACTION LOG EXTERNAL

6.2.1.9.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	1	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	Transferred Sector Number							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			TSU
Command	ABh							

Feature register -

Bit6 and bit5 shall be set to one. Bit7, bit4 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred. A value of 00h

specifies that 256 sectors are to be transferred.

LBA Low register -

Transferred Sector Number shall be set to a number of the sector to be transferred. When TSU is set to 1b and this subcommand is issued iteratively in order to transfer all objective data, Transferred Sector Number shall be set to i or $i + 1$, where i is set into this register on the previous issuance by the Host Interface Unit. Moreover, initial value of i is set to 00h in this case. When TSU is set to 0b, Transferred Sector Number shall be set to 00h.

Device register -

DEV shall specify the selected Storage Device.

TSU shall be set to 1b if the unit of sectors to be transferred is one. On the other hand, TSU shall be set to 0b if the whole data is transferred all at once.

6.2.1.9.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to one.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.9.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	ISC	ITSN	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the

execution of this subcommand.

ISC shall be set to 1b if Transferred Sector Count is illegal.

ITSN shall be set to 1b if Transferred Sector Number is illegal.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from whether the size of all entries of Transaction Log or one. The number of entries of Transaction Log which the Usage Pass Transfer Unit in the Storage Device can record is noticed to the Host Device in GET SAFIA FEATURES UT information.
- 6) No valid entry of Transaction Log exists.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.9.4 Data to be transferred to the Host Device

GET TRANSACTION LOG EXTERNAL information of which size is N is set into the Data register if TSU is set to 0b. Here, N is a value which the Host Interface Unit acquires as “Recordable number of Transaction Logs” in GET SAFIA FEATURES UT information. However, if TSU is set to 1b, a 512-byte unit of GET TRANSACTION LOG EXTERNAL information is set into the Data register at a time. The structure of the GET TRANSACTION LOG EXTERNAL information is shown in Table 6.11. In this table, it is supposed that M TransactionLog_External is recorded in the Storage Device. The structure of a Transaction Log is described as TransactionLog_External in SAFIA/PDS2. Note that up_location field of TransactionLog_External consists of two parts. The size of the first part is 6-byte and LBAQ is recorded into the field for each purpose. The size of the second part is 2-byte and Transferred Sector Count is recorded into the field for each purpose.

Table 6.11 GET TRANSACTION LOG EXTERNAL information

BP	Length	Field
0	145	TransactionLog_External (1)
145	367	Filled with zeros
512	145	TransactionLog_External (2)
657	367	Filled with zeros
		Repetition of 512-byte unit where a TransactionLog_External is included, End of the BP is $512 \times M - 1$
$512 \times M$	$512 \times (N - M)$	Filled with zeros

6.2.1.9.5 Prerequisites

DRDY set to 1b.

6.2.1.9.6 Description

After receiving this subcommand, the Usage Pass Transfer Unit in the Storage Device prepares N sector data in which M TransactionLog_Externals are included as described in Table 6.11 in the Buf.UPTU. If $M < N$, $512 \times (N - M)$ -byte are filled with zero as described in Table 6.11. If TSU is set to 0b, the prepared data is set into Data register all at once. If TSU is set to 1b, a 512-byte unit of the prepared data is set into Data register at a time.

When the Storage Interface Unit sets entire Transaction Log into the Data register, the log data is placed from the information recorded in the newest entry to the information recorded in the oldest entry. Then, the fields of which attribute is internal are overwritten with zeros.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in UT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit remains unchanged.

6.2.1.10 GET TRANSACTION STATUS UT RECOVERY

6.2.1.10.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	1	1	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit7, bit5, bit4 and bit3 shall be set to 1b. Bit6 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.10.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.10.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the

data to be set into the Data register.

5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.10.4 Data to be transferred to the Host Device

GET TRANSACTION STATUS UT RECOVERY information of which size is one sector is set into the Data register. The structure is shown in Table 6.12. In the information, Usage Pass Identifier, Session Status, Usage Pass Status and a Hash value, which is calculated from the Usage Pass Identifier, the Session Status, the Usage Pass Status and two Session Keys, are included. The data is called Transaction Status. The structure of the data is described as Transaction_Status in SAFIA/PDS2.

Table 6.12 GET TRANSACTION STATUS UT RECOVERY information

BP	Length	Field
0	75	Transaction_Status
75	437	Filled with zeros

6.2.1.10.5 Prerequisites

DRDY set to 1b.

6.2.1.10.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Transaction Status into the Data register.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) after SEARCH USAGE PASS UT RECOVERY or GET TRANSACTION STATUS UT RECOVERY (this subcommand itself) was executed on Recovery Stage in the Channel.

6.2.1.11 GET USAGE PASS

6.2.1.11.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	1	0	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit7, bit5 and bit3 shall be set to 1b. Bit6 and bit4 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.1.11.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.1.11.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the data to be set into the Data register.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.1.11.4 Data to be transferred to the Host Device

GET USAGE PASS information of which size is one sector is set into the Data register. The structure is shown in Table 6.13. In the information, a Usage Pass, Action Indicator and Checksum are included; E(*KP_{d[1]}, E(K_{s[1]}, UP || AI || CKS)). The structure of the data is described as Transfer_UsagePass in SAFIA/PDS2.

Table 6.13 GET USAGE PASS information

BP	Length	Field
0	372	Transfer_UsagePass
372	140	Filled with zeros

6.2.1.11.5 Prerequisites

DRDY set to 1b.

6.2.1.11.6 Description

After receiving this subcommand, the Storage Module processes the following if the execution of the subcommand which had been previously received (ENCRYPT USAGE PASS COPY/MOVE/PLAY) has completed.

- (1) Updating Session Status of Transaction Log to “SC”.
- (2) Modifying the Control Count of the original Usage Pass (not duplicated one) in Buf.QSTC to comply with the description in section 7.3 of SAFIA/PDS1.
- (3) Overwriting Access Condition for Storage Module of the Usage Pass which exists in Qualified Storage with the Access Condition for Storage Module of the original Usage Pass which exists in Buf.QSTC for Copy or Play. Invalidating the Usage Pass which exists in Qualified Storage for Move.
- (4) Setting one sector data including a Usage Pass, Action Indicator and Checksum into the Data register.

If the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS is “Not Exist” or “Invalid”, Transfer_UsagePass field is filled with zeros and step (2) and (3) are not executed.

This subcommand is allowed for the Storage Interface Unit to execute (1) when the Storage Device is Primal Device, and (2) after ENCRYPT USAGE PASS COPY or MOVE or PLAY was executed on Transfer Stage in the Channel. Iterative execution of the subcommand is not allowed. When the subcommand execution is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to a particular state which is for “Usage Pass movement is completed”.

6.2.2 Subcommands derived from SET QUALIFIED

Protocol is non data.

6.2.2.1 CHECK EXECUTION STATUS

6.2.2.1.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	0	0	CHID		
Sector Count	fz							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	AAh							

Feature register -

Bit7 and bit6 shall be set to 1b. Bit5 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Device register -

DEV shall specify the selected Storage Device.

6.2.2.1.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.2.1.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	IDC	VDCC	TLE	NTL	ABRT	NRDY	VDSW
Sector Count	na						IKH	VDSR
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

IDC indicates the results of collation of Usage Pass Identifier. If the Usage Pass Identifier of the Usage Pass which is fetched from Qualified Storage, retrieved or to be recovered differs from the received one, IDC shall be set to 1b. For any other case, IDC shall be set to 0b.

VDCC indicates the validity of the received Device Class Certificate if this subcommand is received just after the execution of VERIFY DEVICE CLASS CERTIFICATE and PUT PRIMAL CHALLENGE KEY UT CONNECTION. If the received Device Class Certificate is revoked one, which is turned out by the collation of Revoked Device Class List recorded in itself, VDCC shall be set to 1b. For any other case, VDCC shall be set to 0b.

TLE indicates the existence of Transaction Log if this subcommand is received just after the execution of PUT PRIMAL SESSION KEY UT RECONNECTION, SEARCH TRANSACTION LOG UT RECONNECTION, SEARCH USAGE PASS UT RECOVERY and VERIFY TRANSACTION STATUS UT RECOVERY. If a Transaction Log, which includes a Usage Pass Identifier which coincides with the one that the Host Interface Unit specified on the subcommands listed above, does not exist, TLE shall be set to 1b. For any other case, TLE shall be set to 0b.

NTL indicates the existence of a Transaction Log. If no valid entry of Transaction Log exist, NTL shall be set to 1b. For any other case, NTL shall be set to 0b.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.

NRDY shall be set to 1b if the previously received subcommand is not completed.

VDSW indicates the validity of the structure of the received data if this subcommand is received just after the execution of all subcommands derived from WRITE QUALIFIED. If a Storage Device receives these subcommands, it is necessary to verify or decrypt the received data. When the structure of the obtained data is invalid, VDSW shall be set to 1b.

For any other case, VDSW shall be set to 0b. This flag corresponds to VDS in version 1.0. IKH indicates the result of verification of Transaction Status at the Primal Device if this subcommand is received just after the execution of VERIFY TRANSACTION STATUS UT RECOVERY. If the verification fails, IKH shall be set to 1b. For any other case, IKH shall be set to 0b.

VDSR indicates the validity of the structure of the data placed in the Buf.QSTC by fetching Usage Pass from Qualified Storage or in the Buf.UPTU by extracting RDCL, KP_d and so forth to transfer to the Host Device by the subcommands derived from READ QUALIFIED. When the structure of the data is invalid, VDSR shall be set to 1b. For any other case, VDSR shall be set to 0b.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.2.1.4 Data to be transferred from/to the Host Device

Non data.

6.2.2.1.5 Prerequisites

DRDY set to 1b.

6.2.2.1.6 Description

After receiving this subcommand, the Storage Interface Unit sets the state of the execution of subcommand which the Storage Interface Unit previously received into Command Block register.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in UT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit remains unchanged.

6.2.2.2 ENCRYPT USAGE PASS COPY

6.2.2.2.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	1	0	CHID		
Sector Count	fz							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	AAh							

Feature register -

Bit6 and bit4 shall be set to 1b. Bit7, bit5 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Device register -

DEV shall specify the selected Storage Device.

6.2.2.2.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.2.2.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	INA	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

WP shall be set to 1b if modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE with bit 2 of PL set to 1b.

INA shall be set to 1b if the Inceptive Device is not allowed to receive the objective Usage Pass recorded in the Storage Device, which is determined through the comparison of Acceptable Usage Pass Type Map in Device Class Certificate sent from Inceptive Device and Usage Pass Type of the objective Usage Pass.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the created data if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The number of Usage Pass existing in Buf.UPTU is not one because plural or no Usage Passes were fetched from Qualified Storage by READ USAGE PASS that had been previously executed.
- 6) INA in the Error register is set to 1b.
- 7) WP in the Error register is set to 1b.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.2.2.4 Data to be transferred from/to the Host Device

Non data.

6.2.2.2.5 Prerequisites

DRDY set to 1b.

6.2.2.2.6 Description

When the Storage Interface Unit receives this subcommand, the Usage Pass Transfer Unit in the Storage Device processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Comparing the Acceptable Usage Pass Type Map sent from the Inceptive Device and the Usage Pass Type of the objective Usage Pass and determine whether output of the Usage Pass is allowed or not. The comparison shall be executed conforming to the description provided in section 7.1.3 of SAFIA/PDS1. If output of the Usage Pass is not allowed, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Duplicating a Usage Pass which has already been fetched from Qualified Storage and existed in Buf.QSTC.
- (3) Modifying the Control Count of the duplicated Usage Pass to comply with the description of Usage Pass Copy in section 7.3 of SAFIA/PDS1.
- (4) Moving the Usage Pass described in (3) to Buf.UPTU and concatenating the Action Indicator (01h) with it.
- (5) Calculating Checksum from the Usage Pass and Action Indicator and concatenate it with "Usage Pass || Action Indicator".
- (6) Encrypting the concatenated data "Usage Pass || Action Indicator || Checksum" with $K_{s[|I]}$ and $*KP_{d[|P]}$.

If the objective Usage Pass in Buf.QSTC was invalid (namely, the Usage Pass was invalid in Qualified Storage), the step (1) to step (6) are not executed.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after PUT INCEPTIVE SESSION KEY UT TRANSFER or ENCRYPT USAGE PASS MOVE or ENCRYPT USAGE PASS PLAY or ENCRYPT USAGE PASS COPY (this subcommand itself) was executed on Transfer Stage in the Channel.

6.2.2.3 ENCRYPT USAGE PASS MOVE

6.2.2.3.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	1	1	CHID		
Sector Count	fz				Output UP AC _s COUNT			
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	AAh							

Feature register -

Bit6, bit4 and bit3 shall be set to 1b. Bit7 and bit5 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Output UP AC_s COUNT shall be set to a number less than COUNT of the Usage Pass in the Storage Device if FM of the Usage Pass is 01b (Copy Count) and the COUNT is less than Fh. Output UP AC_s COUNT shall be set to 0h if FM is not 01b, or FM is 01b and COUNT is Fh. COUNT of the Usage Pass to be transferred is set to the specified Output UP AC_s COUNT unless the value is 0h. When Output UP AC_s COUNT is 0h, COUNT of the Usage Pass to be transferred is set to COUNT of the Usage Pass in the Storage Device.

Device register -

DEV shall specify the selected Storage Device.

6.2.2.3.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.2.3.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	INA	IC	IFM	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

INA shall be set to 1b if the Inceptive Device is not allowed to receive the objective Usage Pass recorded in the Storage Device, which is determined through the comparison of Acceptable Usage Pass Type Map in Device Class Certificate sent from Inceptive Device and Usage Pass Type of the objective Usage Pass.

IC shall be set to 1b if Output UP AC_s COUNT is greater than COUNT (of the Usage Pass existing in the Buf.QSTC) – 1h when FM is 01b and COUNT is less than Fh.

IFM shall be set to 1b if Output UP AC_s COUNT is not 0h and FM of the Usage Pass existing in the Buf.QSTC is not 01b (Copy Count).

WP shall be set to 1b if modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE with bit 1 of PL set to 1b.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the created data if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The number of Usage Pass existing in Buf.UPTU is not one because plural or no Usage Passes were fetched from Qualified Storage by READ USAGE PASS that had been previously executed.
- 6) INA in the Error register is set to 1b.
- 7) WP in the Error register is set to 1b.
- 8) IC in the Error register is set to 1b
- 9) IFM in the Error register is set to 1b.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.2.3.4 Data to be transferred from/to the Host Device

Non data.

6.2.2.3.5 Prerequisites

DRDY set to 1b.

6.2.2.3.6 Description

When the Storage Interface Unit receives this subcommand, the Usage Pass Transfer Unit in the Storage Device processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Comparing the Acceptable Usage Pass Type Map sent from the Inceptive Device and the Usage Pass Type of the objective Usage Pass and determine whether output of the Usage Pass is allowed or not. The comparison shall be executed conforming to the description provided in section 7.1.3 of 466HSAFIA/PDS1. If output of the Usage Pass is not allowed, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Duplicating a Usage Pass which has already been fetched from Qualified Storage and existed in Buf.QSTC. The newly generated Usage Pass for output and the source Usage Pass for duplication are respectively called as Output Usage Pass and Original Usage Pass in this section.
- (3) Checking MU. If MU is set to 1b, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (4) Modifying the Control Count of the duplicated Usage Pass to comply with the description of Usage Pass MOVE in section 7.3 of SAFIA/PDS1. Especially, when FM and COUNT of the Original Usage Pass is respectively 01b and less than Fh, COUNT of the Original Usage Pass and Output Usage Pass is updated according to the following table. In the table, COUNT_{org} is COUNT of original Usage Pass. Output UP AC_s COUNT shall be less than or equal COUNT_{org} – 1.

Output UP AC _s COUNT	COUNT of Control Count in AC _s	
	Original Usage Pass	Output Usage Pass
0h	- (To be invalidated)	COUNT _{org}
1h, ..., (COUNT _{org} – 1)	COUNT _{org} – (Output UP AC _s COUNT + 1)	Output UP AC _s COUNT
Others	Subcommand execution is aborted	

- (5) Moving the Usage Pass described in (4) to Buf.UPTU and concatenating the Action Indicator (02h) with it.
- (6) Calculating Checksum from the Usage Pass and Action Indicator and concatenate it with “Usage Pass || Action Indicator”.
- (7) Encrypting the concatenated data “Usage Pass || Action Indicator || Checksum” with $K_{s[j]}$ and $*KP_{d[j]}$.

If the objective Usage Pass in Buf.QSTC was invalid (namely, the Usage Pass was invalid in Qualified Storage), the step (1) to step (7) are not executed.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after PUT INCEPTIVE SESSION KEY UT TRANSFER or ENCRYPT USAGE PASS COPY or ENCRYPT USAGE PASS PLAY or ENCRYPT USAGE PASS MOVE (this subcommand itself) was executed on Transfer Stage in the Channel.

6.2.2.4 ENCRYPT USAGE PASS PLAY

6.2.2.4.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	0	1	CHID		
Sector Count	fz							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	AAh							

Feature register -

Bit6 and bit3 shall be set to 1b. Bit7, bit5 and bit4 shall be set to 0b.

CHID shall be set to Channel Identifier.

Device register -

DEV shall specify the selected Storage Device.

6.2.2.4.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not

mean the completion of the execution of all the processes associated with this subcommand.
 DRDY shall be set to 1b.
 DF (Device Fault) shall be cleared to 0b.
 DRQ shall be cleared to 0b.
 ERR shall be cleared to 0b.

6.2.2.4.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	INA	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

INA shall be set to 1b if the Inceptive Device is not allowed to receive the objective Usage Pass recorded in the Storage Device, which is determined through the comparison of Acceptable Usage Pass Type Map in Device Class Certificate sent from Inceptive Device and Usage Pass Type of the objective Usage Pass.

WP shall be set to 1b if modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE with bit 0 of PL set to 1b.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module..
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the created data if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The number of Usage Pass existing in Buf.UPTU is not one because plural or no Usage Passes were fetched from Qualified Storage by READ USAGE PASS that had been previously executed.
- 6) INA in the Error register is set to 1b.
- 7) WP in the Error register is set to 1b.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.2.4.4 Data to be transferred from/to the Host Device

Non data.

6.2.2.4.5 Prerequisites

DRDY set to 1b.

6.2.2.4.6 Description

When the Storage Interface Unit receives the subcommand, the Usage Pass Transfer Unit in the Storage Device processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Comparing the Acceptable Usage Pass Type Map sent from the Inceptive Device and the Usage Pass Type of the objective Usage Pass and determine whether output of the Usage Pass is allowed or not. The comparison shall be executed conforming to the description provided in section 7.1.3 of 466HSAFIA/PDS1. If output of the Usage Pass is not allowed, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Duplicating a Usage Pass which has already been fetched from Qualified Storage and existed in Buf.QSTC.
- (3) Modifying the Control Count of the duplicated Usage Pass to comply with the description of Usage Pass PLAY in section 7.3 of SAFIA/PDS1.
- (4) Moving the Usage Pass described in (3) to Buf.UPTU and concatenating the Action Indicator (03h) with the Usage Pass to be transferred.
- (5) Calculating Checksum from the Usage Pass and Action Indicator and concatenate it with "Usage Pass || Action Indicator".
- (6) Encrypting the concatenated data "Usage Pass || Action Indicator || Checksum" with $K_{s[i]}$ and $*K_{d[i]}$.

If the objective Usage Pass in Buf.QSTC was invalid (namely, the Usage Pass was invalid in Qualified Storage), the step (1) to step (6) are not executed.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after PUT INCEPTIVE SESSION KEY UT TRANSFER or ENCRYPT USAGE PASS COPY or ENCRYPT USAGE PASS MOVE or ENCRYPT USAGE PASS PLAY (this subcommand itself) was executed on Transfer Stage in the Channel.

6.2.2.5 READ USAGE PASS

6.2.2.5.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	1	obs	DEV	LBAQ (27:24)			
Command	AAh							

Feature register -

Bit7 shall be set to 1b. Bit6 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Number of sectors to be fetched from Qualified Storage to Buf.QSTC. A value of 00h specifies that 256 sectors are to be read.

LBA Low register -

LBAQ address bits (7:0) shall be set to the register.

LBA Mid register -

LBAQ address bits (15:8) shall be set to the register.

LBA High register -

LBAQ address bits (23:16) shall be set to the register.

Device register [7:4] -

Bit6 shall be set to 1b.

DEV shall specify the selected Storage Device.

Device register [3:0] -

LBAQ address bits (27:24) shall be set to the register.

6.2.2.5.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							VUP
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Sector Count -

VUP shall indicate the validity of Usage Pass fetched by this subcommand. If some invalid Usage Passes are included in the fetched Usage Passes or Usage Passes are not partly included, VUP shall be set to 1b. If all Usage Passes fetched by this subcommand are valid, VUP shall be set to 0b.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.2.5.3 Error outputs

An unrecoverable error encountered during the execution of this subcommand results in the termination of the subcommand. The Command Block registers contain the address of the sector where the first unrecoverable error occurred.

Register	7	6	5	4	3	2	1	0
Error	CP	UNC	na	IDNF	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	na	obs	DEV	LBAQ (27:24)			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

UNC shall be set to 1b if some data to be fetched from Qualified Storage is uncorrectable.

IDNF shall be set to 1b if the specified address is outside of the range where the Host Device may fetch the Usage Passes and subcommand aborted is not returned.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Qualified Storage Controller detects the structure error of the Usage Pass fetched from Qualified Storage if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The value of Transferred Sector Count specified by the Host Interface Unit exceeds Maximum Transferred Sector Count which Storage Interface Unit noticed to the Host Interface Unit in GET SAFIA FEATURES UT information (Table 6.8).

NRDY shall be set to 1b if the previously received subcommand is not completed.

LBA Low, LBA Mid, LBA High, Device [3:0] -

shall be filled with the address of first unrecoverable error.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.2.5.4 Data to be transferred from/to the Host Device

Non data.

6.2.2.5.5 Prerequisites

DRDY set to 1b.

6.2.2.5.6 Description

After receiving this subcommand, the Qualified Storage Controller fetches a Usage Pass from Qualified Storage to Buf.QSTC. Then, the sector size is 1 to 256 is possible as specified in Sector Count register. A sector count of 0 requests 256 sectors. However, if the Host Interface Unit specifies Transferred Sector Count exceeding Maximum Transferred Sector Count (see Table 6.8), the Storage Interface Unit aborts this subcommand execution.

If READ USAGE PASS was executed before executing another READ USAGE PASS, all Usage Passes which were fetched by the previous READ USAGE PASS and exists in Buf.QSTC or Buf.UPTU shall be flushed by the time when another Usage Passes were fetched by another READ USAGE PASS..

This subcommand is allowed for the Storage Device to execute if a Connection has been established between a Primal Device and the Storage Device. This subcommand execution is allowed not only after PUT PRIMAL SESSION KEY UT CONNECTION (end of Connection Stage for Inceptive Device), GET PRIMAL SESSION KEY UT CONNECTION (end of Connection Stage for Primal Device), PUT PRIMAL SESSION KEY UT RECONNECTION (end of Reconnection Stage for Inceptive Device) or GET PRIMAL SESSION KEY UT RECONNECTION (end of Reconnection Stage for Primal Device) but also after CREATE INCEPTIVE SESSION KEY UT TRANSFER (first step of Transfer Stage for Inceptive Device), PUT INCEPTIVE SESSION KEY UT TRANSFER (first step of Transfer Stage for Primal Device) or READ USAGE PASS (first step of UP Inquiry Stage for both Primal Device and Inceptive Device) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within UP Inquiry Stage whether the Storage Device is Primal or Inceptive.

6.2.2.6 WRITE USAGE PASS

This subcommand is obsolete.

6.2.3 Subcommands derived from WRITE QUALIFIED

Protocol is PIO data out.

6.2.3.1 CREATE INCEPTIVE SESSION KEY UT TRANSFER

6.2.3.1.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	1	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7, bit4 and bit3 shall be set to 1b. Bit6 and bit5 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.1.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.1.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register or will be set into the Data register (only if the data to be set in the register was created associated with the reception of this subcommand) if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The length of the data which the Storage Interface Unit actually received is not one sector.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.1.4 Data to be transferred from the Host Device

CREATE INCEPTIVE SESSION KEY UT TRANSFER information of which size is one sector is set into the Data register. The structure is shown in Table 6.14. In the information, a Usage Pass

Identifier is included; UPID. The structure of the data is described as Open_Transfer in SAFIA/PDS2.

Table 6.14 CREATE INCEPTIVE SESSION KEY UT TRANSFER information

BP	Length	Descriptions
0	36	Open_Transfer
36	476	Filled with zeros

6.2.3.1.5 Prerequisites

DRDY set to 1b.

6.2.3.1.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Usage Pass Identifier and is set into the Data register.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Checking the structure of the received data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Creating a Session Key $K_{s[l]n+1}$, which is shared in Transfer Stage.
- (3) Creating an entry of Transaction Log and recording UPID, $K_{s[l]}$ and state of the Transfer Stage ("RP") into each corresponding field of the entry.
- (4) Encrypting the $K_{s[l]}$ with $K_{s[l]n}$ and $K_{s[P]}$, where $K_{s[P]}$ is shared through Connection or Reconnection Stage and $K_{s[l]n}$ was shared most recently through Connection or Reconnection or Transfer Stage in the past.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) if a Connection has been established between the Primal Device and the Storage Device as Inceptive Device. A condition (2) means that the subcommand execution is allowed not only after PUT PRIMAL SESSION KEY UT CONNECTION (end of Connection Stage) or PUT PRIMAL SESSION KEY UT RECONNECTION (end of Reconnection Stage) but also after SEARCH USAGE PASS UT RECOVERY (first step of Recovery Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Transfer Stage.

6.2.3.2 PUT INCEPTIVE SESSION KEY UT CONNECTION

6.2.3.2.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	0	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	Transferred Sector Number							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			TSU
Command	ACh							

Feature register -

Bit7 and bit3 shall be set to 1b. Bit6 to bit4 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred.

LBA Low register -

Transferred Sector Number shall be set to a number of the sector to be transferred. When TSU is set to 1b and this subcommand is issued iteratively in order to transfer all objective data, Transferred Sector Number shall be set to i or $i + 1$, where i is set into this register on the previous issuance by the Host Interface Unit. Moreover, initial value of i is set to 00h in this case. When TSU is set to 0b, Transferred Sector Number shall be set to 00h.

Device register -

DEV shall specify the selected Storage Device.

TSU shall be set to 1b if the unit of sectors to be transferred is one. On the other hand, TSU shall be set to 0b if the whole data is transferred all at once.

6.2.3.2.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.2.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	ISC	ITSN	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ISC shall be set to 1b if Transferred Sector Count is illegal.

ITSN shall be set to 1b if Transferred Sector Number is illegal.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register as the result of decryption or will be set into the Data register (only if the data to be set into the register was created associated with the reception of this subcommand) if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The value of Transferred sector number specified by the Host Interface Unit is not appropriate.
- 6) The Storage Module detects the write error as to RDCL_[i] if the write operation is necessary and executed.
- 7) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.2.4 Data to be transferred from the Host Device

PUT INCEPTIVE SESSION KEY UT CONNECTION information of which size is SectorNumber(N) sectors or one sector is set into the Data register. The size is determined in accordance with the values of TSU. The structure is shown in Table 6.15. In the information, a Session Key generated in the Destination Module in the Inceptive Device on Connection Stage is included; $E(K_{ch[P]})$, $E(KP_{dc[P]})$, $K_{s[I]}$ || $KP_{d[I]}$ || $MVU_{[I]}$ || $RDCL_{[I]}$. The structure of the data is described as Inceptive_Session in SAFIA/PDS2.

Table 6.15 PUT INCEPTIVE SESSION KEY UT CONNECTION information

BP	Length	Descriptions
0	N	Inceptive_Session
N	$512 \times \text{SectorNumber}(N) - N$	Filled with zeros

6.2.3.2.5 Prerequisites

DRDY set to 1b.

6.2.3.2.6 Description

After receiving this subcommand, the Storage Interface Unit receives SectorNumber(N) sectors data which include a Session Key $K_{s[I]}$ generated in the Destination Module in the Inceptive Device, Device Public Key $KP_{d[I]}$ and Revoked Device Class List $RDCL_{[I]}$, which are installed or recorded in the Inceptive Device respectively, all at once or sector-by-sector. If TSU is set to 0b, the data is set into Data register all at once. If TSU is set to 1b, the data is set into Data register one sector at a time. $K_{s[I]}$ and $KP_{d[I]}$ are whereat doubly encrypted with $KP_{dc[P]}$ and $K_{ch[P]}$, the $RDCL_{[I]}$ is meanwhile encrypted with $K_{ch[P]}$ only.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Decrypting the data with $K_{dc[P]}$ and $K_{ch[P]}$.
- (2) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (3) Verifying $RDCL_{[I]}$. If the verification of Checksum included in Inceptive_Session fails, the Usage Pass Transfer Unit in the Storage Module and the Storage Interface Unit aborts the execution.
- (4) Comparing the issue date of $RDCL_{[I]}$ and $RDCL_{[P]}$.
- (5) Overwriting $RDCL_{[P]}$ with the $RDCL_{[I]}$ if the verification described in (3) succeeds and the issue date of $RDCL_{[P]}$ is older than the issue date of $RDCL_{[I]}$ as the result of the comparison described in (4).
- (6) Invalidating all entries of Transaction Log if $RDCL_{[P]}$ is updated in (5). In this case, all entries

of Connection Log are also invalidated if SAFIA BT feature set is implemented on the Storage Device.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET PRIMAL SESSION KEY UT CONNECTION.

- (7) Creating a Session Key $K_{s[P]}$, which is shared in Connection Stage.
- (8) Encrypting the $K_{s[P]}$ with $K_{s[I]}$.
- (9) Concatenating $RDCL_{[P]}$ with the encrypted data $E(K_{s[I]}, K_{s[P]} || MVU_{[P]})$ if the issue date of $RDCL_{[I]}$ is older than the issue date of $RDCL_{[P]}$.
- (10) Encrypting the concatenated data $E(K_{s[I]}, K_{s[P]} || MVU_{[P]}) || RDCL_{[P]}$ with $KP_{d[I]}$.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) after GET PRIMAL CHALLENGE KEY UT CONNECTION or PUT INCEPTIVE SESSION KEY UT CONNECTION (this subcommand itself) was executed on Connection Stage in the Channel.

6.2.3.3 PUT INCEPTIVE SESSION KEY UT TRANSFER

6.2.3.3.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	1	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7 and bit5 shall be set to 1b. Bit6, bit4 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.3.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.3.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register as the result of decryption if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.3.4 Data to be transferred from the Host Device

PUT INCEPTIVE SESSION KEY UT TRANSFER information of which size is one sector is set into the Data register. The structure is shown in Table 6.16. In the information, a Session Key generated in the Destination Module in the Inceptive Device on Transfer Stage is included; UPID || $E(K_{s[P]}, E(K_{s[I]_{previous}}, K_{s[I]}))$, where $K_{s[I]_{previous}}$ is the Session Key generated in the Destination Module in the Inceptive Device on the previous Transfer Stage. The structure of the data is described as Transfer_Session in SAFIA/PDS2.

Table 6.16 PUT INCEPTIVE SESSION KEY UT TRANSFER information

BP	Length	Descriptions
0	86	Transfer_Session
86	426	Filled with zeros

6.2.3.3.5 Prerequisites

DRDY set to 1b.

6.2.3.3.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Session Key $K_{s[I]}$ generated in the Destination Module in the Inceptive Device and is set into the Data register. $K_{s[I]}$ is doubly encrypted with $K_{s[I]_{previous}}$ and $K_{s[P]}$.

When the Storage Device receives the data, the Storage Device processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Collating the received Usage Pass Identifier with the Usage Pass Identifier of the Usage Pass existing in Buf.QSTC. If the collation fails, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Decrypting the data with $K_{s[P]}$ and $K_{s[I]_{previous}}$.
- (3) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (4) Creating an entry of Transaction Log and recording the Usage Pass Identifier, Acceptable Usage Pass Type Map, $KP_{d[I]}$, $K_{s[I]}$, state of the Transfer Stage ("SP"), Original AC_s of the Usage Pass to be transferred, LBAQ which points out the area where the Usage Pass in Buf.QSTC originally recorded and Sector Length of the Usage Pass into each corresponding field of the entry.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Primal Device, and (2) if a Connection has been established between the Devices. A condition (2) means that the subcommand execution is allowed not only after GET PRIMAL SESSION KEY UT CONNECTION (end of Connection Stage) or GET PRIMAL SESSION KEY UT RECONNECTION (end of Reconnection Stage) but also after VERIFY TRANSACTION STATUS UT RECOVERY

(first step of Recovery Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Transfer Stage.

6.2.3.4 PUT PRIMAL CHALLENGE KEY UT CONNECTION

6.2.3.4.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7 shall be set to 1b. Bit6 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.4.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.4.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register or will be set into the Data register (only if the data to be set in the register was created associated with the reception of this subcommand) if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.4.4 Data to be transferred to the Host Device

PUT PRIMAL CHALLENGE KEY UT CONNECTION information of which size is one sector is set into the Data register. The structure is shown in Table 6.17. In the information, a Challenge Key

generated in the Source Module in the Primal Device on Connection Stage is included; $E(KP_{dc[l]}, K_{ch[P]} || C(K_r, KP_{dc[P]}))$. The structure of the data is described as Primal_Challenge in SAFIA/PDS2.

Table 6.17 PUT PRIMAL CHALLENGE KEY UT CONNECTION information

BP	Length	Descriptions
0	N (from 428 to 492)	Primal_Challenge
N	$512 - N$	Filled with zeros

6.2.3.4.5 Prerequisites

DRDY set to 1b.

6.2.3.4.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Challenge Key $K_{ch[P]}$ generated in the Primal Device with Device Class Certificate $C(K_r, KP_{dc[P]})$ installed in the Primal Device and is set into the Data register. $K_{ch[P]}$ is encrypted with $KP_{dc[l]}$ only.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Verifying $C(K_r, KP_{dc[P]})$ with KP_r and $RDCL_{[l]}$ which are installed and recorded respectively in the Storage Device. If the verification fails or the Device Class Certificate is the revoked one, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Decrypting $E(KP_{dc[l]}, K_{ch[P]})$ with $K_{dc[l]}$.
- (3) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET INCEPTIVE SESSION KEY UT CONNECTION.

- (4) Creating a Session Key $K_{s[l]}$, which is shared in Connection Stage.
- (5) Concatenating $K_{s[l]}$ with $KP_{d[l]}$ installed in the Storage Device.
- (6) Encrypting the concatenated data with $KP_{dc[P]}$.
- (7) Concatenating $RDCL_{[l]}$ recorded in the Usage Pass Transfer Unit with the encrypted data $E(KP_{dc[P]}, K_{s[l]} || KP_{d[l]})$.
- (8) Encrypting the concatenated data $E(KP_{dc[P]}, K_{s[l]} || KP_{d[l]}) || RDCL_{[l]}$ with $K_{ch[P]}$.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is an Inceptive Device, and (2) after GET DEVICE CLASS CERTIFICATE or PUT PRIMAL CHALLENGE KEY UT CONNECTION (this subcommand itself) was executed on Connection Stage in the Channel.

6.2.3.5 PUT PRIMAL SESSION KEY UT CONNECTION

6.2.3.5.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	0	0	1	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	Transferred Sector Number							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			TSU
Command	ACh							

Feature register -

Bit7 and bit4 shall be set to 1b. Bit6, bit5 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred.

LBA Low register -

Transferred Sector Number shall be set to a number of the sector to be transferred. When TSU is set to 1b and this subcommand is issued iteratively in order to transfer all objective data, Transferred Sector Number shall be set to i or $i + 1$, where i is set into this register on the previous issuance by the Host Interface Unit. Moreover, initial value of i is set to 00h in this case. When TSU is set to 0b, Transferred Sector Number shall be set to 00h.

Device register -

DEV shall specify the selected Storage Device.

TSU shall be set to 1b if the unit of sectors to be transferred is one. On the other hand, TSU shall be set to 0b if the whole data is transferred all at once.

6.2.3.5.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.5.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	ISC	ITSN	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ISC shall be set to 1b if Transferred Sector Count is illegal.

ITSN shall be set to 1b if Transferred Sector Number is illegal.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register as the result of decryption if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The value of Transferred sector number specified by the Host Interface Unit is not appropriate.
- 6) The Qualified Storage Controller detects the write error as to RDCL_[P] if the Controller received the RDCL_[P].
- 7) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.5.4 Data to be transferred to the Host Device

PUT PRIMAL SESSION KEY UT CONNECTION information of which size is SectorNumber(N) sectors or one sector is set into the Data register. The size is determined in accordance with the values of TSU. The structure is shown in Table 6.18. In the information, a Session Key generated in the Source Module in the Primal Device on Connection Stage; $E(KP_{d[i]})$, $E(K_{s[i]})$, $K_{s[P]} || MVU_{[P]} || RDCL_{[P]}$. The structure of the data is described as Primal_Session in SAFIA/PDS2.

Table 6.18 PUT PRIMAL SESSION KEY UT CONNECTION information

BP	Length	Descriptions
0	N	Primal_Session
N	$512 \times \text{SectorNumber}(N) - N$	Filled with zeros

6.2.3.5.5 Prerequisites

DRDY set to 1b.

6.2.3.5.6 Description

After receiving this subcommand, the Storage Interface Unit receives SectorNumber(N) sector data which includes a Session Key $K_{s[P]}$ generated in the Source Module in the Primal Device with Revoked Device Class List $RDCL_{[P]}$ recorded in the Primal Device all at once or sector-by-sector. If TSU is set to 0b, the data is set into Data register all at once. If TSU is set to 1b, the data is set into Data register one sector at a time. Note that $RDCL_{[P]}$ is included if the issue date of $RDCL_{[i]}$ sent from the Storage Device is older than the issue date of $RDCL_{[P]}$ recorded in the Primal Device. $K_{s[P]}$ is whereat doubly encrypted with $K_{s[i]}$ and $KP_{d[i]}$, $RDCL_{[P]}$ is meanwhile encrypted with $KP_{d[i]}$ only.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Decrypting the data with $K_{d[i]}$ and $K_{s[i]}$.
- (2) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (3) Verifying $RDCL_{[P]}$ if it is included in the received data. If the verification of Checksum included in Primal_Session fails, the Usage Pass Transfer Unit in the Storage Module and the Storage Interface Unit aborts the execution.
- (4) Comparing the issue date of $RDCL_{[P]}$ and $RDCL_{[i]}$
- (5) Overwriting $RDCL_{[i]}$ with the $RDCL_{[P]}$ if the verification described in (3) succeeds and the issue date of $RDCL_{[i]}$ is older than the issue date of $RDCL_{[P]}$ as the result of the comparison described in (4).
- (6) Invalidating all entries of Transaction Log if $RDCL_{[i]}$ is updated in (5). In this case, all entries of Connection Log are also invalidated if SAFIA BT feature set is implemented on the Storage Device.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) after GET INCEPTIVE SESSION KEY UT CONNECTION or PUT PRIMAL SESSION KEY UT CONNECTION (this subcommand itself) was executed on Connection Stage.

6.2.3.6 PUT PRIMAL SESSION KEY UT RECONNECTION

6.2.3.6.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	0	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7, bit6 and bit3 shall be set to 1b. Bit5 and bit4 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.6.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.6.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register as the result of decryption if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.6.4 Data to be transferred to the Host Device

PUT PRIMAL SESSION KEY UT RECONNECTION information of which size is one sector is set into the Data register. The structure is shown in Table 6.19. In the information, a Session Key generated in the Source Module in the Primal Device on Reconnection Stage is included; UPID || E(KP_{d[|]TL}, E(K_{s[|]TL}, K_{s[|]P})). The structure of the data is described as Recovery_Connection in

SAFIA/PDS2.

Table 6.19 PUT PRIMAL SESSION KEY UT RECONNECTION information

BP	Length	Descriptions
0	151	Recovery_Connection
151	361	Filled with zeros

6.2.3.6.5 Prerequisites

DRDY set to 1b.

6.2.3.6.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Session Key $K_{s[P]}$ generated in the Primal Device. $K_{s[P]}$ is doubly encrypted with $K_{s[I]TL}$ and $KP_{d[I]TL}$ which are fetched from the Transaction Log.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Retrieving Transaction Log with the received Usage Pass Identifier. If such the entry is not retrieved, or, such the entry is retrieved but the value of Session Status recorded in the entry is “UnSpecified” or “Send Prepared” or “Send Completed”, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Decrypting $E(KP_{d[I]TL}, E(K_{s[I]TL}, K_{s[P]}))$ with the retrieved $K_{d[I]}$ and $K_{s[I]TL}$.
- (3) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in UT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Reconnection Stage and the Storage Device turns to Inceptive Device until the Storage Interface Unit receives one of the following subcommands in the Channel, namely VERIFY DEVICE CLASS CERTIFICATE or SEARCH TRANSACTION LOG UT RECONNECTION and the Storage Module completes the processes related to the subcommands.

6.2.3.7 PUT USAGE PASS

6.2.3.7.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	0	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	1	obs	DEV	LBAQ (27:24)			
Command	Ach							

Feature register -

Bit7 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

LBA Low register -

LBAQ address bits (7:0) shall be set to the register.

LBA Mid register -

LBAQ address bits (15:8) shall be set to the register.

LBA High register -

LBAQ address bits (23:16) shall be set to the register.

Device [3:0] register -

Bit6 shall be set to 1b.

DEV shall specify the selected Storage Device.

LBAQ address bits (27:23) shall be set to bit3 to bit 0.

6.2.3.7.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.7.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	ICC	IDNF	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	na	obs	DEV	LBAQ (27:24)			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

WP shall be set to one if modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE regardless of the value set in PL.

ICC shall be set to 1b if writing the Usage Pass into Qualified Storage is not allowed in terms of the Control Count (see section 7.3.1 of SAFIA/PDS1).

IDNF shall be set to 1b if the specified address is outside of the range where the Host may write the Usage Passes and subcommand aborted is not returned.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register as the result of decryption if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) The Storage Device detects the write error as to the received Usage Pass.
- 6) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 7) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.
- 8) WP in the Error register is set to 1b..

NRDY shall be set to 1b if the previously received subcommand is not completed.

LBA Low, LBA Mid, LBA High, Device [3:0] registers -

shall be filled with the address of first unrecoverable error occurred on writing of Usage Passes to the specified area in the Qualified Storage.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.7.4 Data to be transferred to the Host Device

PUT USAGE PASS information of which size is one sector is set into the Data register. The structure is shown in Table 6.20. In the information, a Usage Pass, Action Indicator and Checksum are included; $E(*KP_{d[1]})$, $E(K_{s[1]})$, UP || AI || CKS)). The structure of the data is described as

Transfer_UsagePass in SAFIA/PDS2.

Table 6.20 PUT USAGE PASS information

BP	Length	Field
0	372	Transfer_UsagePass
372	140	Filled with zeros

6.2.3.7.5 Prerequisites

DRDY set to 1b.

6.2.3.7.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Usage Pass, Action Indicator and Checksum.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Decrypting the data with $*K_{d[i]}$ and $K_{s[i]}$.
- (2) Checking the structure of the decrypted data by the calculation of Checksum and collating the Usage Pass Identifier with the one recorded in Transaction Log. If the structure error is detected or collation of the Usage Pass Identifier fails, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (3) Modifying Control Count appropriately.
- (4) Updating the value of Session Status recorded in the entry of Transaction Log to "RC", LBAQ and Sector Length field of Transaction Status to LBAQ and Transferred Sector Count specified by the Host.
- (5) Writing the Usage Pass existing in Buf.QSTC to Qualified Storage and validate it.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) after GET INCEPTIVE SESSION KEY UT TRANSFER was executed on Transfer Stage. Iterative execution of the subcommand is not allowed. When the subcommand execution is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to a particular state which is for "Usage Pass movement is completed".

6.2.3.8 SEARCH TRANSACTION LOG UT RECONNECTION

6.2.3.8.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7 and bit6 shall be set to 1b. Bit5 to bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.8.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.8.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register or will be set into the Data register (only if the data to be set in the register was created associated with the reception of this subcommand) if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.8.4 Data to be transferred to the Host Device

SEARCH TRANSACTION LOG UT RECONNECTION information of which size is one sector is set into the Data register. The structure is shown in Table 6.21. In the information, Usage Pass

Identifier is included; UPID. The structure of the data is described as Open_Reconnection in SAFIA/PDS2.

Table 6.21 SEARCH TRANSACTION LOG UT RECONNECTION information

BP	Length	Descriptions
0	36	Open_Reconnection
36	476	Filled with zeros

6.2.3.8.5 Prerequisites

DRDY set to 1b.

6.2.3.8.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Usage Pass Identifier.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Retrieving Transaction Log with the received Usage Pass Identifier. If such the Transaction Log is not retrieved, or, such the Transaction Log is retrieved but Session Status of the Transaction Log is “UnSpecified” or “Receive Prepared” or “Receive Completed”, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET PRIMAL SESSION KEY UT RECONNECTION.

- (2) Creating $K_{s[P]}$ which is shared in Reconnection Stage.
- (3) Encrypting $K_{s[P]}$ with the retrieved $K_{s[TL]}$ and $KP_{d[TL]}$.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in UT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Reconnection Stage and the Storage Device turns to Primal Device until it receives one of the following subcommands, namely GET DEVICE CLASS CERTIFICATE or PUT PRIMAL SESSION KEY UT RECONNECTION and Storage Module completes the processes related to the subcommands.

6.2.3.9 SEARCH USAGE PASS UT RECOVERY

6.2.3.9.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	1	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7, bit6 and bit4 shall be set to 1b. Bit5 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.9.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.9.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was and will be set into the Data register if the verification of the structure is executed before subcommand completion when BSY is set to 0b. Note that the case in which a Usage Pass retrieved in Qualified Storage by this subcommand has already included structure error (for example, cases like UPS is “NE”) may not be recognized as the structure error.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.9.4 Data to be transferred to the Host Device

SEARCH USAGE PASS UT RECOVERY information of which size is one sector is set into the

Data register. The structure is shown in Table 6.22. In the information, Usage Pass Identifier is included; UPID. The structure of the data is described as Retrieval_UPID in SAFIA/PDS2.

Table 6.22 SEARCH USAGE PASS UT RECOVERY information

BP	Length	Descriptions
0	36	Retrieval_UPID
36	476	Filled with zeros

6.2.3.9.5 Prerequisites

DRDY set to 1b.

6.2.3.9.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Usage Pass Identifier.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Retrieving Transaction Log with the received Usage Pass Identifier. If such the Transaction Log is not retrieved, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Collating the Usage Pass Identifier of the Usage Pass pointed by the LBAQ which is recorded in the retrieved Transaction Log with the received one and setting Usage Pass Status in Transaction_Status. If the Usage Pass Identifiers differ or no Usage Pass is recorded, Usage Pass Status is set to “Not Exist”. If the Usage Pass Identifiers coincide, Usage Pass Status is set to “Valid” or “Invalid” according the state of the Usage Pass recorded in Qualified Storage.
- (3) Keyed hash value calculation with $K_{s[P]}$ shared most recently and $K_{s[TL]}$ recorded in the Transaction Log, Usage Pass Identifier and Session Status recorded in the Transaction Log, and the Usage Pass Status set at (2).
- (4) Concatenating the data: Usage Pass Identifier || Session Status || Usage Pass Status || keyed hash value obtained at (3). As the result, Transaction_Status defined in section 4.4.17.1 of SAFIA/PDS2 is obtained.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Device, and (2) if a Connection has been established between the Primal Device and the Storage Device as Inceptive Device. A condition (2) means that the subcommand execution is allowed not only after PUT PRIMAL SESSION KEY UT CONNECTION (end of Connection Stage) or PUT PRIMAL SESSION KEY UT RECONNECTION (end of Reconnection Stage) but also after CREATE INCEPTIVE SESSION KEY UT TRANSFER (first step of Transfer Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Recovery Stage.

6.2.3.10 VERIFY DEVICE CLASS CERTIFICATE

6.2.3.10.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	0	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit6 shall be set to 1b. Bit7, bit5, bit4 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.10.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.10.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	na	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the data which was set into the Data register or will be set into the Data register (only if the data to be set in the register was created associated with the reception of this subcommand) if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.
- 7) The received Device Class Certificate is the revoked one if the verification is executed before subcommand completion when BSY is set to 0b.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.10.4 Data to be transferred to the Host Device

VERIFY DEVICE CLASS CERTIFICATE information of which size is one sector is set into the Data register. The structure is shown in Table 6.23. In the information, a Device Class Certificate installed in the Inceptive Device is included; $C(K_r, KP_{dc[I]})$. The structure of the data is described as Open_Connection in SAFIA/PDS2.

Table 6.23 VERIFY DEVICE CLASS CERTIFICATE information

BP	Length	Descriptions
0	N (from 326 to 390)	Open_Connection
N	$512 - N$	Filled with zeros

6.2.3.10.5 Prerequisites

DRDY set to 1b.

6.2.3.10.6 Description

After receiving this subcommand, the Storage Device receives the Device Class Certificate installed in the Inceptive Device.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Verifying $C(K_r, KP_{dc[I]})$ with KP_r and $RDCL_{[P]}$ which are installed and recorded respectively in the Storage Device. If the verification fails or the Device Class Certificate is the revoked one, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET PRIMAL CHALLENGE KEY UT CONNECTION.

- (2) Creating a Challenge Key $K_{ch[P]}$.
- (3) Encrypting the data with $KP_{dc[I]}$.
- (4) Concatenating the encrypted data $E(KP_{dc[I]}, K_{ch[P]})$ with $C(K_r, KP_{dc[P]})$.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Connection Stage and the Storage Device turns to Primal Device until the receives one of the following subcommands, namely GET DEVICE CLASS CERTIFICATE or PUT PRIMAL SESSION KEY UT RECONNECTION Storage Module completes the processes related to the subcommands.

6.2.3.11 VERIFY TRANSACTION STATUS UT RECOVERY

6.2.3.11.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	1	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7, bit6, bit4 and bit3 shall be set to 1b. Bit5 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

Device register -

DEV shall specify the selected Storage Device.

6.2.3.11.2 Normal outputs

Register	7	6	5	4	3	2	1	0
Error	na							
Sector Count	na							RAC
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Sector Count register -

RAC shall indicate whether AC_s is recovered or not. RAC shall be set to 1b if the AC_s is overwritten with the one fetched from Transaction Log. For any other case, RAC shall be set to 0b.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be cleared to 0b.

DRQ shall be cleared to 0b.

ERR shall be cleared to 0b.

6.2.3.11.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

WP shall be set to one if modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE regardless of the value set in PL.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.
- 4) The Usage Pass Transfer Unit in the Storage Device detects the structure error on the Usage Pass of which AC_s is to be overwritten with the one recorded in the Transaction Log if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 5) Transferred Sector Count specified by the Host Interface Unit differs from 01h.
- 6) The length of the data which the Storage Interface Unit actually received differs from Transferred Sector Count which the Host Interface Unit specified.
- 7) The Usage Pass Identifier recorded in the Transaction Log which has been retrieved in Reconnection Stage differs from the one included in the received Transaction Status.
- 8) The Usage Pass Identifier of the Usage Pass pointed by the LBAQ which is recorded in the entry of Transaction Log differs from the one recorded in the entry of Transaction Log which has been retrieved in Reconnection Stage.
- 9) Modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE regardless of the valule set in PL.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.2.3.11.4 Data to be transferred to the Host Device

VERIFY TRANSACTION STATUS UT RECOVERY information of which size is one sector is set into the Data register. The structure is shown in Table 6.24. In the information, Usage Pass Identifier, Session Status, Usage Pass Status and a Hash value, which is calculated from the Usage Pass Identifier, the Session Status, the Usage Pass Status and two Session Keys, are included. The data is called Transaction Status. The structure of the data is described as Transaction_Status in SAFIA/PDS2.

Table 6.24 VERIFY TRANSACTION STATUS UT RECOVERY information

BP	Length	Descriptions
0	75	Transaction_Status
75	437	Filled with zeros

6.2.3.11.5 Prerequisites

DRDY set to 1b.

6.2.3.11.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Transaction Status.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Collating the Usage Pass Identifier in the received Transaction Status with the one recorded in the entry of Transaction Log which has been retrieved in the Reconnection Stage. If they differ, the Usage Pass Transfer Unit retrieves all entries of the Transaction Log with the received Usage Pass Identifier. If such the Usage Pass is not retrieved, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Verifying the keyed hash value in the received Transaction Status if the verification fails, the Storage Module abort the execution.
- (3) Collating the Usage Pass Identifier of the Usage Pass pointed by the LBAQ which is recorded in the retrieved entry of Transaction Log with the received one. If they differ, the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit abort the execution.
- (4) Overwriting the AC_s of the objective Usage Pass and validate the Usage Pass if it has been invalidated.
- (5) Updating the value of Session Status recorded in the entry of Transaction Log to “SP”.

This subcommand is allowed for the Storage Device to execute (1) when the Storage Device is Inceptive Devcie, and (2) if a Connection has been established between the Primal Device and the Storage Device. A condition (2) means that the subcommand execution is allowed not only after

GET PRIMAL SESSION KEY UT CONNECTION (end of Connection Stage) or GET PRIMAL SESSION KEY UT RECONNECTION (end of Reconnection Stage) but also after PUT INCEPTIVE SESSION KEY UT TRANSFER (first step of Transfer Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Recovery Stage.

6.3 SAFIA BT feature set subcommands

In the following section, detail of subcommand included in SAFIA BT feature set is described. The subcommands included in the feature set are executable only when a Channel is opened with BT mode.

This feature set is subordinate feature set of iVDR Qualified Access feature set in the sense that the feature set shall not be implemented unless iVDR Qualified Access feature set is implemented in the Storage Device.

It is noted that the Storage Device in this section is always Inceptive Device because it is assumed that the Channel is opened in BT mode.

6.3.1 Subcommands derived from READ QUALIFIED

Protocol is PIO data in.

6.3.1.1 GET DEVICE CLASS CERTIFICATE

6.3.1.1.1 Inputs

The description other than the one as to DCCN in the LBA Low register is the same as the one provided in section 6.2.1.1.1. As for DCCN, the word “GET SAFIA FEATURES BT information” is replaced by the word “GET SAFIA FEATURES UT information” appeared in the description about the LBA Low register.

6.3.1.1.2 Normal outputs

The description is the same as the one provided in section 6.2.1.1.2.

6.3.1.1.3 Error outputs

The description is the same as the one provided in section 6.2.1.1.3.

6.3.1.1.4 Data to be transferred to the Host Device

The description is the same as the one provided in section 6.2.1.1.4.

6.3.1.1.5 Prerequisites

The description is the same as the one provided in section 6.2.1.1.5.

6.3.1.1.6 Description

After receiving this subcommand, the Storage Interface Unit sets the Device Class Certificate

$C(K_r, KP_{dc[l]})$ installed in the Storage Device into the Data register.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in BT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Connection Stage.

6.3.1.2 GET INCEPTIVE CHALLENGE KEY BT CONNECTION

6.3.1.2.1 Inputs

The description is mostly the same as the one provided in section 6.2.1.2.1. However, bit 3 of Features register shall be set to 0b.

6.3.1.2.2 Normal outputs

The description is the same as the one provided in section 6.2.1.2.2.

6.3.1.2.3 Error outputs

The description other than the condition 6) for ABRT to set to 1b in Error register is the same as the one provided in section 6.2.1.2.3 (conditions from 1) to 5) are similarly applied). As for condition 6), the word “GET SAFIA FEATURES BT information” substitutes for the word “GET SAFIA FEATURES UT information” appeared in the sentence.

6.3.1.2.4 Data to be transferred to the Host Device

GET INCEPTIVE CHALLENGE KEY BT CONNECTION information of which size is SectorNumber(N) sectors or one sector is set into the Data register. The size is determined in accordance with the values of TSU. The structure is shown in Table 6.25. In the information, a Challenge Key generated in the Storage Device on Connection Stage is included; $E(K_{ch[P]}, E(KP_{dc[P]}, K_{ch[l]} || KP_{dc[l]} || MVB[l]) || RDCL[l])$. The structure of the data is described as Inceptive_Challenge in SAFIA/PDS2.

Table 6.25 GET INCEPTIVE CHALLENGE KEY BT CONNECTION information

BP	Length	Descriptions
0	N	Inceptive Challenge
N	$512 \times \text{SectorNumber}(N) - N$	Filled with zeros

6.3.1.2.5 Prerequisites

The description is the same as the one provided in section 6.2.1.2.5.

6.3.1.2.6 Description

After receiving this subcommand, the Usage Pass Transfer Unit in the Storage Device prepares one sector data including a Challenge Key $K_{ch[l]}$ generated in the Storage Device with Device Public Key installed in the Storage Device and Revoked Device Class List recorded in the Storage Device. If TSU is set to 0b, the prepared data is set into Data register all at once. If TSU is set to 1b,

the prepared data is set into Data register one sector at a time. The Challenge Key and the Device Public Key are doubly encrypted with $K_{ch[P]}$ and $KP_{dc[P]}$, meanwhile, the Revoked Device Class List is encrypted with $K_{ch[P]}$ only. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating a Challenge Key $K_{ch[I]}$.
- (2) Concatenating $K_{ch[I]}$ with $KP_{d[I]}$ installed in the Storage Device.
- (3) Encrypting the concatenated data with $KP_{dc[P]}$.
- (4) Concatenating $RDCL_{[I]}$ recorded in the Storage Device with the encrypted data $E(KP_{dc[P]}, K_{ch[I]} || KP_{d[I]} || MVB_{[I]})$.
- (5) Encrypting the concatenated data $E(KP_{dc[P]}, K_{ch[I]} || KP_{d[I]} || MVB_{[I]} || RDCL_{[I]})$ with $K_{ch[P]}$.

This subcommand is allowed for the Storage Device to execute after PUT PRIMAL CHALLENGE KEY BT CONNECTION or GET INCEPTIVE CHALLENGE KEY BT CONNECTION (this subcommand itself) was executed on Connection Stage.

6.3.1.3 GET INCEPTIVE SESSION KEY BT CONNECTION

6.3.1.3.1 Inputs

The description other than LBA Low and Device register is the same as the one provided in section 6.2.1.2.1. LBA Low shall be filled with zeros and TSU in Device register shall be set to 0b.

6.3.1.3.2 Normal outputs

The description is the same as the one provided in section 6.2.1.2.2.

6.3.1.3.3 Error outputs

The description other than the condition 5) and 6) for ABRT to set to 1b in Error register is the same as the one provided in section 6.2.1.2.3 (conditions from 1) to 4) are similarly applied and the condition 5) is not applied.) The condition 6) in section 6.2.1.2.3 is replaced by the following.

Error register -

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 6) Transferred Sector Count specified by the Host Interface Unit differs from 01h.

6.3.1.3.4 Data to be transferred to the Host Device

GET INCEPTIVE SESSION KEY BT CONNECTION information of which size is one sector is set into the Data register. The structure is shown in Table 6.26. In the information, a Session Key generated in the Storage Module on Connection Stage is included; $E(KP_{d[P]}, E(K_{s[P]}, K_{s[I]}))$. The structure of the data is described as Initial_InceptiveSession in SAFIA/PDS2.

Table 6.26 GET INCEPTIVE SESSION KEY BT CONNECTION information

BP	Length	Descriptions
0	114	Initial_InceptiveSession
114	398	Filled with zeros

6.3.1.3.5 Prerequisites

The description is the same as the one provided in section 6.2.1.2.5.

6.3.1.3.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Session Key generated in the Storage Module into the Data register. The Session Key is doubly encrypted with $K_{s[P]}$ and $KP_{d[P]}$. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating a Session Key $K_{s[I]}$, which is shared in Connection Stage.
- (2) Encrypting $K_{s[I]}$ with $K_{s[P]}$ and $KP_{d[P]}$.
- (3) Search Connection Log for the entry to record proper information. If an entry, where same $KP_{d[P]}$, Acceptable Usage Pass Type Map and Serial Number as the received one in this Connection Stage is recorded, exists, the entry shall be selected. If such entry does not exist, a new entry is created.
- (4) Recording $KP_{d[P]}$ and $K_{s[P]}$, $K_{s[I]}$, Acceptable Usage Pass Type Map, $MVB_{[P]}$ and Serial Number of received Device Class Certificate to the entry of Connection Log selected in (3). It is noted that $KP_{d[P]}$ and $K_{s[P]}$ generated in the Primal Device are set into the Data register by the Host Interface Unit on PUT PRIMAL SESSION KEY BT CONNECTION.

This subcommand is allowed for the Storage Device to execute after PUT PRIMAL SESSION KEY BT CONNECTION or GET INCEPTIVE SESSION KEY BT CONNECTION (this subcommand itself) was executed on Connection Stage.

6.3.1.4 GET INCEPTIVE SESSION KEY BT RECONNECTION

6.3.1.4.1 Inputs

The description is the same as the one provided in section 6.2.1.7.1.

6.3.1.4.2 Normal outputs

The description is the same as the one provided in section 6.2.1.7.2.

6.3.1.4.3 Error outputs

The description is the same as the one provided in section 6.2.1.7.3.

6.3.1.4.4 Data to be transferred to the Host Device

GET INCEPTIVE SESSION KEY BT RECONNECTION information of which size is one sector is set into the Data register. The structure is shown in Table 6.27. In the information, a Session Key generated in itself on Reconnection Stage is included; $E(KP_{d[P]CL}, E(K_{s[P]CL}, K_{s[I]}))$. The structure of the data is described as Recovery_InceptiveConnection in SAFIA/PDS2.

Table 6.27 GET INCEPTIVE SESSION KEY BT RECONNECTION information

BP	Length	Descriptions
0	114	Recovery_InceptiveConnection
114	398	Filled with zeros

6.3.1.4.5 Prerequisites

The description is the same as the one provided in section 6.2.1.7.5.

6.3.1.4.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Session Key generated in the Storage Module into the Data register. The Session Key is doubly encrypted with $K_{s[P]CL}$ and $KP_{d[P]CL}$ which are fetched from the Connection Log recorded in the Storage Device. Then, if the following processes have not executed yet, the Storage Module executes them before output of the data.

- (1) Creating a Session Key $K_{s[I]}$, which is shared in Reconnection Stage.
- (2) Concatenating RPI with $K_{s[I]}$.
- (3) Encrypting the concatenated data $K_{s[I]} || RPI$ with $K_{s[P]CL}$ and $KP_{d[P]CL}$.
- (4) Updating $K_{s[P]}$, $K_{s[I]}$ recorded in the entry of Connection Log which CL Entry Pointer designates.

It is noted that $K_{s[P]}$ generated in the Primal Device is set in the Data register by the Host Interface Unit on PUT PRIMAL SESSION KEY BT RECONNECTION.

This subcommand is allowed for the Storage Device to execute after PUT PRIMAL SESSION KEY BT RECONNECTION or GET INCEPTIVE SESSION KEY BT RECONNECTION (this subcommand itself) was executed on Reconnection Stage.

6.3.1.5 GET INCEPTIVE SESSION KEY BT TRANSFER

6.3.1.5.1 Inputs

The description is the same as the one provided in section 6.2.1.3.1.

6.3.1.5.2 Normal outputs

The description is the same as the one provided in section 6.2.1.3.2.

6.3.1.5.3 Error outputs

The description is the same as the one provided in section 6.2.1.3.3.

6.3.1.5.4 Data to be transferred to the Host Device

GET INCEPTIVE SESSION KEY BT TRANSFER information of which size is one sector is set into the Data register. The structure is shown in Table 6.28. In the information, a Session Key generated in the Storage Module on Transfer Stage is included; $E(K_{s[P]}, E(K_{s[I]n}, K_{s[I]n+1}))$, where $K_{s[I]n}$ is the Session Key generated most recently in the Storage Module and $K_{s[P]}$ is the Session Key generated most recently in the Primal Device. The structure of the data is described as

Transfer_InceptiveSession in SAFIA/PDS2.

Table 6.28 GET INCEPTIVE SESSION KEY BT TRANSFER information

BP	Length	Descriptions
0	50	Transfer_InceptiveSession
50	462	Filled with zeros

6.3.1.5.5 Prerequisites

The description is the same as the one provided in section 6.2.1.3.5.

6.3.1.5.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Session Key generated in the Storage Module into the Data register. The Session Key is doubly encrypted with $K_{s[P]}$ and $K_{s[|]n}$.

This subcommand is allowed for the Storage Device to execute after CREATE INCEPTIVE DEVICE SESSION KEY BT TRANSFER or GET INCEPTIVE SESSION KEY BT TRANSFER (this subcommand itself) was executed on Transfer Stage.

6.3.1.6 GET MASKED USAGE PASS

6.3.1.6.1 Inputs

The description is the same as the one provided in section 6.2.1.4.1.

6.3.1.6.2 Normal outputs

The description is the same as the one provided in section 6.2.1.4.2.

6.3.1.6.3 Error outputs

The description is the same as the one provided in section 6.2.1.4.3.

6.3.1.6.4 Data to be transferred to the Host Device

The description is the same as the one provided in section 6.2.1.4.4.

6.3.1.6.5 Prerequisites

The description is the same as the one provided in section 6.2.1.4.5.

6.3.1.6.6 Description

The description is basically the same as the one provided in section 6.2.1.4.6, other than that the subcommand is allowed for the Storage Device to execute after READ USAGE PASS is executed on UP Inquiry Stage when the Storage Device is Inceptive Device. The reason is that the Storage Device is always inceptive Device in BT mode.

6.3.1.7 GET MASKED USAGE PASS WITH KEYED HASH

6.3.1.7.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	0	1	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ABh							

Feature register -

Bit6, bit4 and bit3 shall be set to 1b. Bit7 and bit5 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred. A value of 00h specifies that 256 sectors are to be transferred.

Device register -

DEV shall specify the selected Storage Device.

6.3.1.7.2 Normal outputs

The description is the same as the one provided in section 6.2.1.4.2.

6.3.1.7.3 Error outputs

The description is the same as the one provided in section 6.2.1.4.3.

6.3.1.7.4 Data to be transferred to the Host Device

GET MASKED USAGE PASS WITH KEYED HASH information of which size is N sectors is set into the Data register. The structure is shown in Table 6.29. In the information, Masked Usage Pass, Usage Pass Status and Hash value are included; $UPS \parallel MUP \parallel H(K_{s[P]} \parallel K_{s[I]} \parallel UPS \parallel MUP)$. The structure of the data is described as Signed_Masked_UsagePass in SAFIA/PDS2.

Table 6.29 GET MASKED USAGE PASS WITH KEYED HASH information

BP	Length	Descriptions
0	380	Signed_Masked_UsagePass (1)
380	132	Filled with zeros
512	380	Signed_Masked_UsagePass (2)
892	132	Filled with zeros
		Repetition of 1 sector unit where Signed_Masked_UsagePass is included

6.3.1.7.5 Prerequisites

The description is the same as the one provided in section 6.2.1.4.5.

6.3.1.7.6 Description

After receiving this subcommand, the Storage Interface Unit sets the information of the Usage Pass that exists in the Buf.UPTU as the GET MASKED USAGE PASS WITH KEYED HASH information into the Data register. If the Host Interface Unitl sets $N (>1)$ into Sector Count register as N Usage Passes exist in Buf.UPTU, N sector data in which N Usage Passes are included is set into the Data register. If the number that the Host Interface Unitl sets into Sector Count register differs from the number of Usage Passes which exists in Buf.UPTU, which means that different Transferred Sector Count is set for previously executed READ USAGE PASS, the subcommand is aborted.

If the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS is “Not Exist” or “Invalid”, up_masked field of Signed_Masked_UsagePass is filled with zeros.

This subcommand is allowed for the Storage Device to execute after READ USAGE PASS is executed on UP Inquiry Stage.

6.3.1.8 GET SAFIA FEATURES BT

6.3.1.8.1 Inputs

The description is the same as the one provided in section 6.2.1.8.1.

6.3.1.8.2 Normal outputs

The description is the same as the one provided in section 6.2.1.8.2.

6.3.1.8.3 Error outputs

The description is the same as the one provided in section 6.2.1.8.3.

6.3.1.8.4 Data to be transferred to the Host Device

GET SAFIA FEATURES BT information of which size is one sector is set into the Data register. The structure is shown in Table 6.30.

Table 6.30 GET SAFIA FEATURES BT information

BP	Length	Descriptions
0	64	Installed Device Class Certificate List
64	1	SAFIA Device Interface Version
65	2	Reference Completion Time [GET DEVICE CLASS CERTIFICATE]
67	2	Reference Completion Time [GET INCEPTIVE CHALLNGE KEY BT CONNECTION]
69	2	Reference Completion Time [GET INCEPTIVE SESSION KEY BT CONNECTION]
71	2	Reference Completion Time [GET INCEPTIVE SESSION KEY BT RECONNECTION]
73	2	Reference Completion Time [GET INCEPTIVE SESSION KEY BT TRANSFER]
75	2	Reference Completion Time [GET MASKED USAGE PASS (for one Usage Pass)]
77	2	Reference Completion Time

		[GET MASKED USAGE PASS WITH KEYED HASH (for one Usage Pass)]
79	2	Reference Completion Time [GET TRANSACTION STATUS BT RECOVERY]
81	2	Reference Completion Time [GET USAGE PASS for one Usage Pass]
83	2	Reference Completion Time [CREATE INCEPTIVE SESSION KEY BT TRANSFER]
85	2	Reference Completion Time [ENCRYPT USAGE PASS COPY (for one Usage Pass)]
87	2	Reference Completion Time [ENCRYPT USAGE PASS MOVE (for one Usage Pass)]
89	2	Reference Completion Time [ENCRYPT USAGE PASS PLAY (for one Usage Pass)]
91	2	Reference Completion Time [READ USAGE PASS (for one Usage Pass)]
93	2	Filled with zeros (0000h)
95	2	Reference Completion Time [PUT PRIMAL CHALLENGE KEY BT CONNECTION]
97	2	Reference Completion Time [PUT PRIMAL SESSION KEY BT CONNECTION]
99	2	Reference Completion Time [PUT PRIMAL SESSION KEY BT RECONNECTION]
101	2	Reference Completion Time [PUT PRIMAL SESSION KEY BT TRANSFER]
103	2	Reference Completion Time [PUT USAGE PASS (for one Usage Pass)]
105	2	Reference Completion Time [RECOVER USAGE PASS]
107	2	Reference Completion Time [SEARCH USAGE PASS BT RECOVERY]
109	6	Start LBAQ of Qualified Storage
115	6	End LBAQ of Qualified Storage
121	2	Recorded Size of Revoked Device Class List
123	2	Maximum Transferred Sector Count
125	1	Recordable Entry Number of Connection Log
126	1	CLEAR CONNECTION LOG Availability
127	1	Recovery Allowed Entry Number of Connection Log
128	10	Serial Number of Device Class Certificate of Primal Device 1 [SNPD1]
138	10	Serial Number of Device Class Certificate of Primal Device 2 [SNPD2]
		...
268	10	Serial Number of Device Class Certificate of Primal Device 15 [SNPD15]
278	234	Filled with zeros

- Installed Device Class Certificate List

The description is the same as the one provided in section 6.2.1.8.4.

- SAFIA Device Interface Version

The description is the same as the one provided in section 6.2.1.8.4.

- Reference Completion Time (BP 65, ..., BP 108)

The description is the same as the one provided in section 6.2.1.8.4.

- Start LBAQ of Qualified Storage
The description is the same as the one provided in section 6.2.1.8.4.
- End LBAQ of Qualified Storage
The description is the same as the one provided in section 6.2.1.8.4.
- Recorded Size of Revoked Device Class List
The description is the same as the one provided in section 6.2.1.8.4.
- Maximum Transferred Sector Count
The description is the same as the one provided in section 6.2.1.8.4.
- Recordable Entry Number of Connection Log
Recordable Entry Number of Connection Log indicates a maximum number of entries of Connection Log which the Storage Device can retain.
- CLEAR CONNECTION LOG Availability
CLEAR CONNECTION LOG Availability indicates whether CLEAR CONNECTION LOG is functional or not on the connected Storage Device.
If the MSB of CLEAR CONNECTION LOG Availability is 1b, the subcommand is functional. Other bits are reserved.
- Recordable Entry Number of Connection Log
Recordable Entry Number of Connection Log indicates the number of entries of Connection Log which Storage Device can record. The value shall be less than or equal 0Fh.
If the value is 00h, fields from BP 127 to BP 277 are invalid.
- Recovery Allowed Entry Number of Connection Log
Recovery Allowed Entry Number of Connection Log indicates which Primal Device is allowed to execute Recovery Stage for the Storage Device. The value shall be less than or equal 0Fh. If the value is 01h, it means that only Primal Device specified by SNPD1 in Table 6.30 is allowed to execute Recovery Stage for the Storage Device with the recorded Transaction Log. Similarly, if the value is 02h, only Primal Device specified by SNPD2 is allowed to execute Recovery Stage with the recorded Transaction Log, and so forth. However, if the value is 00h, any Primal Device is not allowed to execute Recovery Stage for the Storage Device with the recorded Transaction Log.
- Serial Number of Device Class Certificate of Partner Primal Device (BP 128, ..., BP 277)
Serial Number of Device Class Certificate of Partner Primal Device indicate the Serial Number of Device Class Certificate of Primal Device, with which Connection Stage or Reconnection Stage was completed, and for which the entry of Connection Log retained in the Storage Device. The number of entries shall be less than or equal 15. If Recordable Number of Connection Log (RNCL) is less than 15, from SNPD(RNCL+1) to SNPD15 shall be set to 00 00 00 00 00 00 00 00 00h.
Serial Number of Device Class Certificate of Partner Primal Device shall be set to 00 00 00 00 00 00 00 00 00h if SAFIA Device Interface Version is less than the value described in 6.2.1.8.4 or no Connection Log is retained.

6.3.1.8.5 Prerequisites

The description is the same as the one provided in section 6.2.1.8.5.

6.3.1.8.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data in which various parameters are included as described in Table 6.30 into the Data register.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in BT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit remains unchanged.

6.3.1.9 GET TRANSACTION STATUS BT RECOVERY

6.3.1.9.1 Inputs

The description is the same as the one provided in section 6.2.1.10.1.

6.3.1.9.2 Normal outputs

The description is the same as the one provided in section 6.2.1.10.2.

6.3.1.9.3 Error outputs

The description is the same as the one provided in section 6.2.1.10.3.

6.3.1.9.4 Data to be transferred to the Host Device

GET TRANSACTION STATUS BT RECOVERY information of which size is one sector is set into the Data register. The structure is shown in Table 6.31. In the information, Usage Pass Identifier, Access Condition for Storage Module, Usage Pass Status, Usage Pass Location and Hash value, which is calculated from the Usage Pass Identifier, the Access Condition for Storage Module, the Usage Pass Status, the Usage Pass Location and two Session Keys, are included. The structure of the data is described as Transaction_Status in SAFIA/PDS2. Note that up_location field of Transaction_Status consists of two parts. The size of the first part is 6-byte and LBAQ is recorded into the field for the purpose. The size of the second part is 2-byte and Transferred Sector Count is recorded into the field for the purpose.

Table 6.31 GET TRANSACTION STATUS BT RECOVERY information

BP	Length	Field
0	102	Transaction_Status
102	410	Filled with zeros

6.3.1.9.5 Prerequisites

The description is the same as the one provided in section 6.2.1.10.5.

6.3.1.9.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data including a Transaction Status into the Data register.

This subcommand is allowed for the Storage Device to execute after SEARCH USAGE PASS

BT RECOVERY or GET TRANSACTION STATUS BT RECOVERY (this subcommand itself) was executed on TS Creation Stage.

6.3.1.10 GET USAGE PASS

6.3.1.10.1 Inputs

The description other than the value of Transferred Sector Count set in Sector Count register is the same as the one provided in section 6.2.1.11.1.

Sector Count register -

Number of sectors to be transferred. A value of 00h specifies that 256 sectors are to be transferred.

6.3.1.10.2 Normal outputs

The description is the same as the one provided in section 6.2.1.11.2.

6.3.1.10.3 Error outputs

The description other than the condition 5) for ABRT to set to 1b in Error register is the same as the one provided in section 6.2.1.11.3 (conditions from 1) to 4) are similarly applied). The condition 5) in section 6.2.1.11.3 is replaced by the following.

Error register -

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 5) The value of Transferred Sector Count specified by the Host Interface Unit differs from the number of sectors for the objective Usage Passes existing in Buf.UPTU.

6.3.1.10.4 Data to be transferred to the Host Device

GET USAGE PASS information of which size is N sectors is set into the Data register. The structure is shown in Table 6.13. In the information, multiple Transfer_UsagePass(es) are included. A Transfer_UsagePass includes a Usage Pass, an Action Indicator and a Checksum are included; $E(*KP_{d[P]}, E(K_{s[P]}, UP || AI || CKS))$). The structure of the data is described as Transfer_UsagePass in SAFIA/PDS2.

Table 6.32 GET USAGE PASS information

BP	Length	Field
0	372	Transfer_UsagePass (1)
372	140	Filled with zeros
512	372	Transfer_UsagePass (2)
884	140	Filled with zeros
		Repetition of one sector unit where Transfer_UsagePass are Included

6.3.1.10.5 Prerequisites

The description is the same as the one provided in section 6.2.1.11.5.

6.3.1.10.6 Description

After receiving this subcommand, the Storage Module processes the following if the execution of the subcommand which had been previously received (ENCRYPT USAGE PASS COPY or MOVE or PLAY) has completed.

- (1) Setting Recovery-Allowed Primal Device Indicator to designate the entry of Connection Log if the Indicator does not designate the entry.
- (2) Modifying the Control Count of the original Usage Pass (not duplicated one) in Buf.QSTC to comply with the description in section 7.3 of SAFIA/PDS1.
- (3) Overwriting Access Condition for Storage Module of the Usage Pass which exists in Qualified Storage with the Access Condition for Storage Module of the original Usage Pass which exists in Buf.QSTC for Copy or Play. Invalidating the Usage Pass which exists in Qualified Storage for Move.
- (4) Setting *N* sector data including a Usage Pass, Action Indicator and Checksum into the Data register.

If the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS is “Not Exist” or “Invalid”, Transfer_UsagePass field is filled with zeros and step (1) and step (3) are not executed.

This subcommand is allowed for the Storage Device to execute after ENCRYPT USAGE PASS COPY or ENCRYPT USAGE PASS MOVE or ENCRYPT USAGE PASS PLAY was executed on IP Transfer Stage. Iterative execution of the subcommand is not allowed. When the subcommand execution is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to a particular state which is for “Usage Pass movement is completed”.

6.3.2 Subcommands derived from SET QUALIFIED

Protocol is non data.

6.3.2.1 CHECK EXECUTION STATUS

6.3.2.1.1 Inputs

The description is the same as the one provided in section 6.2.2.1.1.

6.3.2.1.2 Normal outputs

The description is the same as the one provided in section 6.2.2.1.2.

6.3.2.1.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	IDC	VDCC	fz	fz	ABRT	NRDY	VDSW
Sector Count	na							VDSR
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

IDC indicates the results of collation of Usage Pass Identifier. If the Usage Pass Identifier of the Usage Pass which is fetched from Qualified Storage, retrieved or to be recovered differs from the received one, IDC shall be set to 1b. For any other case, IDC shall be set to 0b.

VDCC indicates the validity of the received Device Class Certificate if this subcommand is received just after the execution of PUT PRIMAL CHALLENGE KEY BT CONNECTION. If the received Device Class Certificate is revoked one, which is turned out by the collation of Revoked Device Class List recorded in itself, VDCC shall be set to 1b. For any other case, VDCC shall be set to 0b.

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module.
- 2) A Channel of which Channel Identifier is the same as the one that the Host Interface Unit specified at the input is not opened.
- 3) The Storage Interface Unit received the subcommand in illegal order.

NRDY shall be set to 1b if the previously received subcommand is not completed.

VDSW indicates the validity of the structure of the received data if this subcommand is received just after the execution of all subcommands derived from WRITE QUALIFIED. If a Storage Device receives these subcommands, it is necessary to verify or decrypt the received data. When the structure of the obtained data is invalid, VDSW shall be set to 1b. For any other case, VDSW shall be set to 0b. This flag corresponds to VDS in version 1.0.

VDSR indicates the validity of the structure of the data placed in the Buf.QSTC by fetching Usage Pass from Qualified Storage or in the Buf.UPTU by extracting RDCL, KP_d and so forth to transfer to the Host Device by the subcommands derived from READ QUALIFIED. When the structure of the data is invalid, VDSR shall be set to 1b. For any other case, VDSR shall be set to 0b.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit or a Sector Count register bit is set to 1b.

6.3.2.1.4 Data to be transferred from/to the Host Device

The description is the same as the one provided in section 6.2.2.1.4.

6.3.2.1.5 Prerequisites

The description is the same as the one provided in section 6.2.2.1.5.

6.3.2.1.6 Description

The description is basically the same as the one provided in section 6.2.2.1.6. However, a Channel specified with the Channel identifier shall have been opened in BT mode.

6.3.2.2 CLEAR CONNECTION LOG

This subcommand is optional. The availability on a Storage Device is indicated to the connected Host Device in GET SAFIA FEATURES BT information (Table 6.30).

6.3.2.2.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	1	1	0	0	CHID		
Sector Count	Invalidated Entry Number							
LBA Low	Invalidated First Entry Number							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	AAh							

Feature register -

Bit6 and bit5 shall be set to 1b. Bit7, bit4 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Invalidated Entry Number shall be set to a number of entries of Connection Log to be invalidated. When Invalidated First Entry Number is 00h, Invalidated Entry Number shall be set to 00h.

LBA Low register -

Invalidated First Entry Number shall be set to the first entry number of Connection Log to be invalidated. When both Invalidated First Entry Number and Invalidated Entry Number are 00h, all entries of Connection Log in the Storage Device are invalidated.

Device register -

DEV shall specify the selected Storage Device.

6.3.2.2.2 Normal outputs

The description is the same as the one provided in section 6.2.2.1.2.

6.3.2.2.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	CN	IEN	IFEN	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

Error register -

CP shall be set to 1b if some errors occurred on the execution of the subcommand which Storage Interface Unit had previously received, set to 0b if some errors occur on the execution of this subcommand.

WP shall be set to one if modification of the data recorded in Qualified Storage is prohibited by DISABLE WRITE QUALIFIED SPACE regardless of the value set in PL.

CN shall be set to 1b if the state of the Storage Device has already transited to the state to execute Connection Stage or Reconnection Stage, which means that GET DEVICE CLASS CERTIFICATE (see section 6.3.1.1) or PUT PRIMAL SESSION KEY BT RECONNECTION (see section 6.3.3.3) has already been executed.

IEN shall be set to 1b if Invalidated First Entry Number + Invalidated Entry Number exceeds the recordable entry number for the Storage Device.

IFEN shall be set to 1b if Invalidated First Entry Number is out of range from 00h to the recordable entry number for the Storage Device..

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 1) The received subcommand is not executable in the Storage Interface Unit and the Storage Module..
- 2) The Storage Interface Unit received the subcommand in illegal order.
- 3) WP in the Error register is set to 1b.
- 4) CN in the Error register is set to 1b.
- 5) IEN in the Error register is set to 1b.
- 6) IFEN in the Error register is set to 1b.

NRDY shall be set to 1b if the previously received subcommand is not completed.

Device register -

DEV shall indicate the selected Storage Device.

Status register -

BSY shall be cleared to 0b indicating subcommand completion. Clearing BSY to 0b does not mean the completion of the execution of all the processes associated with this subcommand.

DRDY shall be set to 1b.

DF (Device Fault) shall be set to 1b if a device fault has occurred.

DRQ shall be cleared to 0b.

ERR shall be set to 1b if an Error register bit is set to 1b.

6.3.2.2.4 Data to be transferred from/to the Host Device

Non data.

6.3.2.2.5 Prerequisites

DRDY set to 1b.

6.3.2.2.6 Description

When the Storage Interface Unit receives the subcommand, the Usage Pass Transfer Unit in the Storage Device invalidates the specified entries of Connection Log according to Invalidated Entry Number and Invalidated First Entry Number.

This subcommand is allowed for the Storage Device to execute when a Channel has already opened in BT mode with the proviso that GET DEVICE CLASS CERTIFICATE and PUT PRIMAL SESSION KEY BT RECONNECTION has not been executed.

6.3.2.3 CREATE INCEPTIVE SESSION KEY BT TRANSFER

6.3.2.3.1 Inputs

The description is mostly the same as the one provided in section 6.2.3.1.1, other than the command code of the subcommand is not the one of WRITE QUALIFIED but the one of SET QUALIFIED.

Register	7	6	5	4	3	2	1	0
Features	1	0	0	1	1	CHID		
Sector Count	fz							
LBA Low	fz							
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	AAh							

Feature register -

Bit7, bit4 and bit3 shall be set to 1b. Bit6 and bit5 shall be set to 0b.

CHID shall be set to Channel Identifier.

Device register -

DEV shall specify the selected Storage Device.

6.3.2.3.2 Normal outputs

The description is the same as the one provided in section 6.2.3.1.2.

6.3.2.3.3 Error outputs

The description other than the condition 5) for ABRT to set to 1b in Error register is the same as the one provided in section 6.2.3.1.3 (conditions from 1) to 4) are similarly applied).

6.3.2.3.4 Data to be transferred from/to the Host Device

Non data.

6.3.2.3.5 Prerequisites

The description is the same as the one provided in section 6.2.3.1.5.

6.3.2.3.6 Description

After receiving this subcommand, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Creating a Session Key $K_{s[[]]n+1}$, which is shared in Transfer Stage.
- (2) Encrypting the $K_{s[[]]n+1}$ with $K_{s[[]]n}$ and $K_{s[P]}$, where $K_{s[P]}$ was a Session Key shared most recently through Connection or Reconnection or IP Transfer Stage executed in the past and $K_{s[[]]n}$ was also a Session Key shared most recently through Connection or Reconnection or PI Transfer Stage executed in the past.

This subcommand is allowed for the Storage Device to execute if a Connection has been established between the Usage Pass Transfer Unit in the Primal Device and the Usage Pass Transfer Unit in the Storage Device. The condition means that the subcommand execution is allowed not only after GET INCEPTIVE SESSION KEY BT CONNECTION (end of Connection Stage) or GET INCEPTIVE SESSION KEY BT RECONNECTION (end of Reconnection Stage) but also after SEARCH USAGE PASS BT RECOVERY (first step of TS Creation Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device transits to the first state within PI Transfer and IP Recovery Stage.

6.3.2.4 ENCRYPT USAGE PASS COPY

6.3.2.4.1 Inputs

The description is the same as the one provided in section 6.2.2.2.1.

6.3.2.4.2 Normal outputs

The description is the same as the one provided in section 6.2.2.2.2.

6.3.2.4.3 Error outputs

The description other than INA and the condition 5) for ABRT to set to 1b in Error register are the same as the one provided in section 6.2.2.2.3 (conditions from 1) to 4), 6) and 7) are similarly applied). Inceptive Device in the description of INA is replaced by Primal Device and the condition 5) in section 6.2.2.2.3 is replaced by the following.

Error register -

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 5) No Usage Pass was fetched from Qualified Storage by READ USAGE PASS that had

been previously executed.

6.3.2.4.4 Data to be transferred from/to the Host Device

The description is the same as the one provided in section 6.2.2.2.4.

6.3.2.4.5 Prerequisites

The description is the same as the one provided in section 6.2.2.2.5.

6.3.2.4.6 Description

The description is the same as the one provided in section 6.2.2.2.6 other than the phrase Inceptive Device in (1), the keys for encryption in (6) and the explanation related to the state transition. Inceptive Device in appeared in (1) is replaced by Primal Device. As for the keys appeared in (6), $*KP_{d[P]}$ and $K_{s[P]}$ are used instead of $*KP_{d[I]}$ and $K_{s[I]}$. As for the state transition, this subcommand is allowed for the Storage Device to execute after PUT PRIMAL SESSION KEY BT TRANSFER or ENCRYPT USAGE PASS MOVE or ENCRYPT USAGE PASS PLAY or ENCRYPT USAGE PASS COPY (this subcommand itself) was executed on IP Transfer Stage. Moreover, the operations may be concurrently executed for multiple Usage Passes. Then, if the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS is “Not Exist” or “Invalid”, data field of UPwithChecksum is filled with zeros.

6.3.2.5 ENCRYPT USAGE PASS MOVE

6.3.2.5.1 Inputs

The description is the same as the one provided in section 6.2.2.3.1.

6.3.2.5.2 Normal outputs

The description is the same as the one provided in section 6.2.2.3.2.

6.3.2.5.3 Error outputs

The description other than the INA, IC, IFM, and the condition 5) for ABRT to set to 1b in Error register is the same as the one provided in section 6.2.2.3.3 (conditions from 1) to 4), 6) and 9) are similarly applied). Inceptive Device in the description of INA is replaced by Primal Device and the description about IC and IFM, and the condition 5) in section 6.2.2.3.3 are replaced by the following.

Error register -

IC shall be set to 1b if Output UP AC_s COUNT is greater than COUNT (of all the valid Usage Pass existing in the Buf.QSTC) – 1 when FM is set to 01b.

IFM shall be set to 1b if Output UP AC_s COUNT is not 0h and FM of all the valid Usage Pass existing in the Buf.QSTC are not 01b (Copy Count).

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 5) No Usage Pass was fetched from Qualified Storage by READ USAGE PASS that had been previously executed.

6.3.2.5.4 Data to be transferred from/to the Host Device

The description is the same as the one provided in section 6.2.2.3.4.

6.3.2.5.5 Prerequisites

The description is the same as the one provided in section 6.2.2.3.5.

6.3.2.5.6 Description

The description is the same as the one provided in section 6.2.2.3.6 other than the phrase Inceptive Device in (1), the keys for encryption in (7), process (3), and the explanation related to the state transition. Inceptive Device in appeared in (1) is replaced by Primal Device. As for the keys appeared in (7), $*KP_{d[P]}$ and $K_{s[P]}$ are used instead of $*KP_{d[I]}$ and $K_{s[I]}$. As for the process described in (3), MB is checked instead of MU. If MB is 1b, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution. As for the state transition, this subcommand is allowed for the Storage Device to execute after PUT PRIMAL SESSION KEY BT TRANSFER or ENCRYPT USAGE PASS COPY or ENCRYPT USAGE PASS PLAY or ENCRYPT USAGE PASS MOVE (this subcommand itself) was executed on IP Transfer Stage. Moreover, the operations may be concurrently executed for multiple Usage Pass. Then, if the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS is “Not Exist” or “Invalid”, data field of UPwithChecksum is filled with zeros.

6.3.2.6 ENCRYPT USAGE PASS PLAY

6.3.2.6.1 Inputs

The description is the same as the one provided in section 6.2.2.4.1.

6.3.2.6.2 Normal outputs

The description is the same as the one provided in section 6.2.2.4.2.

6.3.2.6.3 Error outputs

The description other than INA and the condition 5) for ABRT to set to 1b in Error register are the same as the one provided in section 6.2.2.4.3 (conditions from 1) to 4), 6) and 7) are similarly applied). Inceptive Device in the description of INA is replaced by Primal Device and the condition 5) in section 6.2.2.4.3 is replaced by the following.

Error register -

ABRT shall be set to 1b if the received subcommand or the result of the execution of it is in the following states:

- 5) No Usage Pass was fetched from Qualified Storage by READ USAGE PASS that had been previously executed.

6.3.2.6.4 Data to be transferred from/to the Host Device

The description is the same as the one provided in section 6.2.2.4.4.

6.3.2.6.5 Prerequisites

The description is the same as the one provided in section 6.2.2.4.5.

6.3.2.6.6 Description

The description is the same as the one provided in section 6.2.2.4.6 other than the phrase Inceptive Device in (1), the keys for encryption in (6) and the explanation related to the state transition. Inceptive Device in appeared in (1) is replaced by Primal Device. As for the keys appeared in (6), $*KP_{d[P]}$ and $K_{s[P]}$ are used instead of $*KP_{d[I]}$ and $K_{s[I]}$. As for the state transition, this subcommand is allowed for the Storage Device to execute after PUT PRIMAL SESSION KEY BT TRANSFER or ENCRYPT USAGE PASS COPY or ENCRYPT USAGE PASS MOVE or ENCRYPT USAGE PASS PLAY (this subcommand itself) was executed on IP Transfer Stage. Moreover, the operations may be concurrently executed for multiple Usage Pass. Then, if the validity of a Usage Pass fetched from Qualified Storage by READ USAGE PASS is “Not Exist” or “Invalid”, data field of UPwithChecksum is filled with zeros.

6.3.2.7 READ USAGE PASS

6.3.2.7.1 Inputs

The description is the same as the one provided in section 6.2.2.5.1.

6.3.2.7.2 Normal outputs

The description is the same as the one provided in section 6.2.2.5.2.

6.3.2.7.3 Error outputs

The description is the same as the one provided in section 6.2.2.5.3.

6.3.2.7.4 Data to be transferred from/to the Host Device

The description is the same as the one provided in section 6.2.2.5.4.

6.3.2.7.5 Prerequisites

The description is the same as the one provided in section 6.2.2.5.5.

6.3.2.7.6 Description

After receiving this subcommand, the Storage Device fetches a Usage Pass from Qualified Storage to Buf.QSTC. Then, the sector size is 1 to 256 is possible as specified in Sector Count register. A sector count of 0 requests 256 sectors. However, if the Host Interface Unit specifies Transferred Sector Count exceeding Maximum Transferred Sector Count (see Table 6.30), the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort this subcommand execution.

If READ USAGE PASS was executed before executing another READ USAGE PASS, all Usage Passes which were fetched by the previous READ USAGE PASS and exists in Buf.QSTC shall be flushed by the time when another Usage Passes were fetched by another READ USAGE PASS.

The DRQ bit is always set to 1b prior to data fetch regardless of the presence or absence of an

error condition.

This subcommand is allowed for the Storage Device to execute if a Connection has been established between the Usage Pass Transfer Unit in the Primal Device and the Usage Pass Transfer Unit in the Storage Device. This subcommand execution is allowed not only after GET INCEPTIVE SESSION KEY BT CONNECTION (end of Connection Stage) or GET INCEPTIVE SESSION KEY BT RECONNECTION (end of Reconnection Stage), but also after CREATE INCEPTIVE SESSION KEY BT TRANSFER (first step of PI Transfer and IP Recovery Stage), PUT PRIMAL SESSION KEY BT TRANSFER (first step of IP Transfer Stage) or READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within UP Inquiry Stage.

6.3.2.8 WRITE USAGE PASS

This subcommand is obsolete.

6.3.3 Subcommands derived from WRITE QUALIFIED

Protocol is PIO data out.

6.3.3.1 PUT PRIMAL CHALLENGE KEY BT CONNECTION

6.3.3.1.1 Inputs

The description is the same as the one provided in section 6.2.3.4.1.

6.3.3.1.2 Normal outputs

The description is the same as the one provided in section 6.2.3.4.2.

6.3.3.1.3 Error outputs

The description is the same as the one provided in section 6.2.3.4.3.

6.3.3.1.4 Data to be transferred from the Host Device

PUT PRIMAL CHALLENGE KEY BT CONNECTION information of which size is one sector is set in the Data register. The structure is shown in Table 6.33. In the information, a Challenge Key generated in the Primal Device on Connection Stage is included; $E(KP_{dc[I]}, K_{ch[P]}) || C(K_r, KP_{dc[P]})$. The structure of the data is described as Primal_Challenge in SAFIA/PDS2.

Table 6.33 PUT PRIMAL CHALLENGE KEY BT CONNECTION information

BP	Length	Descriptions
0	N (from 428 to 492)	Primal_Challenge
N	$512 - N$	Filled with zeros

6.3.3.1.5 Prerequisites

The description is the same as the one provided in section 6.2.3.4.5.

6.3.3.1.6 Description

After receiving this subcommand, the Storage Interface Unit sets one sector data which includes a Challenge Key $K_{ch[P]}$ generated in the Primal Device with Device Class Certificate $C(K_r, KP_{dc[P]})$ installed in the Primal Device into the Data register. $K_{ch[P]}$ is encrypted with $KP_{dc[I]}$ only.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Verifying $C(K_r, KP_{dc[P]})$ with KP_r and $RDCL_{[I]}$ which are installed and recorded respectively in the Storage Device. If the verification fails or the Device Class Certificate is the revoked one, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (2) Decrypting the data with $K_{dc[I]}$.
- (3) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET INCEPTIVE CHALLENGE KEY BT CONNECTION.

- (4) Creating a Challenge Key $K_{ch[I]}$.
- (5) Concatenating $K_{ch[I]}$ with $KP_{d[I]}$ installed in the Storage Device.
- (6) Encrypting the concatenated data with $KP_{dc[P]}$.
- (7) Concatenating $RDCL_{[I]}$ recorded in the Storage Device with the encrypted data $E(KP_{dc[P]}, K_{ch[I]} || KP_{d[I]})$.
- (8) Encrypting the concatenated data $E(KP_{dc[P]}, K_{ch[I]} || KP_{d[I]} || RDCL_{[I]})$ with $K_{ch[P]}$.

This subcommand is allowed for the Storage Device to execute after GET DEVICE CLASS CERTIFICATE or PUT PRIMAL CHALLENGE KEY BT CONNECTION (this subcommand itself) was executed on Connection Stage.

6.3.3.2 PUT PRIMAL SESSION KEY BT CONNECTION

6.3.3.2.1 Inputs

The description is the same as the one provided in section 6.2.3.5.1.

6.3.3.2.2 Normal outputs

The description is the same as the one provided in section 6.2.3.5.2.

6.3.3.2.3 Error outputs

The description is the same as the one provided in section 6.2.3.5.3.

6.3.3.2.4 Data to be transferred from the Host Device

PUT PRIMAL SESSION KEY BT CONNECTION information of which size is N sectors or one sector is set into the Data register. The size is determined in accordance with the values of TSU. The structure is shown in Table 6.34. In the information, a Session Key generated in the Primal

Device on Connection Stage and Device Public Key installed in the Primal Device are included; $E(K_{ch[I]}, E(KP_{d[P]}, K_{s[P]} || KP_{d[P]} || MVB_{[P]} || RDCL_{[P]}))$. The structure of the data is described as Initial_PrimalSession in SAFIA/PDS2.

Table 6.34 PUT PRIMAL SESSION KEY BT CONNECTION information

BP	Length	Descriptions
0	N	Initial_PrimalSession
N	$512 \times \text{SectorNumber}(N) - N$	Filled with zeros

6.3.3.2.5 Prerequisites

The description is the same as the one provided in section 6.2.3.5.5.

6.3.3.2.6 Description

After receiving this subcommand, the Storage Interface Unit receives N sector data which includes a Session Key $K_{s[P]}$ generated in the Primal Device, Device Public Key $KP_{d[P]}$ and Revoked Device Class List $RDCL_{[P]}$, which are installed or recorded in the Primal Device respectively, all at once or sector-by-sector. If TSU is set to 0b, the data is set into Data register all at once. If TSU is set to 1b, the data is set into Data register one sector at a time. Note that $RDCL_{[P]}$ is included if the issue date of $RDCL_{[I]}$ sent from the Storage Device is older than the issue date of $RDCL_{[P]}$ recorded in the Primal Device. $K_{s[P]}$ and $KP_{d[P]}$ are whereat doubly encrypted with $KP_{d[I]}$ and $K_{ch[I]}$, $RDCL_{[P]}$ is meanwhile encrypted with $K_{ch[I]}$ only.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Decrypting the data with $K_{ch[I]}$ and $K_{d[I]}$.
- (2) Checking the structure of the decrypted data. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (3) Verifying $RDCL_{[P]}$ if it is included in the received data. If the verification of Checksum included in Initial_PrimalSession fails, the Usage Pass Transfer Unit in the Storage Module and the Storage Interface Unit aborts the execution.
- (4) Comparing the issue date of $RDCL_{[P]}$ and $RDCL_{[I]}$.
- (5) Overwriting $RDCL_{[I]}$ with the $RDCL_{[P]}$ if the verification described in (3) succeeds and the issue date of $RDCL_{[I]}$ is older than the issue date of $RDCL_{[P]}$ as the result of the comparison described in (4).
- (6) Invalidating all entries of Connection Log if $RDCL_{[I]}$ is updated in (5). In this case, all entries of Transaction Log are also invalidated if SAFIA UT feature set is implemented on the Storage Device.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET INCEPTIVE SESSION KEY BT CONNECTION.

- (7) Creating a Session Key $K_{s[I]}$, which is shared in Connection Stage.
- (8) Encrypting $K_{s[I]}$ with $K_{s[P]}$ and $KP_{d[P]}$.

This subcommand is allowed for the Storage Device to execute after GET INCEPTIVE CHALLENGE KEY BT CONNECTION or PUT PRIMAL SESSION KEY BT CONNECTION (this subcommand itself) was executed on Connection Stage.

6.3.3.3 PUT PRIMAL SESSION KEY BT RECONNECTION

6.3.3.3.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	0	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	fz				CL Entry Pointer			
LBA Mid	fz							
LBA High	fz							
Device	obs	na	obs	DEV	fz			
Command	ACh							

Feature register -

Bit7, bit6 and bit3 shall be set to 1b. Bit5 and bit4 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

LBA Low -

CL Entry Pointer shall be set to a value which designates the objective entry of Connection Log to execute Reconnection Stage. The value was notified from the Storage Device to the Host Device in GET SAFIA FEATURES BT information (see Table 6.30). CL Entry Pointer shall be set to 1h, if the Host Device tries to execute Reconnection Stage with the entry of Connection Log in which SNPD1 (in GET SAFIA FEATURES information) is recorded as Primal Device Specifier. Similarly, Host Device shall set 2h to execute Reconnection Stage with the entry of Connection Log for SNPD2, and so forth. CL Entry Pointer shall be set to 0h to execute Reconnection Stage with the entry of Connection Log which is designated by Recovery-Allowed Primal Device Indicator. CL Entry Pointer shall also be set to 0h if MVB_[i] in the objective entry of Connection Log is 0000h.

Device register -

DEV shall specify the selected Storage Device.

6.3.3.3.2 Normal outputs

The description is the same as the one provided in section 6.2.3.6.2.

6.3.3.3.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	IEN	na	na	na	ABRT	NRDY	na
Sector Count	na							
LBA Low	na							
LBA Mid	na							
LBA High	na							
Device	obs	na	obs	DEV	na			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

The description other than the conditions for IEN and ABRT to set to 1b in Error register is the same as the one provided in section 6.2.3.6.3 (conditions from 1) to 6) are similarly applied). The condition for IEN and an additional condition for ABRT to set to 1b in Error register are as the followings.

IEN shall be set to 1b if the following conditions are satisfied:

- 1) No information is recorded on the entry designated by CL Entry Pointer.
- 2) CL Entry Pointer does not coincide with the Entry Pointer in Recovery_PrimalConnection described in SAFIA/PDS2 (ref. description (3)).
- 3) CL Entry Pointer is 00h when RAPDI in Storage Device does not designate any Connection Log Entry.

The additional condition for ABRT shall be set to 1b is as the following:

- 7) IEN in Error register is set to 1b.
- 8) CL Entry Pointer is greater than 0h when MVB_[P] is 00h.

6.3.3.3.4 Data to be transferred from the Host Device

PUT PRIMAL SESSION KEY BT RECONNECTION information of which size is one sector is set in the Data register. The structure is shown in Table 6.35. In the information, a Session Key generated in the Primal Device on Reconnection Stage is included; $E(KP_{d[I]CL}, E(K_{s[I]CL}, K_{s[P]}))$. The structure of the data is described as Recovery_PrimalConnection in SAFIA/PDS2.

Table 6.35 PUT PRIMAL SESSION KEY BT RECONNECTION information

BP	Length	Descriptions
0	114	Recovery_PrimalConnection
114	398	Filled with zeros

6.3.3.3.5 Prerequisites

The description is the same as the one provided in section 6.2.3.6.5.

6.3.3.3.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Session Key $K_{s[P]}$ generated in the Primal Device. $K_{s[P]}$ is doubly encrypted with $K_{s[I]CL}$ and $KP_{d[I]CL}$ which are fetched from Connection Log recorded in the Primal Device.

When the Storage Interface Unit receives the data, the Storage Module processes the following

if the execution of the subcommand which had been previously received has completed.

- (1) Selecting the entry of Connection Log; If CL Entry Pointer is 0h, the entry designated by Recovery-Allowed Primary Device Indicator shall be selected. In other cases, entry designated by CL Entry Number shall be selected.
- (2) Decrypting the data with $K_{s[|]CL}$ fetched from Connection Log and $K_{d[|]}$ installed in the Storage Device.
- (3) Checking coincidence of the CL Entry Pointer set in Command Block register and Entry Pointer included in Recovery_PrimalConnection. If $MVB_{[P]}$ recorded in the objective entry of Connection Log is greater than 0000h and CL Entry Pointer is different from Entry Pointer, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (4) Checking Recovery-Allowed Primal Device Indicator; if the Indicator designates the objective entry of the Connection Log or CL Entry Pointer is 0h, Recovery Permission Indicator is allowed to set to 01h. In other cases, Recovery Permission Indicator shall be set to 00h.

The followings are not necessarily executed. If the processes are not executed, they shall be executed after receiving GET INCEPTIVE SESSION KEY BT RECONNECTION.

- (5) Creating a Session Key $K_{s[|]}$, which is shared in Reconnection Stage.
- (6) Encrypting $K_{s[|]}$ with $K_{s[P]CL}$ and $KP_{d[P]CL}$.

This subcommand is allowed for the Storage Device in any state to execute if a Channel specified with the Channel Identifier has been opened in BT mode. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Reconnection Stage.

6.3.3.4 PUT PRIMAL SESSION KEY BT TRANSFER

6.3.3.4.1 Inputs

The description is the same as the one provided in section 6.2.3.3.1.

6.3.3.4.2 Normal outputs

The description is the same as the one provided in section 6.2.3.3.2.

6.3.3.4.3 Error outputs

The description is the same as the one provided in section 6.2.3.3.3.

6.3.3.4.4 Data to be transferred from the Host Device

PUT PRIMAL SESSION KEY BT TRANSFER information of which size is 512-byte is set in the Data register. The structure is shown in Table 6.36. In the information, a Session Key generated in the Primal Device on Transfer Stage is included; $E(K_{s[|]}, E(K_{s[P]n}, K_{s[P]n+1}))$, where $K_{s[P]n}$ is the Session Key generated most recently in the Primal Device and $K_{s[|]}$ is the Session Key generated most recently in itself. The structure of the data is described as Transfer_PrimalSession in

SAFIA/PDS2.

Table 6.36 PUT PRIMAL SESSION KEY BT TRANSFER information

BP	Length	Descriptions
0	50	Transfer_PrimalSession
50	462	Filled with zeros

6.3.3.4.5 Prerequisites

The description is the same as the one provided in section 6.2.3.3.5.

6.3.3.4.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Session Key $K_{s[P]n+1}$ generated in the Primal Device. $K_{s[P]n+1}$ is doubly encrypted with $K_{s[P]n}$ and $K_{s[I]}$.

When the Storage Interface Unit receives the data, the Usage Pass Transfer Unit in the Storage Device decrypts the data with $K_{s[P]n}$ and $K_{s[I]}$, where $K_{s[P]n}$ was a Session Key shared most recently through Connection or Reconnection or IP Transfer Stage executed in the past and $K_{s[I]}$ was also a Session Key shared most recently through Connection or Reconnection or PI Transfer Stage executed in the past.

This subcommand is allowed for the Storage Device to execute if a Connection has been established between the Primal Device and the Storage Device. The condition means that the subcommand execution is allowed not only after GET INCEPTIVE SESSION KEY BT CONNECTION (end of Connection Stage) or GET INCEPTIVE SESSION KEY BT RECONNECTION (end of Reconnection Stage) but also after SEARCH USAGE PASS BT RECOVERY (first step of TS Creation Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within IP Transfer Stage.

6.3.3.5 PUT USAGE PASS

6.3.3.5.1 Inputs

The description other than the value of Transferred Sector Count in Sector Count register is the same as the one provided in section 6.2.3.7.1.

Sector Count register -

Transferred Sector Count shall be set to a number of sectors to be transferred. A value of 00h specifies that 256 sectors are to be transferred.

6.3.3.5.2 Normal outputs

The description is the same as the one provided in section 6.2.3.7.2.

6.3.3.5.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	ICC	IDNF	na	ABRT	NRDY	ICD
Sector Count	na							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	na	obs	DEV	LBAQ (27:24)			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

The description other than the conditions for ICC, ICD and 6) for ABRT to set to 1b in Error register is the same as the one provided in section 6.2.3.7.3 (conditions from 1) to 5) and from 7) to 8) for ABRT are similiary applied, therefore they are renumbered from 1) to 7)). The condition for ICD and the additional condition for ICC and ABRT to set to 1b in Error register are as the followings.

Error register -

The additional condition for ICC to set to 1b in Error register is as the following: ICC shall be set to 1b even if one of the plural received Usage Passes is not allowed to be written into Qualified Storage in terms of the Control Count (see section 7.3.1 of SAFIA/PDS1).

ICD shall be set to 1b if the LBAQ described in section 6.3.3.5.1 is different from the Domicile described in section 6.3.3.5.4.

The additional condition for ABRT shall be set to 1b is as the following:

- 9) ICD in the Error register is set to 1b.

6.3.3.5.4 Data to be transferred from the Host Device

PUT USAGE PASS information of which size is N sectors is set into the Data register. The structure is shown in Table 6.37. In the information, multiple Transfer_UsagePass(es) are included. A Transfer_UsagePass includes a Usage Pass an Action Indicator and a Checksum; $E(*KP_{d[i]}$, $E(K_{s[i]}$, UP || AI || CKS)). It is noted that only the first Transfer_UsagePass includes a Usage Pass, an Action Indicator, a Checksum and a Domicile. The Domicile is the same as the LBAQ described in section 6.3.3.5.1; $E(*KP_{d[i]}$, $E(K_{s[i]}$, UP || AI || CKS || Domicile)). The structure of the data is described as Transfer_UsagePass in SAFIA/PDS2.

Table 6.37 PUT USAGE PASS information

BP	Length	Field
0	372	Transfer_UsagePass (1) including Domicile
372	140	Filled with zeros
512	372	Transfer_UsagePass (2)
884	140	Filled with zeros
		Repetition of one sector unit where a Transfer_UsagePass are Included

The structure of Domicile in Transfer_UsagePass (1) is shown in Table 6.38.

Table 6.38 The structure of Domicile

bit BP	7	6	5	4	3	2	1	0
0	0	0	0	0	LBAQ (27:24)			
1	LBAQ (23:16)							
2	LBAQ (15:8)							
3	LBAQ (7:0)							

6.3.3.5.5 Prerequisites

The description is the same as the one provided in section 6.2.3.7.5.

6.3.3.5.6 Description

After receiving this subcommand, the Storage Interface Unit receives N sector data which includes a Usage Pass, Action Indicator and Checksum. Then, N is 1 to 256 is possible as specified in Sector Count register. A sector count of 0 requests 256 sectors. However, if the Host Interface Unit specifies Transferred Sector Count exceeding Maximum Transferred Sector Count which Storage Interface Unit noticed to the Host Interface Unit in GET SAFIA FEATURES BT information (Table 6.30), the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort this subcommand execution.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Decrypting the data with $*K_{d[i]}$ and $K_{s[i]}$.
- (2) Checking the structure of the decrypted data by the calculation of Checksum. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (3) Checking the integrity of the specified LBAQ by verifying whether the LBAQ and Domicile in the first Transfer_UsagePass coincides or not, when $MVB_{[P]}$ recorded in the entry of Connection Log, which was created/updated in the Connection/Reconnection Stage, is greater than 0000h. If (i) up_domicile field does not exist in the first Transfer_UsagePass, or (ii) up_domicile field regularly exists there but the two values differ, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (4) Setting Recovery-Allowed Primal Device Indicator to designate the entry of Connection Log if the Indicator does not designate the entry.
- (5) Modifying Control Count appropriately.
- (6) Writing the Usage Pass existing in Buf.QSTC to Qualified Storage and validate it.

This subcommand is allowed for the Storage Device to execute after GET INCEPTIVE SESSION KEY BT TRANSFER was executed on PI Transfer and IP Recovery Stage. Iterative execution of the subcommand is not allowed. When the subcommand execution is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit shall transit to a particular state which is for “Usage Pass movement is completed”.

6.3.3.6 RECOVER USAGE PASS

6.3.3.6.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	0	0	0	0	1	CHID		
Sector Count	Transferred Sector Count							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	1	obs	DEV	LBAQ (27:24)			
Command	ACh							

Feature register -

Bit7 to bit4 shall be set to 0b. Bit3 shall be set to 1b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

LBA Low register -

LBAQ address bits (7:0) shall be set to the register.

LBA Mid register -

LBAQ address bits (15:8) shall be set to the register.

LBA High register -

LBAQ address bits (23:16) shall be set to the register.

Device register [7:4] -

Bit6 shall be set to 1b.

DEV shall specify the selected Storage Device.

Device register [3:0] -

LBAQ address bits (27:24) shall be set to the register.

6.3.3.6.2 Normal outputs

The description is the same as the one provided in section 6.2.3.7.2.

6.3.3.6.3 Error outputs

Register	7	6	5	4	3	2	1	0
Error	CP	WP	na	IDNF	na	ABRT	NRDY	ICD
Sector Count	na							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	na	obs	DEV	LBAQ (27:24)			
Status	BSY	DRDY	DF	na	DRQ	na	na	ERR

The description other than the conditions for ICC, ICD and ABRT set to 1b in Error register is the same as the one provided in section 6.2.3.7.3 (conditions for ABRT to set to 1b in Error register from 1) to 8) are similarly applied). ICC is not configured for this subcommand. ,The condition for

ICD and the additional conditions for ABRT set to 1b are as the followings.

Error register -

ICD shall be set to 1b if the LBAQ described in section 6.3.3.6.1 is different from the Domicile described in section 6.3.3.6.4.

ABRT shall be set to 1b if the received subcommand is in the following states:

- 9) The Usage Pass Transfer Unit in the Storage Device detects the structure error of the Usage Pass of which AC_s is to be overwritten with the received one if the verification of the structure is executed before subcommand completion when BSY is set to 0b.
- 10) The Usage Pass Identifier of the Usage Pass pointed by the the LBAQ which the Host Interface Unit specified differs from the received one.
- 11) ICD in the Error register is set to 1b.

6.3.3.6.4 Data to be transferred from the Host Device

RECOVER USAGE PASS information of which size is one sector is set in the Data register. The structure is shown in Table 6.39. In the information, a Transfer_RestorationAC is included. A Transfer_RestorationAC includes a Usage Pass Identifier, an Access Condition for Storage Module recorded in the Transaction Log and a Domicile. The Domicile is the same as the LBAQ described in section 6.3.3.6.1; $E(*K_{d[1]}, E(K_{s[1]}, UPID || AC_{sTL} || Domicile))$. The structure of the data is described as Transfer_RestorationAC in SAFIA/PDS2.

Table 6.39 RECOVER USAGE PASS information

BP	Length	Field
0	82	Transfer_RestorationAC
82	430	Filled with zeros

The structure of Domicile in Transfer_RestorationAC is the same as Table 6.38.

6.3.3.6.5 Prerequisites

The description is the same as the one provided in section 6.2.3.7.5

6.3.3.6.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Usage Pass Identifier and Access Condition for Storage Module recorded in Transaction Log of Primal Device.

When the Storage Interface Unit receives the data, the Usage Pass Transfer Unit and the Qualified Storage Controller in the Usage Pass Transfer Unit in the Storage Device processes the following if the execution of the subcommand which had been previously received has completed.

- (1) Decrypting the data with $*K_{d[1]}$ and $K_{s[1]}$.
- (2) Verifying the structure of the received data by the calculation of Checksum. If the structure error is detected, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (3) Checking the integrity of the specified LBAQ by verifying whether the LBAQ and Domicile in the Transfer_RestorationAC coincides or not, when $MVB_{[P]}$ recorded in the entry of Connection

Log, which was created/updated in the Connection/Reconnection Stage is greater than 0000h. If (i) up_domicile field does not exist in the Transfer_RestorationAC, or (ii) up_domicile field regularly exist there but the two values differ, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.

- (4) Collating the Usage Pass Identifier with the one recorded in the area pointed by the specified LBAQ. If the collation fails, the Storage Interface Unit and the Usage Pass Transfer Unit in the Storage Device abort the execution.
- (5) Overwriting the AC_s of the Usage Pass in Qualified Storage with the received AC_{sTL} and validate the Usage Pass if it has been invalidated.

This subcommand is allowed for the Storage Device to execute after GET INCEPTIVE SESSION KEY BT TRANSFER was executed on PI Transfer and IP Recovery Stage. Iterative execution of the subcommand is not allowed. When the subcommand execution is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit shall transit to a particular state which is for “Usage Pass movement is completed”.

6.3.3.7 SEARCH USAGE PASS BT RECOVERY

6.3.3.7.1 Inputs

Register	7	6	5	4	3	2	1	0
Features	1	1	0	1	0	CHID		
Sector Count	Transferred Sector Count							
LBA Low	LBAQ (7:0)							
LBA Mid	LBAQ (15:8)							
LBA High	LBAQ (23:16)							
Device	obs	1	obs	DEV	LBAQ (27:24)			
Command	ACh							

Feature register -

Bit7, bit6 and bit4 shall be set to 1b. Bit5 and bit3 shall be set to 0b.

CHID shall be set to Channel Identifier.

Sector Count register -

Transferred Sector Count shall be set to 01h.

LBA Low register -

LBAQ address bits (7:0) shall be set to the register.

LBA Mid register -

LBAQ address bits (15:8) shall be set to the register.

LBA High register -

LBAQ address bits (23:16) shall be set to the register.

Device register [7:4] -

Bit6 shall be set to 1b.

DEV shall specify the selected Storage Device.

Device register [3:0] -

LBAQ address bits (27:24) shall be set to the register.

6.3.3.7.2 Normal outputs

The description is the same as the one provided in section 6.2.3.9.2.

6.3.3.7.3 Error outputs

The description is the same as the one provided in section 6.2.3.9.3.

6.3.3.7.4 Data to be transferred from the Host Device

SEARCH USAGE PASS BT RECOVERY information of which size is one sector is set in the Data register. The structure is shown in Table 6.40. In the information, Usage Pass Identifier is included; UPID. The structure of the data is described as Retrieval_UPID in SAFIA/PDS2.

Table 6.40 SEARCH USAGE PASS BT RECOVERY information

BP	Length	Descriptions
0	36	Retrieval_UPID
36	476	Filled with zeros

6.3.3.7.5 Prerequisites

The description is the same as the one provided in section 6.2.3.9.5.

6.3.3.7.6 Description

After receiving this subcommand, the Storage Interface Unit receives one sector data which includes a Usage Pass Identifier.

When the Storage Interface Unit receives the data, the Storage Module processes the following if the execution of the subcommand which had been previously received has completed.

Checking the state of the Usage Pass pointed by the LBAQ which the Host Interface Unit specified.

- (1) Collating the Usage Pass Identifier of the Usage Pass pointed by the LBAQ which the Host specified with the received one and setting Usage Pass Status in Transaction_Status. If the Usage Pass Identifiers differ or no Usage Pass is recorded, Usage Pass Status is set to “Not Exist”. If the Usage Pass Identifiers coincide, Usage Pass Status is set to “Valid” or “Invalid” according the state of the Usage Pass recorded in Qualified Storage.
- (2) Keyed hash value calculation with $K_{s[P]}$ and $K_{s[I]}$ which were shared most recently, Usage Pass Identifier which the Host specified, AC_s of the specified Usage Pass, the Usage Pass Status set at (1) and Usage Pass Location in terms of LBAQ which the Storage Interface Unit received on this subcommand. Then, data field of ac_storage in tbsAccessCondition is filled with zeros if the state of the Usage Pass checked at (1) is “Not Exist”.
- (3) Concatenating the data: Usage Pass Identifier || Access Condition for Storage Module || Usage Pass Status || Usage Pass Location || keyed hash value obtained at (2). As the result, Transaction_Status defined in section 4.4.17.2 of SAFIA/PDS2 is obtained. It is noted that up_location field of Transaction_Status and tbsAccessCondition consists of two parts. The size of the first part is 6-byte and LBAQ which the Storage Interface Unit received on this

subcommand is set to this field. The size of the second part is 2-byte and Transferred Sector Count which the the Storage Interface Unit received on this subcommand is set to this field.

This subcommand is allowed for the Storage Device to execute if a Connection has been established between the Primal Device and the Storage Device. The condition means that the subcommand execution is allowed not only after GET INCEPTIVE SESSION KEY BT CONNECTION (end of Connection Stage) or GET INCEPTIVE SESSION KEY BT RECONNECTION (end of Reconnection Stage) but also after CREATE INCEPTIVE SESSION KEY BT TRANSFER (first step of PI Transfer and IP Recovery Stage), READ USAGE PASS (first step of UP Inquiry Stage) and so forth. If the Storage Interface Unit receives the subcommand and the execution of the subcommand is completed, the state of the Usage Pass Transfer Unit in the Storage Device and the Storage Interface Unit transit to the first state within Recovery Stage.

7 State transition diagrams

In this chapter, only normal state transition diagrams are described. Each state transition occurs when the execution of a subcommand which is followed by the action including cryptographic operation and so forth completes. The subcommands executed in the Storage Interface Unit and the Storage Module are described on each arrow. Abbreviated subcommand names are following the notations described in Table 4.1, Table 4.2, Table 4.3, Table 4.4, Table 4.5 and Table 4.6. On the subcommand execution, the sequence shall follow the diagram described in this chapter.

In section 7.1, 7.2 and their subsections, state transition diagrams on UT mode and BT mode are respectively described. In section 7.1 and 7.2, top level state transition which starts from channel opening and ends at channel closing is illustrated. In other words, diagrams following “Channel Opened” are illustrated in terms of a specific Channel. Channel opening and closing are accomplished by OPEN CHANNEL and CLOSE CHANNEL. Descriptions of these two subcommands are provided in iVDR/IF. State transitions within each state are described in each following subsection.

Error state transition diagrams are not described in this chapter because transition shall not occur at all (all states remain still) without exception by any errors that occurs on the execution of subcommands included in SAFIA UT and BT feature set.

7.1 State transition diagrams on UT mode

In this section, top level diagram on UT mode is illustrated.

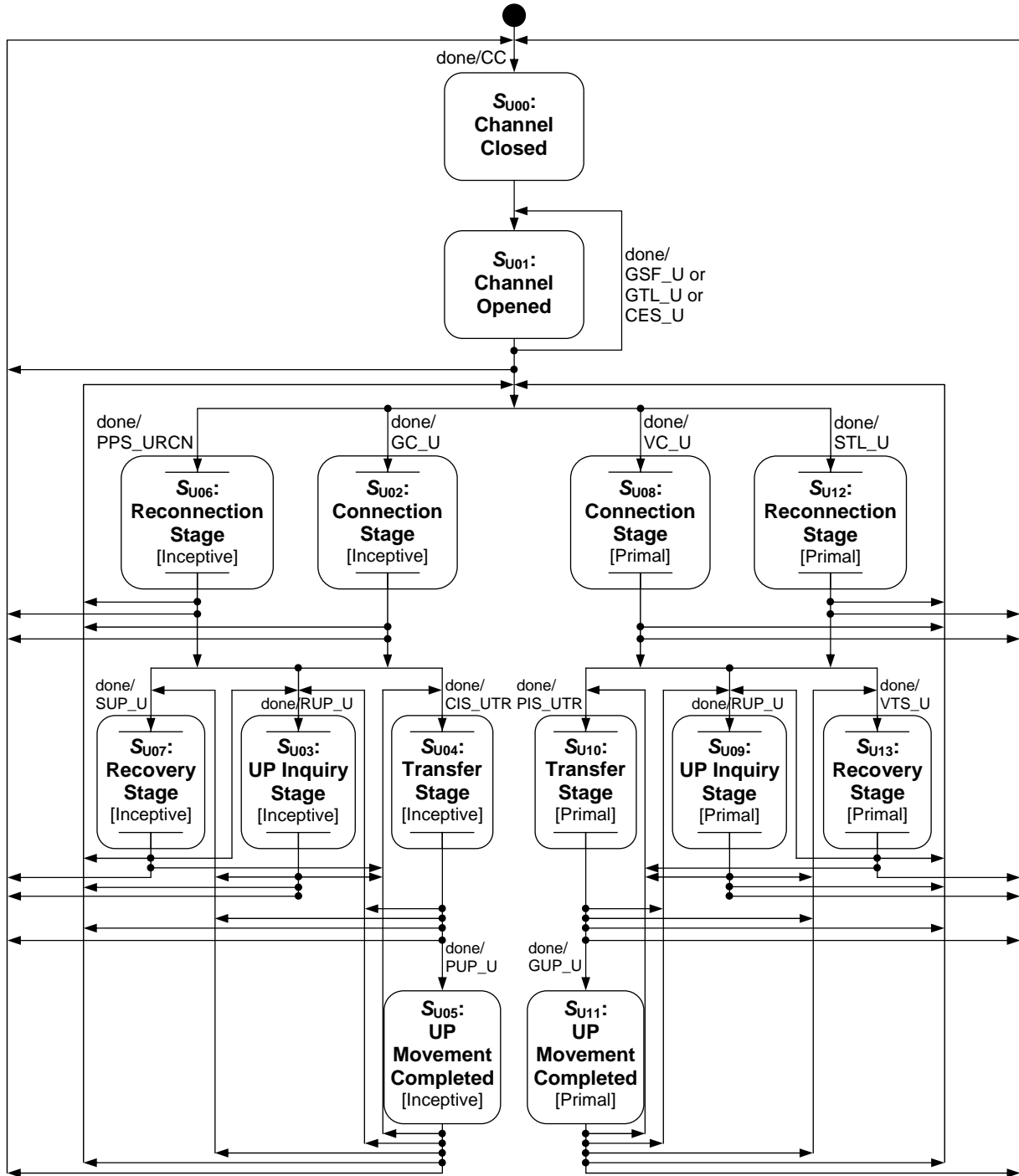


Figure 7.1 State transition diagram for Usage Pass transfer on UT mode

In Figure 7.1, transition from **S_{U00}** to **S_{U01}** is completed when 000b is set to least 3 bits in Sector Count register for OPEN CHANNEL.

7.1.1 State transition diagram within S_{U02}

In this section, substate transition diagram within S_{U02} (Connection Stage on Inceptive Device) is illustrated.

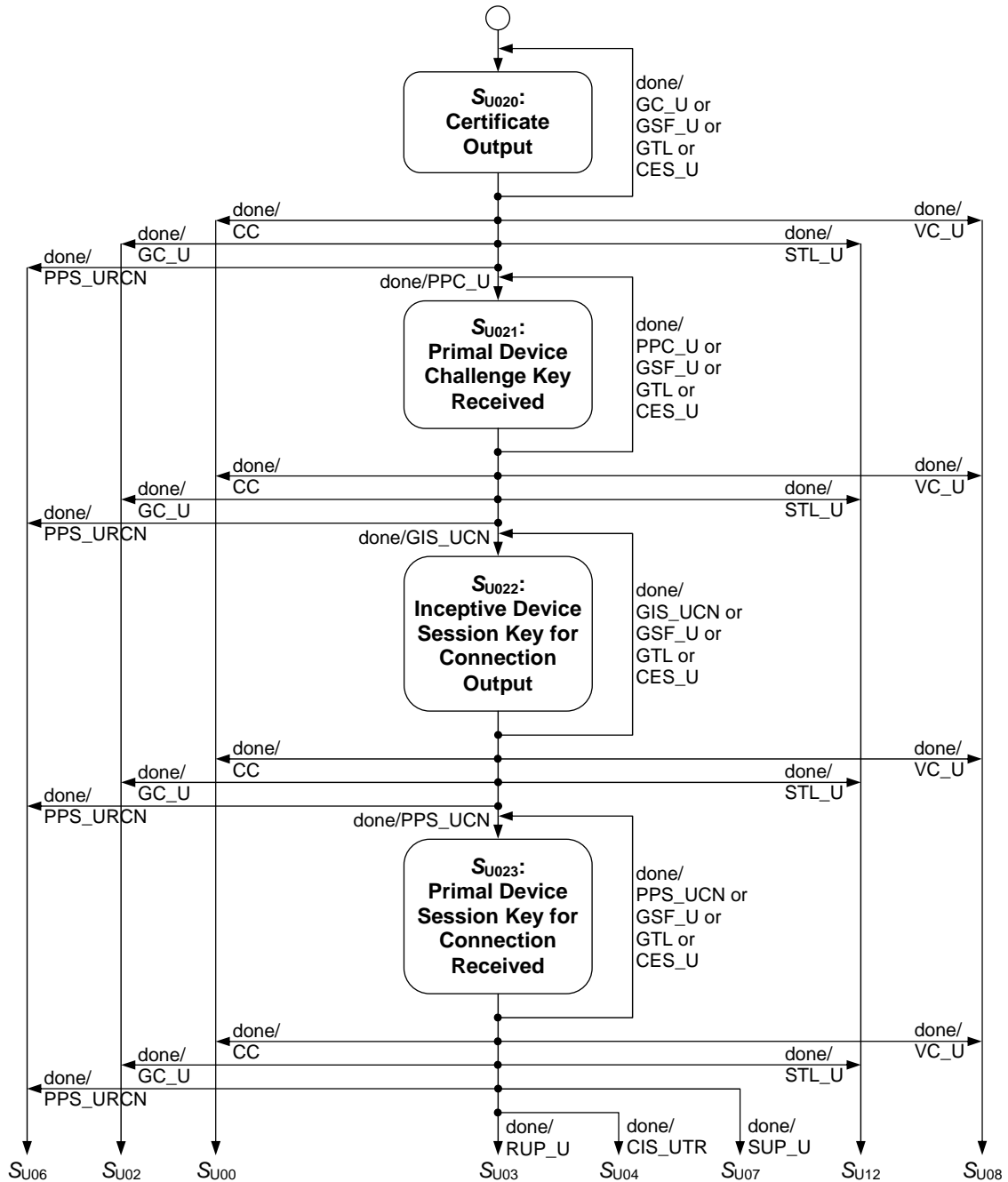


Figure 7.2 Substate transition diagram within S_{U02} (Connection Stage on Inceptive Device)

7.1.2 State transition diagram within S_{U06}

In this section, substate transition diagram within S_{U06} (Reconnection Stage on Inceptive Device) is illustrated.

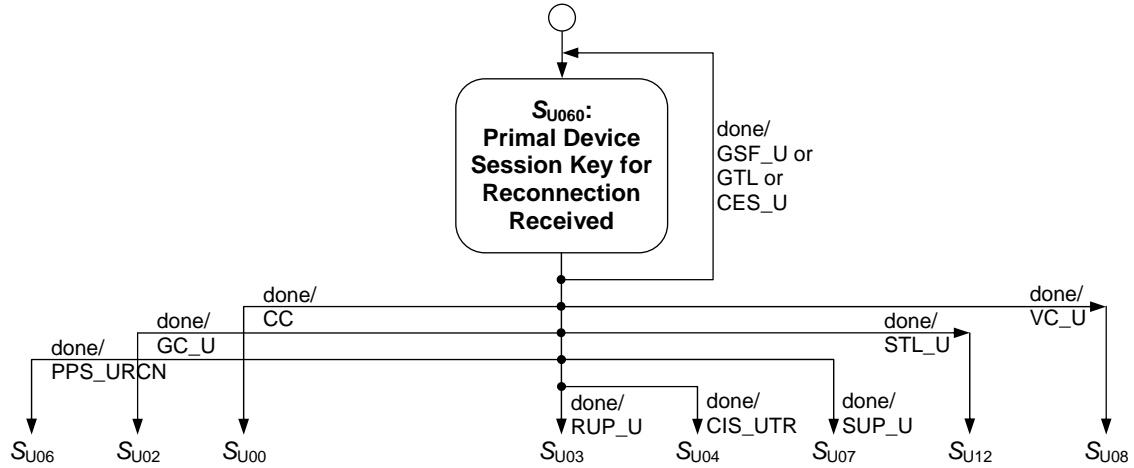


Figure 7.3 Substate transition diagram within S_{U06} (Reconnection Stage on Inceptive Device)

7.1.3 State transition diagram within S_{U03}

In this section, substate transition diagram within S_{U03} (UP Inquiry Stage on Inceptive Device) is illustrated.

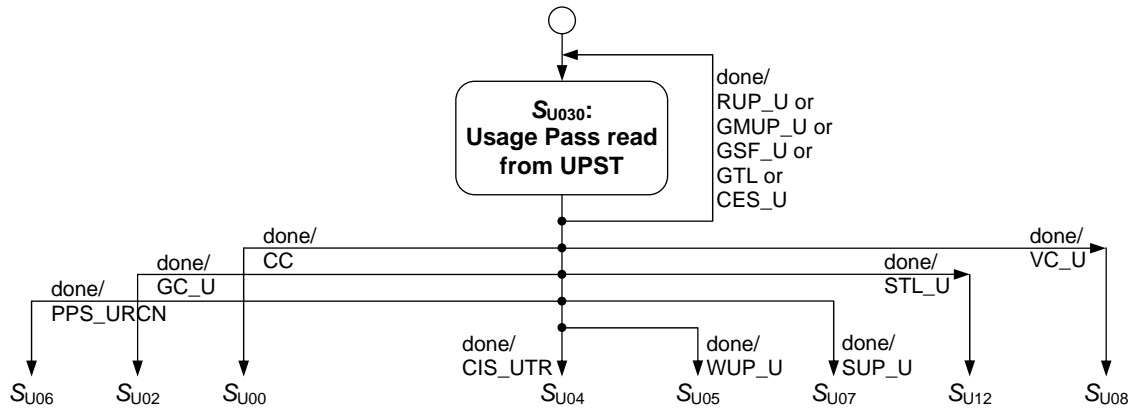


Figure 7.4 Substate transition diagram within S_{U03} (UP Inquiry Stage on Inceptive Device)

7.1.4 State transition diagram within S_{U04}

In this section, substate transition diagram within S_{U04} (Transfer Stage on Inceptive Device) is illustrated.

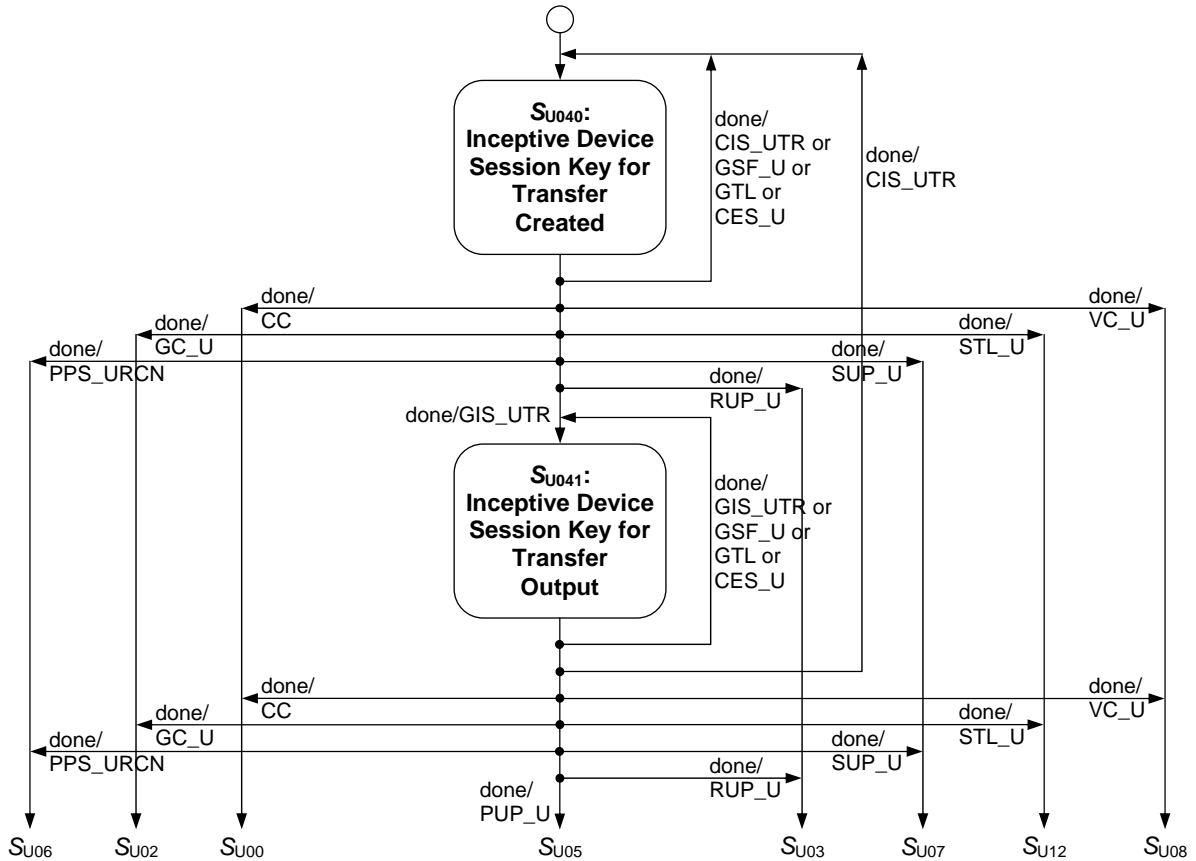


Figure 7.5 Substate transition diagram within S_{U04} (Transfer Stage on Inceptive Device)

7.1.5 State transition diagram within S_{U07}

In this section, substate transition diagram within S_{U07} (Recovery Stage on Inceptive Device) is illustrated.

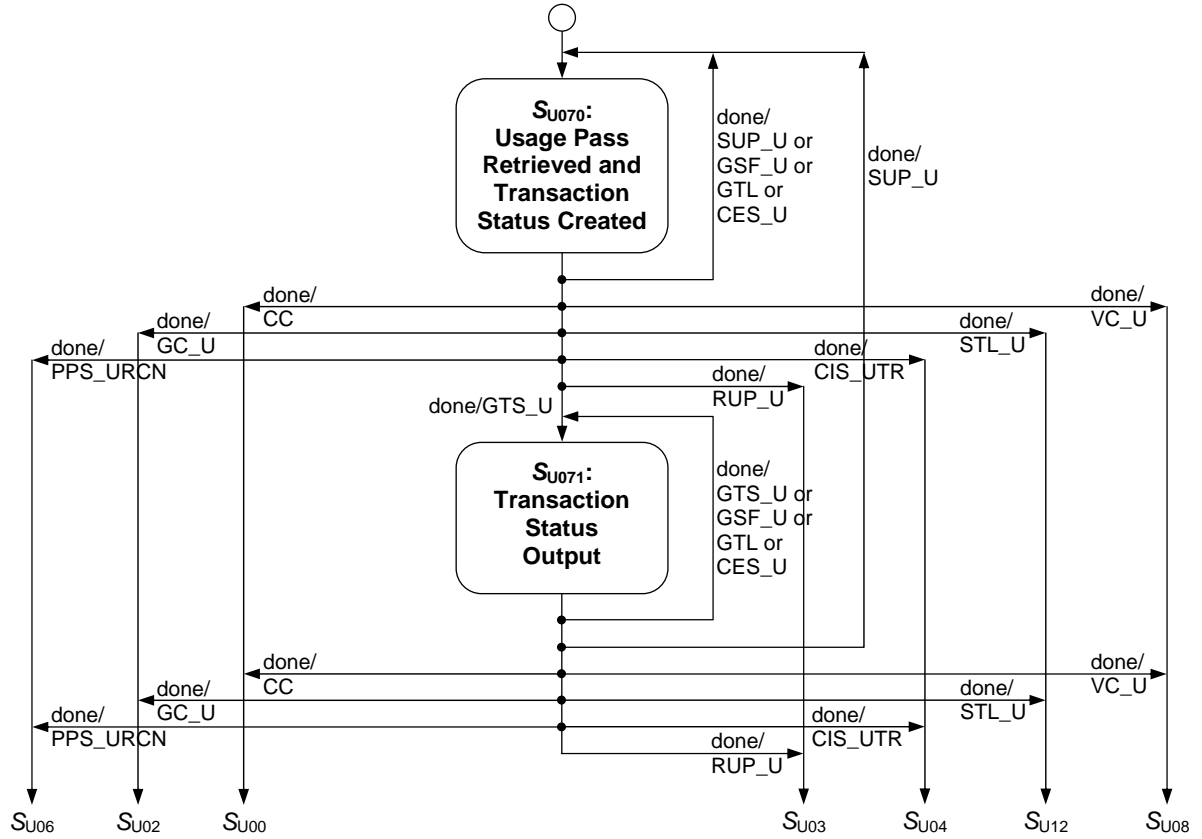


Figure 7.6 Substate transition diagram within S_{U07} (Recovery Stage on Inceptive Device)

7.1.6 State transition diagram within S_{U08}

In this section, substate transition diagram within S_{U08} (Connection Stage on Primal Device) is illustrated.

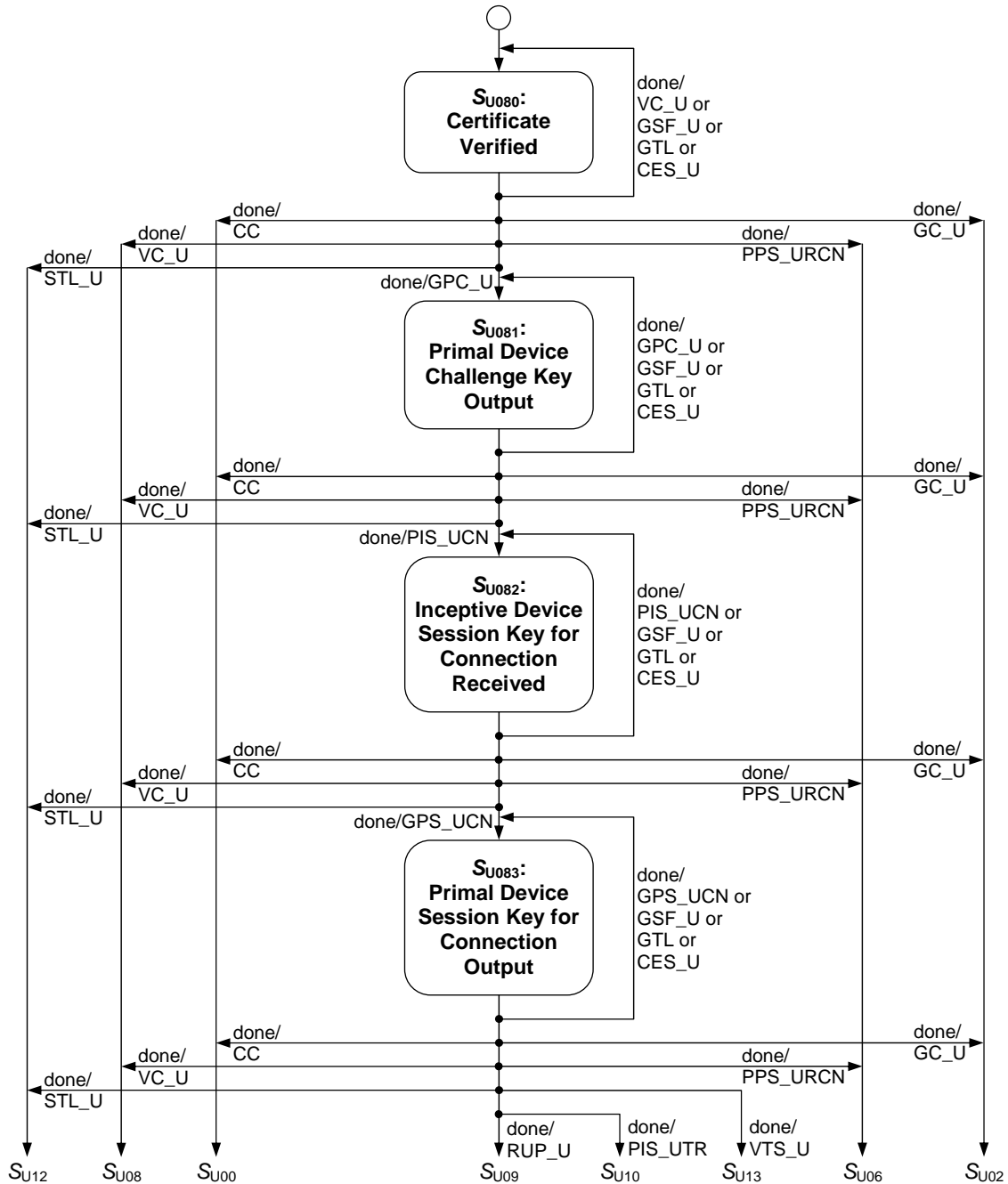


Figure 7.7 Substate transition diagram within S_{U08} (Connection Stage on Primal Device)

7.1.7 State transition diagram within S_{U12}

In this section, substate transition diagram within S_{U12} (Reconnection Stage on Primal Device) is illustrated.

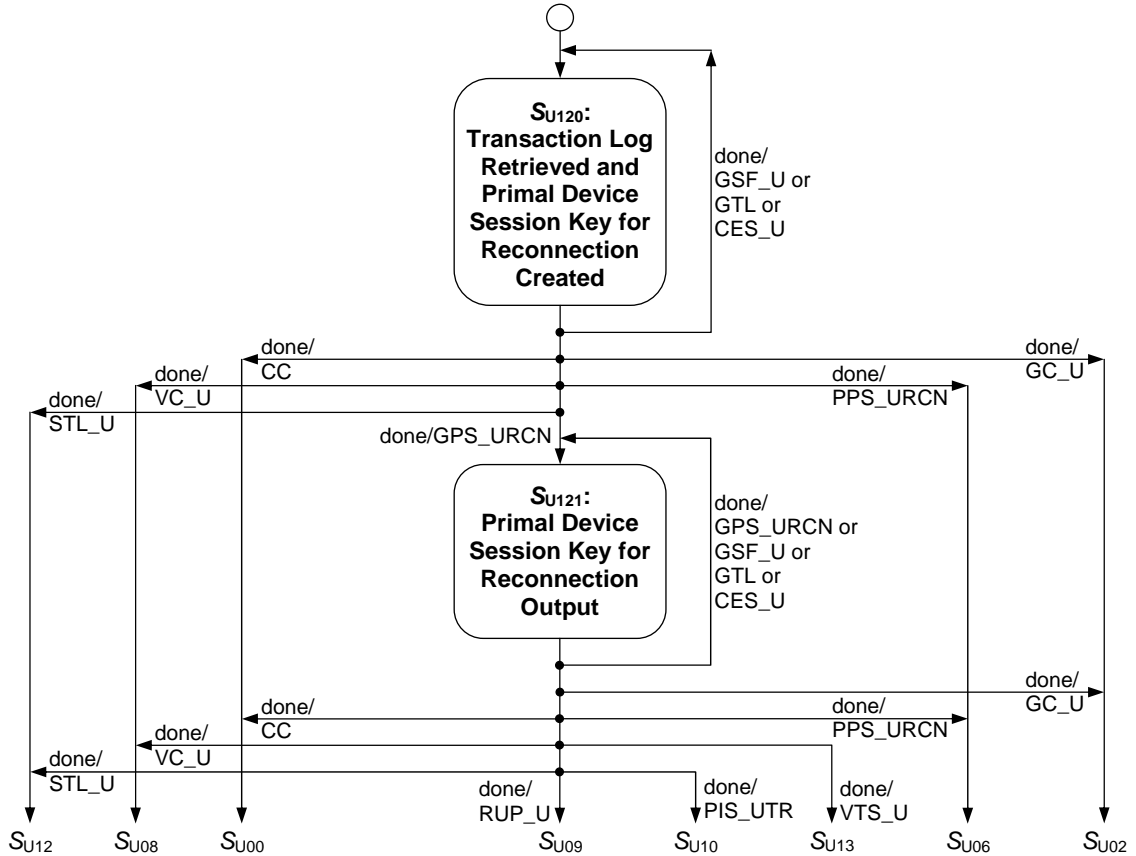


Figure 7.8 Substate transition diagram within S_{U12} (Reconnection Stage on Primal Device)

7.1.8 State transition diagram within S_{U09}

In this section, substate transition diagram within S_{U09} (UP Inquiry Stage on Primal Device) is illustrated.

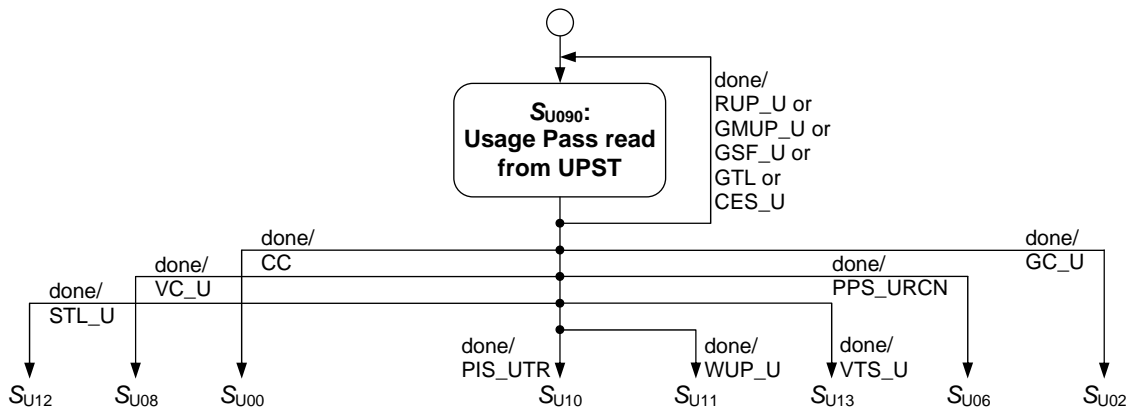


Figure 7.9 Substate transition diagram within S_{U09} (IP Inquiry Stage on Primal Device)

7.1.9 State transition diagram within S_{U10}

In this section, substate transition diagram within S_{U10} (Transfer Stage on Primal Device) is illustrated. In Figure 7.10, the letter “x” means “C” or “M” or “P”.

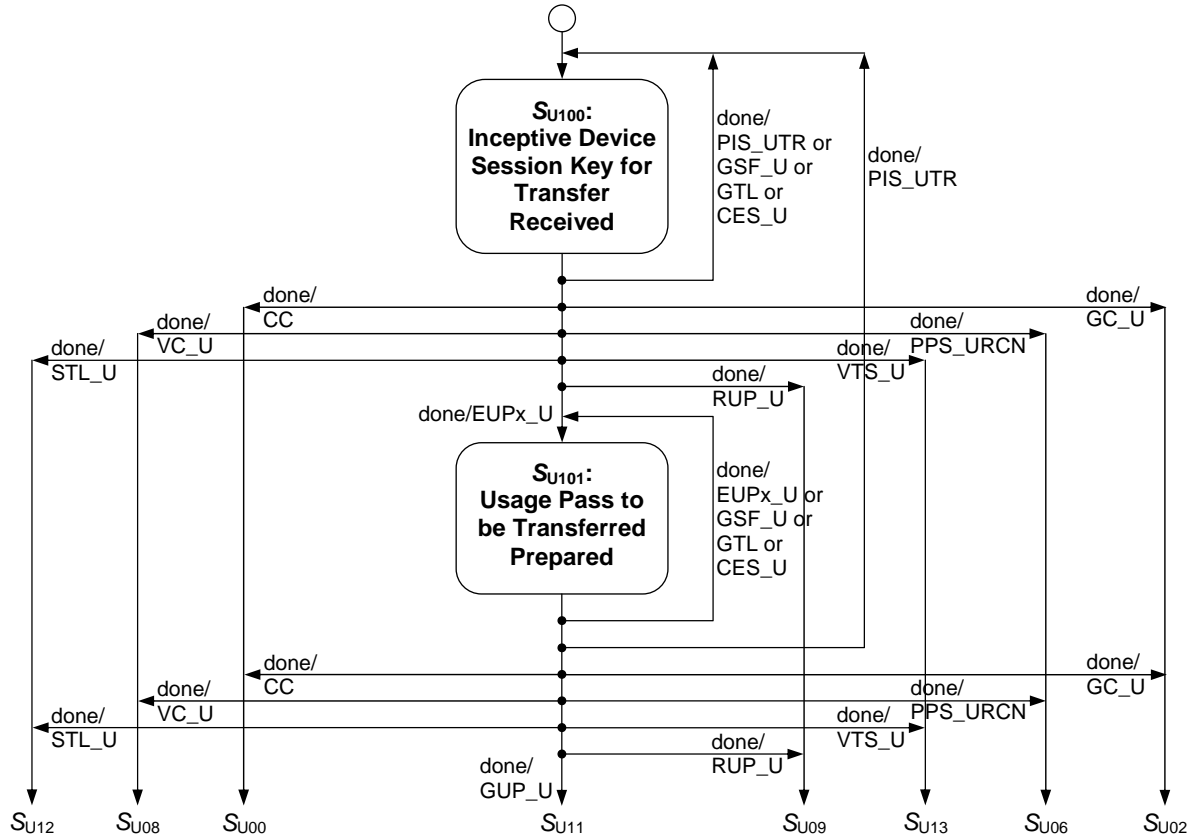


Figure 7.10 Substate transition diagram within S_{U10} (Transfer Stage on Primal Device)

7.1.10 State transition diagram within S_{U13}

In this section, substate transition diagram within S_{U13} (Recovery Stage on Primal Device) is illustrated.

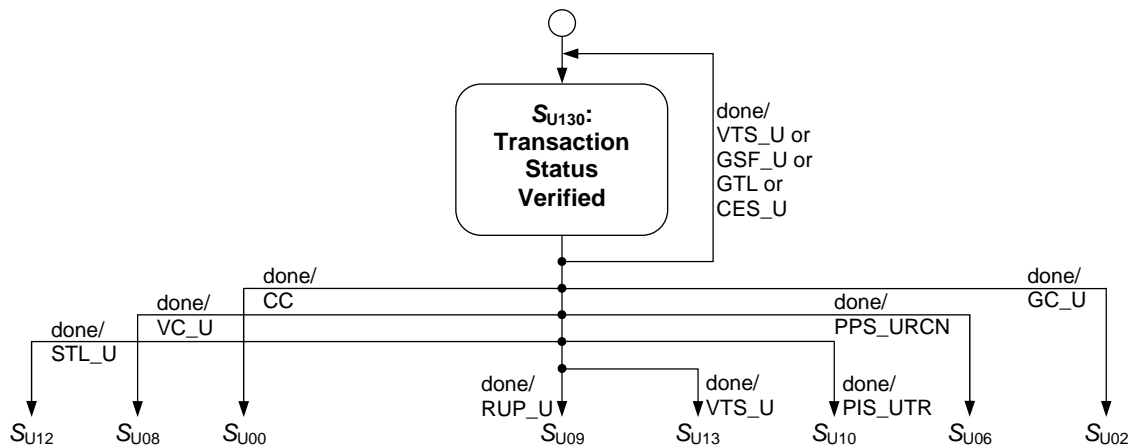


Figure 7.11 Substate transition diagram within S_{U13} (Recovery Stage on Primal Device)

7.2 State transition diagrams on BT mode

In this section, top level diagram on BT mode is illustrated.

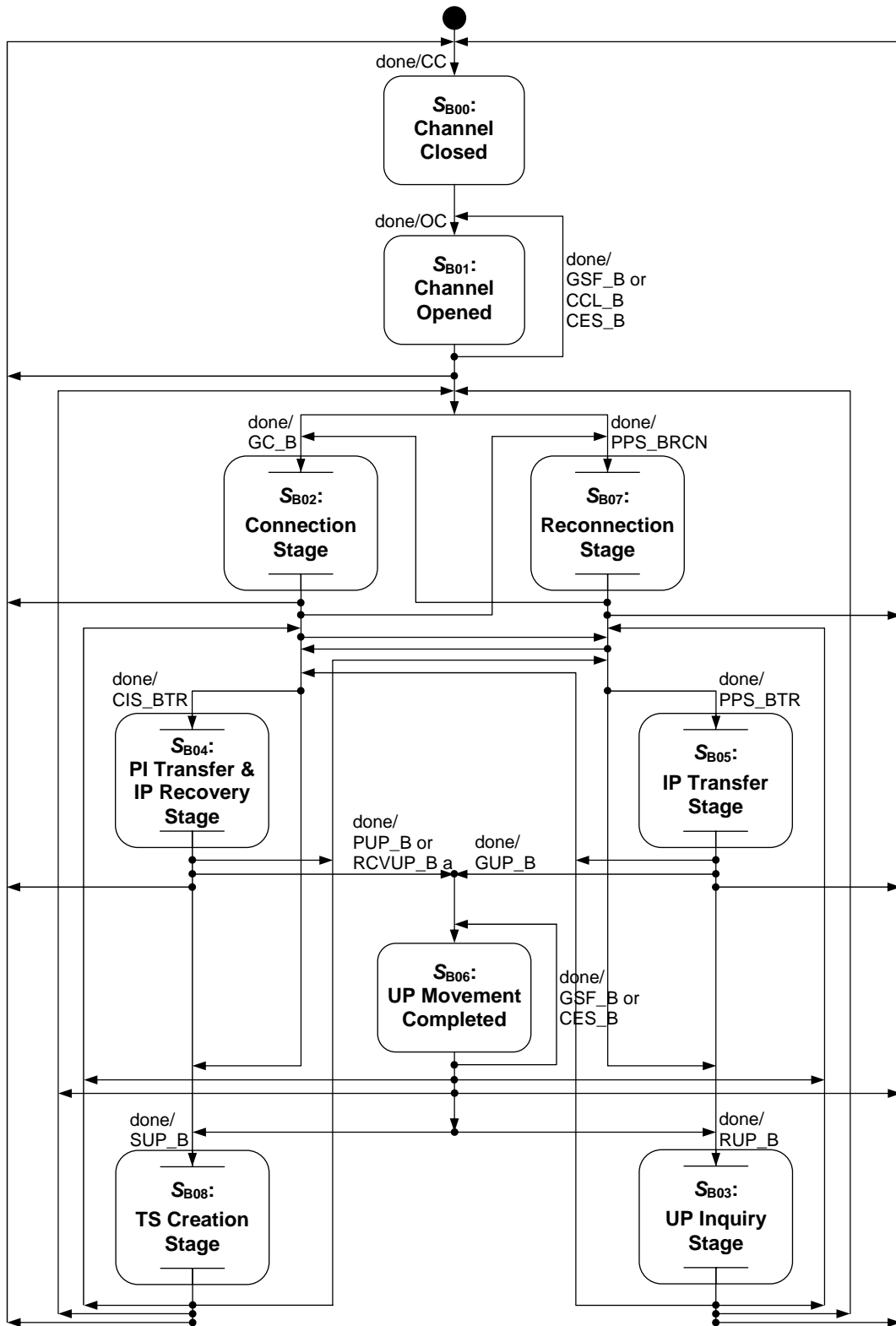


Figure 7.12 State transition diagram for Usage Pass transfer on BT mode

In Figure 7.12, transition from S_{B00} to S_{B01} is completed when 001b is set to least 3 bits in Sector Count register for OPEN CHANNEL.

7.2.1 State transition diagram within S_{B02}

In this section, substate transition diagram within S_{B02} (Connection Stage) is illustrated.

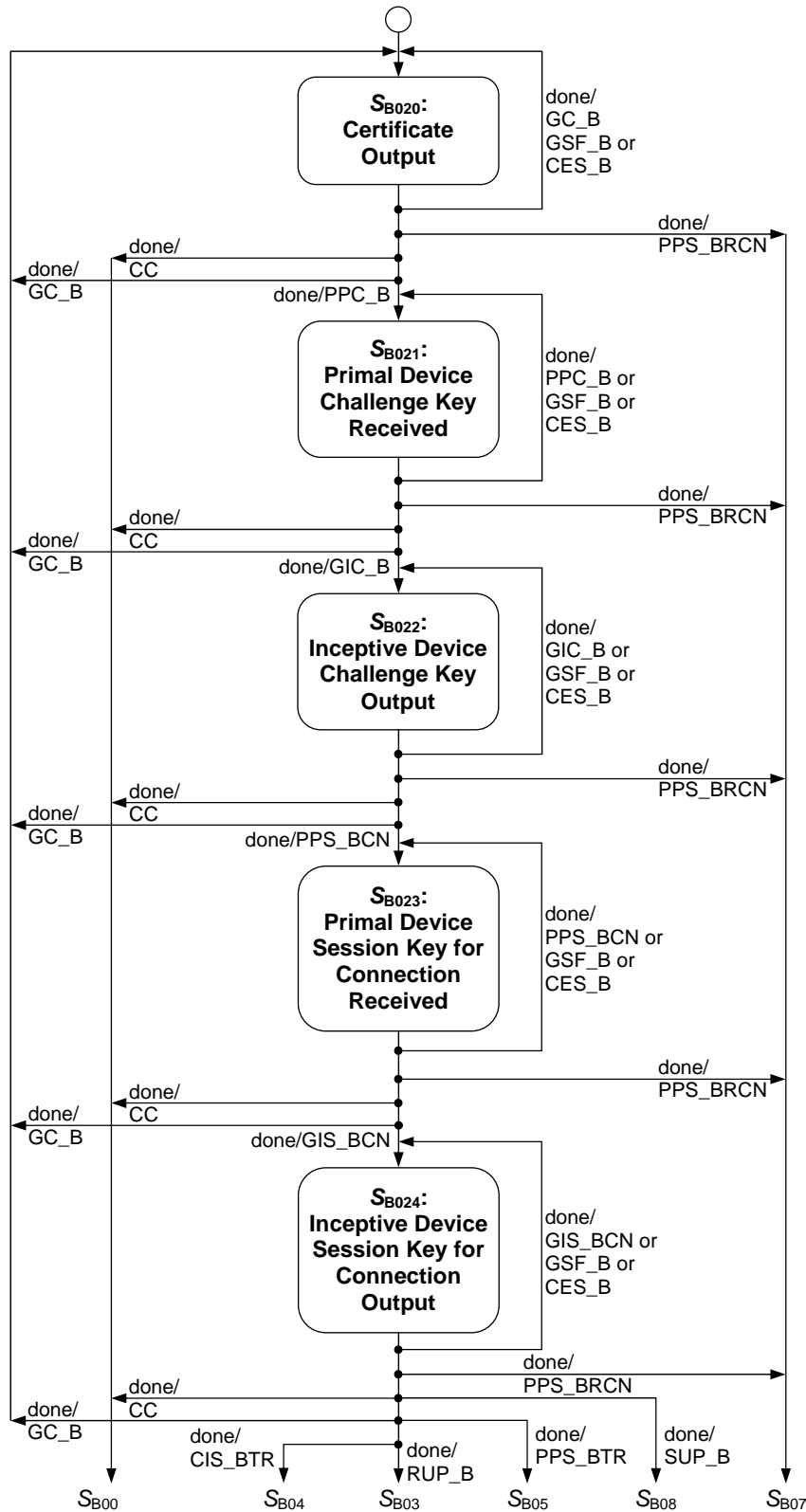


Figure 7.13 Substate transition diagram within S_{B02} (Connection Stage)

7.2.2 State transition diagram within S_{B07}

In this section, substate transition diagram within S_{B07} (Reconnection Stage) is illustrated.

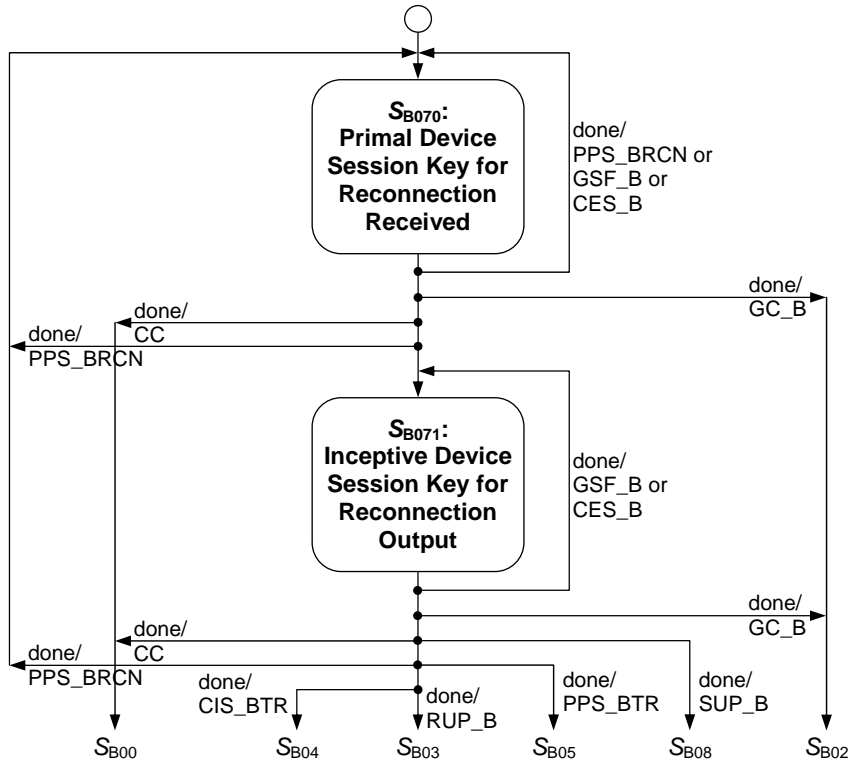


Figure 7.14 Substate transition diagram within S_{B07} (Reconnection Stage)

7.2.3 State transition diagram within S_{B03}

In this section, substate transition diagram within S_{B03} (UP Inquiry Stage) is illustrated.

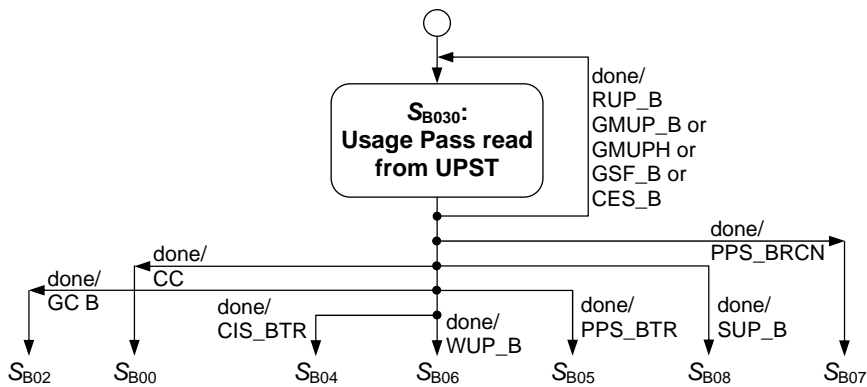


Figure 7.15 Substate transition diagram within S_{B03} (UP Inquiry Stage)

7.2.4 State transition diagram within S_{B04}

In this section, substate transition diagram within S_{B04} (PI Transfer and IP Recovery Stage) is illustrated.

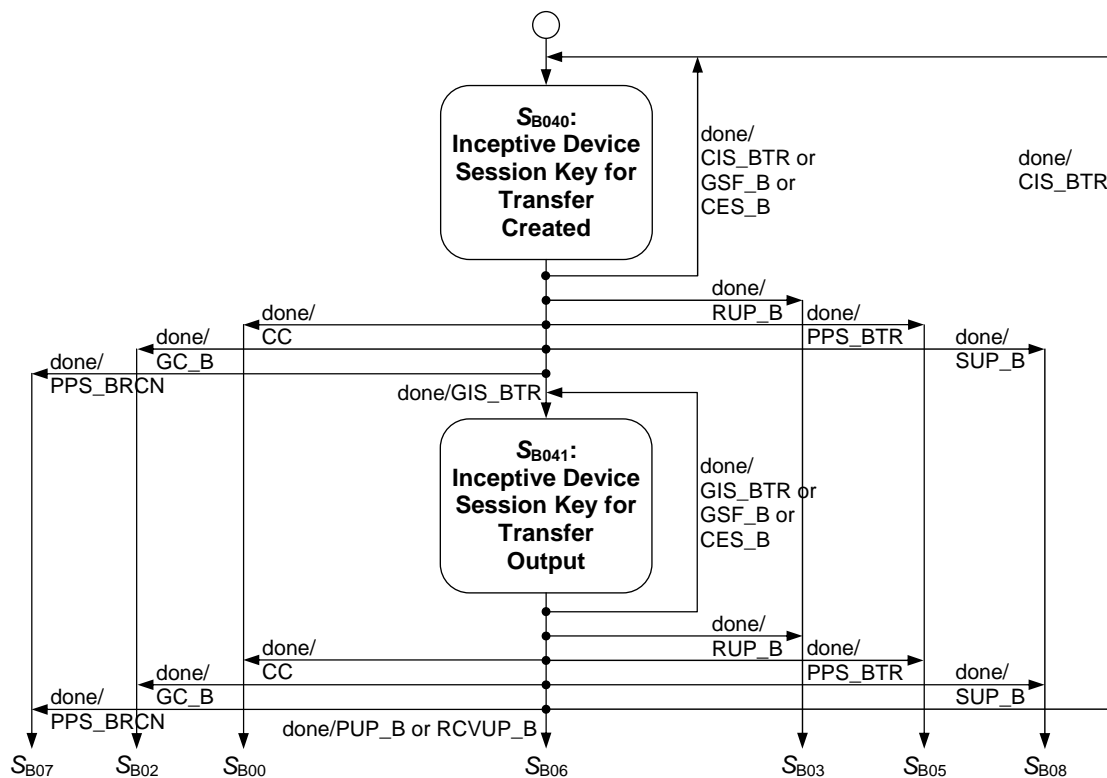


Figure 7.16 Substate transition diagram within S_{B04} (PI Transfer and IP Recovery Stage)

7.2.5 State transition diagram within S_{B05}

In this section, substate transition diagram within S_{B05} (IP Transfer Stage) is illustrated. In Figure 7.17, the letter “x” means “C” or “M” or “P”.

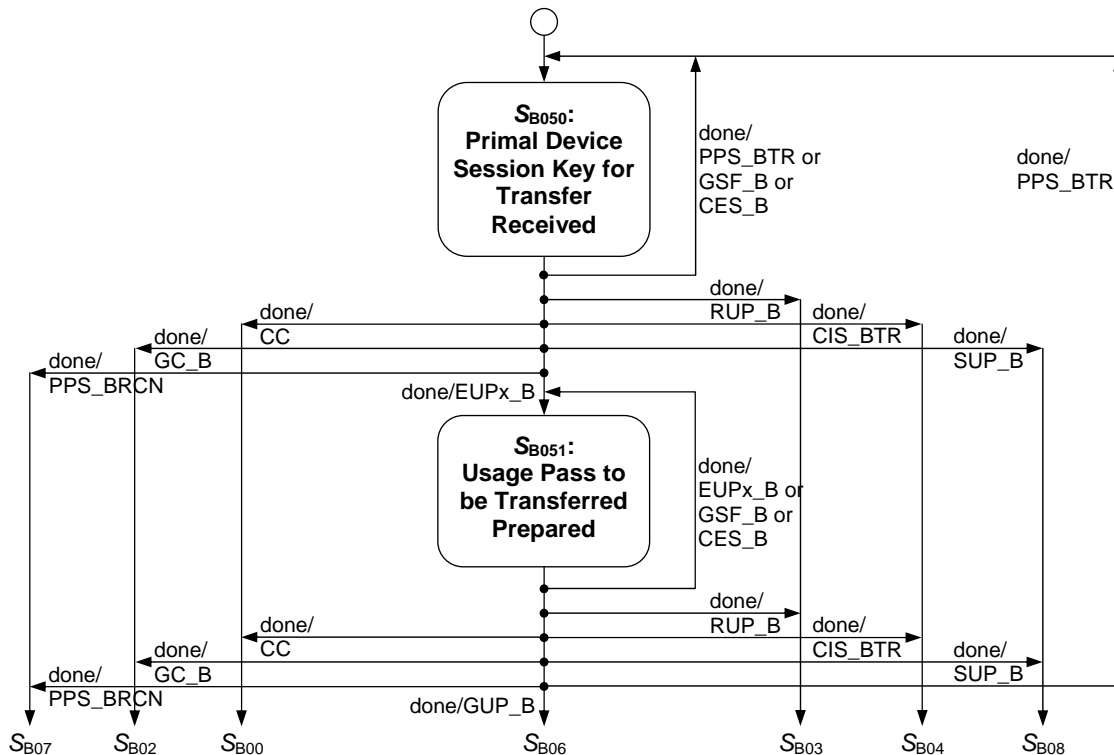


Figure 7.17 Substate transition diagram within S_{B05} (IP Transfer Stage)

7.2.6 State transition diagram within S_{B08}

In this section, substate transition diagram within S_{B08} (TS Creation Stage) is illustrated.

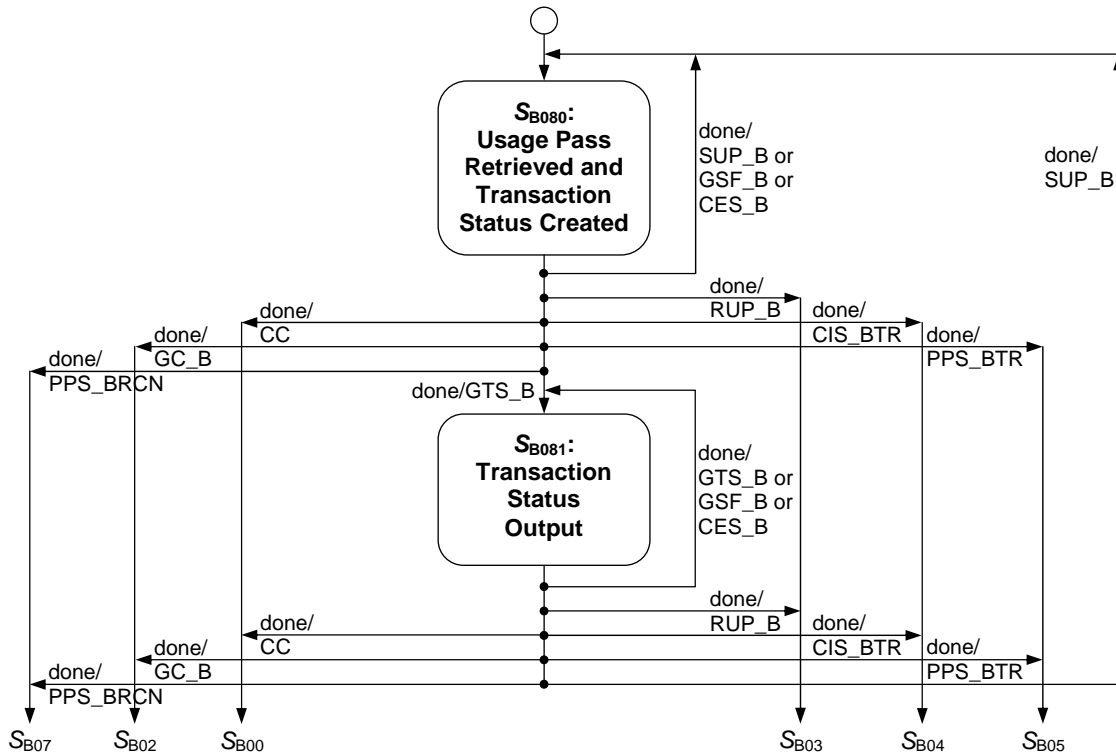


Figure 7.18 Substate transition diagram within S_{B08} (TS Creation Stage)

8 Sequence examples

In this chapter, sequence examples of subcommands issued by the Host Interface Unit on the Device Interface and transactions followed by the subcommands.

8.1 Sequence example for Storage Device recognition

This is a process to recognize for a Host Device whether a connected Device is Storage Device or not.

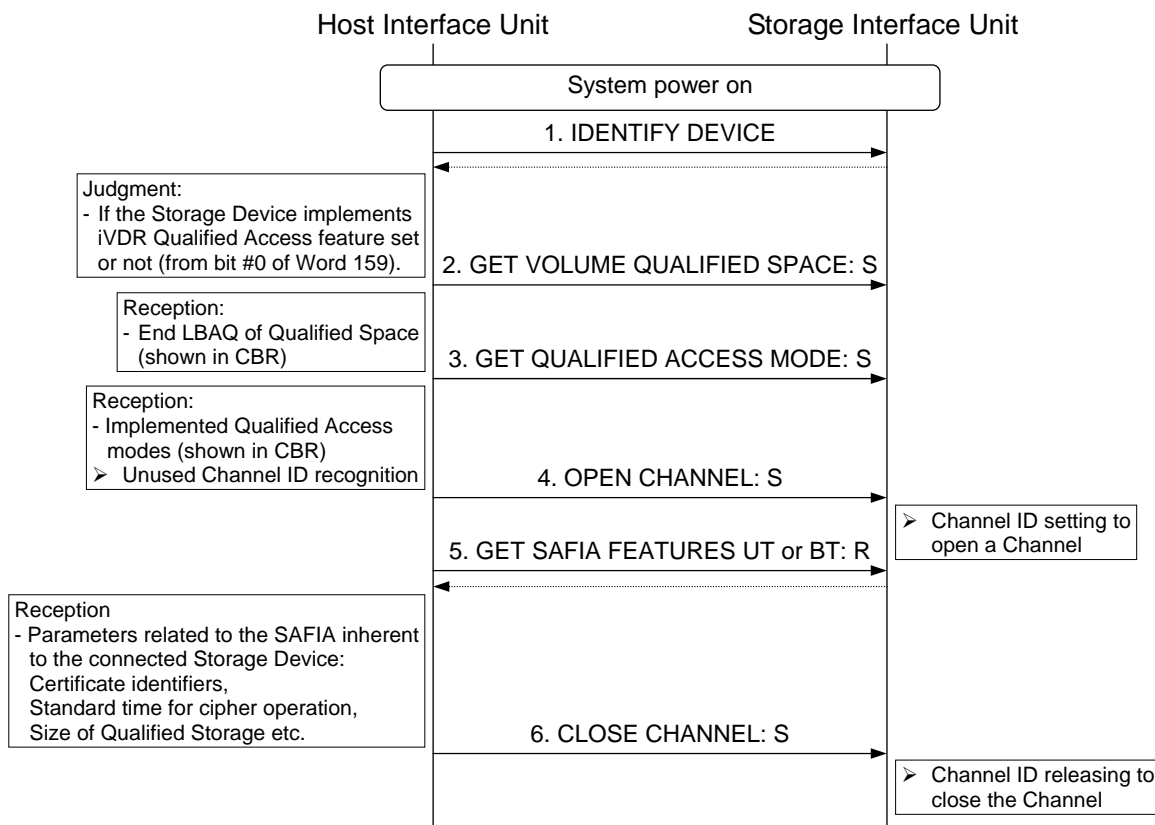


Figure 8.1 Recognition sequence of security architecture implemented on the Storage Device

In the beginning, the Host Interface Unit issues IDENTIFY DEVICE to the Storage Interface Unit to recognize whether the iVDR Qualified Access feature set is implemented in the Storage Device or not. When the feature set is implemented, then the Host Interface Unit issues to the Storage Interface Unit GET VOLUME QUALIFIED SPACE and GET QUALIFIED ACCESS MODE. When the Storage Interface Unit receives GET VOLUME QUALIFIED SPACE, the Unit returns the value of end LBAQ of Qualified Space of its own.

Following the subcommand, when the Storage Interface Unit receives GET QUALIFIED ACCESS MODE, it returns the information of Qualified Access mode that is implemented in the Storage Device and the maximum Channels that can be opened concurrently for each mode. On the basis of this information, the Host Interface Unit issues OPEN CHANNEL. By this subcommand, the Channel Identifier and the Qualified Access mode for each purpose is set to the Storage Interface Unit.

After the Channel is opened, the Host Interface Unit issues GET SAFIA FEATURES UT or BT, corresponding to the Qualified Access mode which was set to the opened Channel, to the Storage Interface Unit. In the response, the Storage Interface Unit returns the information particular to each Storage Device, necessary for Usage Pass transfer (identifier of the embedded certificate, reference time for the execution of subcommands etc.). Using this information, the Host Device executes the Usage Pass transfer adequately.

After completion of Usage Pass transfer, when to release the Channel, the Host Interface Unit issues CLOSE CHANNEL to the Storage Interface Unit.

8.2 Sequence examples for the transaction on UT mode and BT mode

In the remaining portion of this chapter, the flow of the subcommands which the Host Interface Unit sets into the Command Block register in the Storage Interface Unit, the responses which the Storage Interface Unit returns, and the processes that are executed in the Host Device or Storage Device after receiving a subcommand or a response are described. Note that the sequences shown here are just the examples.

The characteristic of this architecture lies in that when the subcommand requires encryption or decryption process in the Usage Pass Transfer Unit in the Storage Device, in order to use Device Interface bus for other data transfer during the process, after the Storage Interface Unit receives the subcommand, the bus can be released temporarily. After lapse of appropriate time, the Host Interface Unit may issue the next subcommand. The reference time required for the execution of each subcommand is sent to the Host Interface Unit in GET SAFIA FEATURES UT or BT information.

8.2.1 Abbreviations used in the figures in this section

8.2.1.1 Key names and others

The names of the keys and others in the figures illustrated in this section are abbreviated as shown in Table 8.1.

Table 8.1 Abbreviations of the keys and so forth used in chapter 8

Abbreviations	Description
ID	Usage Pass Identifier
xD.Puc.Key	Device Class Public Key installed in x Device; x is Primal or Inceptive
xD.Prc.Key	Device Class Private Key installed in x Device; x is Primal or Inceptive
xD.Pu.Key	Device Public Key installed in x Device; x is Primal or Inceptive
xD.Pr.Key	Device Private Key installed in x Device; x is Primal or Inceptive
xD.*Pu.Key	ECDH Shared Key, with proviso that this key is calculated with Device Public Key sent from the partner Device; x is Primal or Inceptive; PD.*Pu.Key is used only in BT mode
xD.*Pr.Key	ECDH Shared Key, with proviso that this key is calculated with Device Private Key installed in the Storage Device; x is Primal or Inceptive; PD.*Pr.Key is used only in BT mode
x.C.Key	Challenge Key created in one of the Import Module, Export Module, Transmit Module, or Storage Module in x Device; x is Primal or Inceptive; I.C.Key is used only for BT mode
x.S.Key	Session Key created in one of the Import Module, Export Module, Transmit Module, or Storage Module in x Device; x is Primal or Inceptive

8.2.1.2 Wait time for completing the cryptographic operations in the Storage Device

When Usage Pass transfer is executed, even after the Host Interface Unit releases the right to use Device Interface bus, cryptographic operations and so forth may be performed continuously in the Storage Module. The abbreviations of wait time required for completing these processes are shown in Table 8.2.

Table 8.2 Abbreviations of wait time

Abbreviations	Description
CV	Device Class Certificate Verification
KHC	Keyed hash Calculation
UPF ¹	A Usage Pass Fetch from Qualified Storage to Buf.QSTC
UPW ²	A Usage Pass Write from Buf.QSTC to Qualified Storage
PKE	Encryption with a public key
PKD	Decryption with a private key
SKD	Decryption with a symmetric key
SKE	Encryption with a symmetric key
SC	Status Confirmation

8.2.2 Channel management

8.2.2.1 Channel opening

This is a process that must be executed as the first step before transferring Usage Passes. Usage Pass transfer transaction is realized on a Channel opened between the Host Interface Unit and the Storage Interface Unit in advance. When a Host Interface Unit issues this subcommand, the Unit sets a Channel Identifier and Qualified Access mode on which Usage Pass transfer is executed into the Command Block register.



Figure 8.2 Channel Identifier and Qualified Access mode setting to the Storage Device

8.2.2.2 Channel closing

This is a process for the Storage Device to release Channel Identifier and to close the opened channel. When a Host Interface Unit issues this subcommand, the Unit sets the Channel Identifier into the Command Block register to be released.

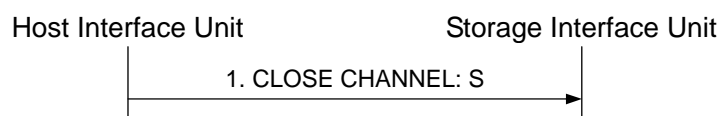


Figure 8.3 Channel Identifier release

8.2.3 Masked Usage Pass transfer

This is a process for the Host Device to obtain the Masked Usage Pass recorded in the Qualified Storage. When the Storage Interface Unit receives GET MASKED USAGE PASS, the Unit sets entire Usage Pass of which CIC is zero into the Data register. Successive transfer of plural Masked Usage Passes is possible if plural Usage Passes are fetched from the Qualified Storage to Buf.QSTC, with the proviso that the Usage Passes are recorded in the continuous region in

¹ Decryption time is included if Usage Passes were encrypted.

² Encryption time is included if Usage Passes will be encrypted.

terms of LBAQ.

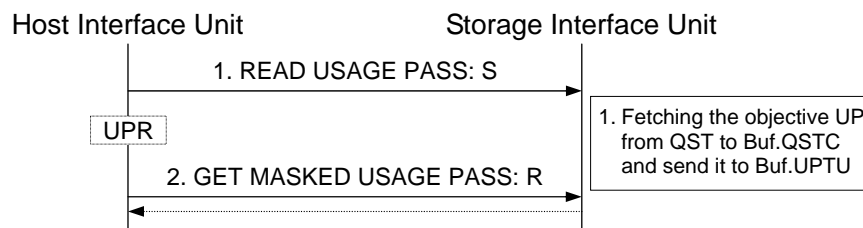


Figure 8.4 Transfer of Masked Usage Pass

When the Storage Interface Unit receives GET MASKED USAGE PASS WITH KEYED HASH, the Usage Pass Transfer Unit in the Storage Device calculates the keyed hash value with Usage Pass of which CIC is zeros, two latest Session Keys generated in the Source or Destination Module in both Primal Device and Inceptive Device, specified LBAQ, Transferred Sector Count respectively. GET MASKED USAGE PASS WITH KEYED HASH is executable in only in BT mode.

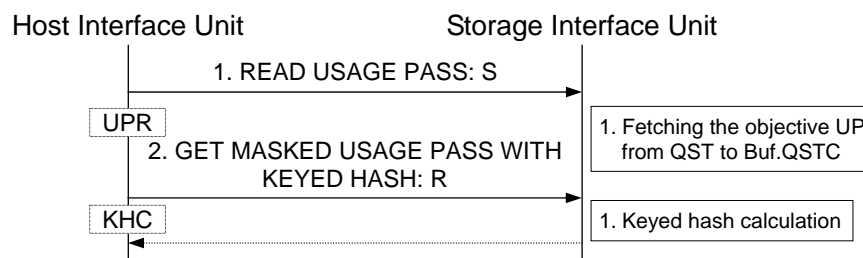


Figure 8.5 Transfer of Masked Usage Pass with keyed hash

8.2.4 Subcommand belonging to SAFIA feature set execution status transfer

This is a process for the Host Device to obtain the state of subcommand execution.

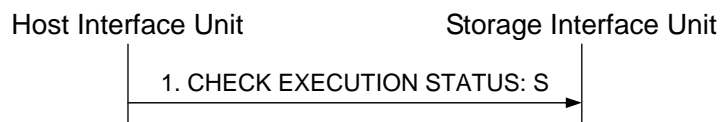


Figure 8.6 Transfer of executed status of SAFIA feature set subcommands

8.2.5 A Usage Pass relocation in the drive

WRITE USAGE PASS has been obsoleted in this document.

8.2.6 The sequence examples for Usage Pass transfer in UT mode

In this section, subcommand execution sequences in UT mode are described.

8.2.6.1 Transfer of External Log portion of Transaction Log

This is a process to transfer Transaction Log recorded in the Usage Pass Transfer Unit to the Host Interface Unit. In Usage Pass transfer in UT mode, when the process has not completed normally, the Host Interface Unit can issue this subcommand to the Storage Interface Unit. In response to this, the Storage Interface Unit sets the information recorded in Transaction Log into the Data register, with the proviso that the information is the one of which attribute is external. After interpreting the returned data, the Usage Pass Transfer Unit in the Primal Device can grasp the

UPID of the Usage Pass that was tried to be transferred, but has not completed normally. A process like this generally referred to as UPID recognition process hereinafter.

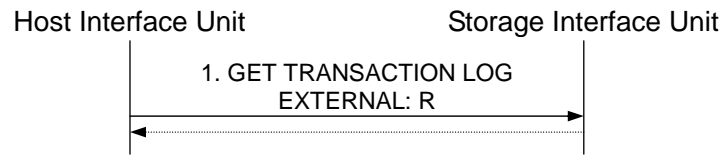


Figure 8.7 Transfer of External Log portion of Transaction Log

8.2.6.2 Connection Stage

A sequence example of Connection Stage on Device Interface is shown in Figure 8.8.

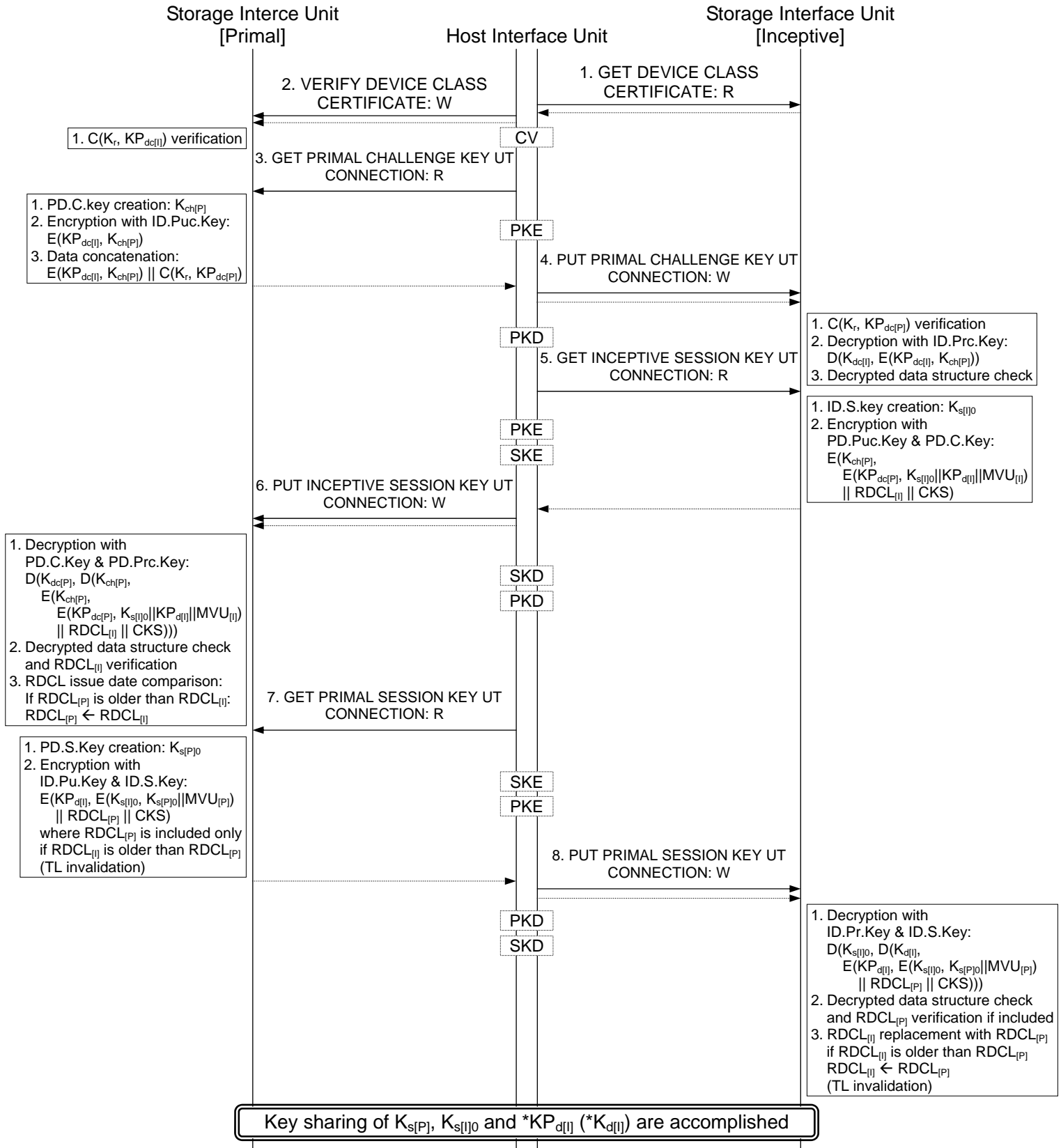


Figure 8.8 Subcommand execution sequence on Connection Stage (UT mode)

8.2.6.3 Reconnection Stage

A sequence example of Reconnection on Device Interface is shown in Figure 8.9.

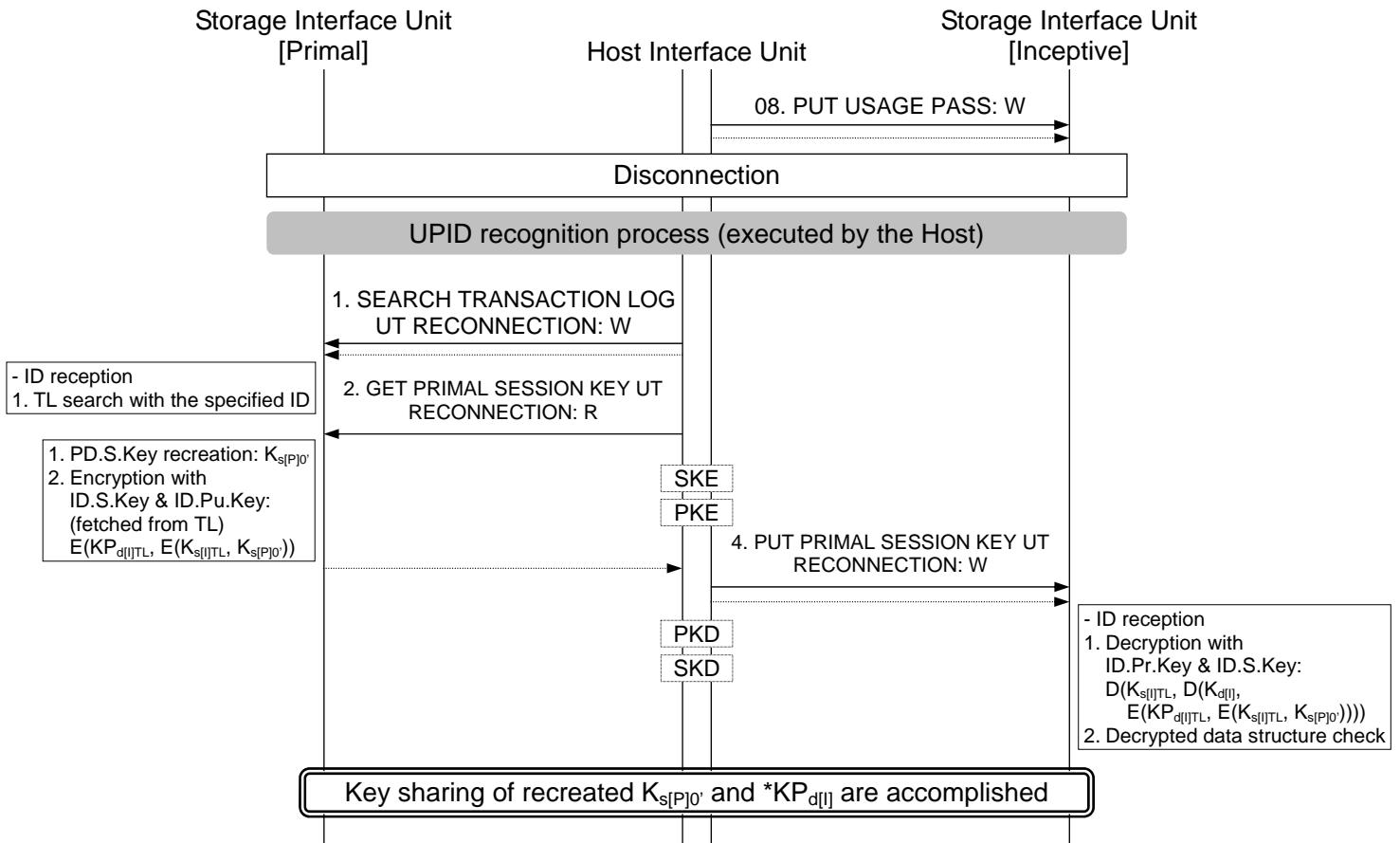
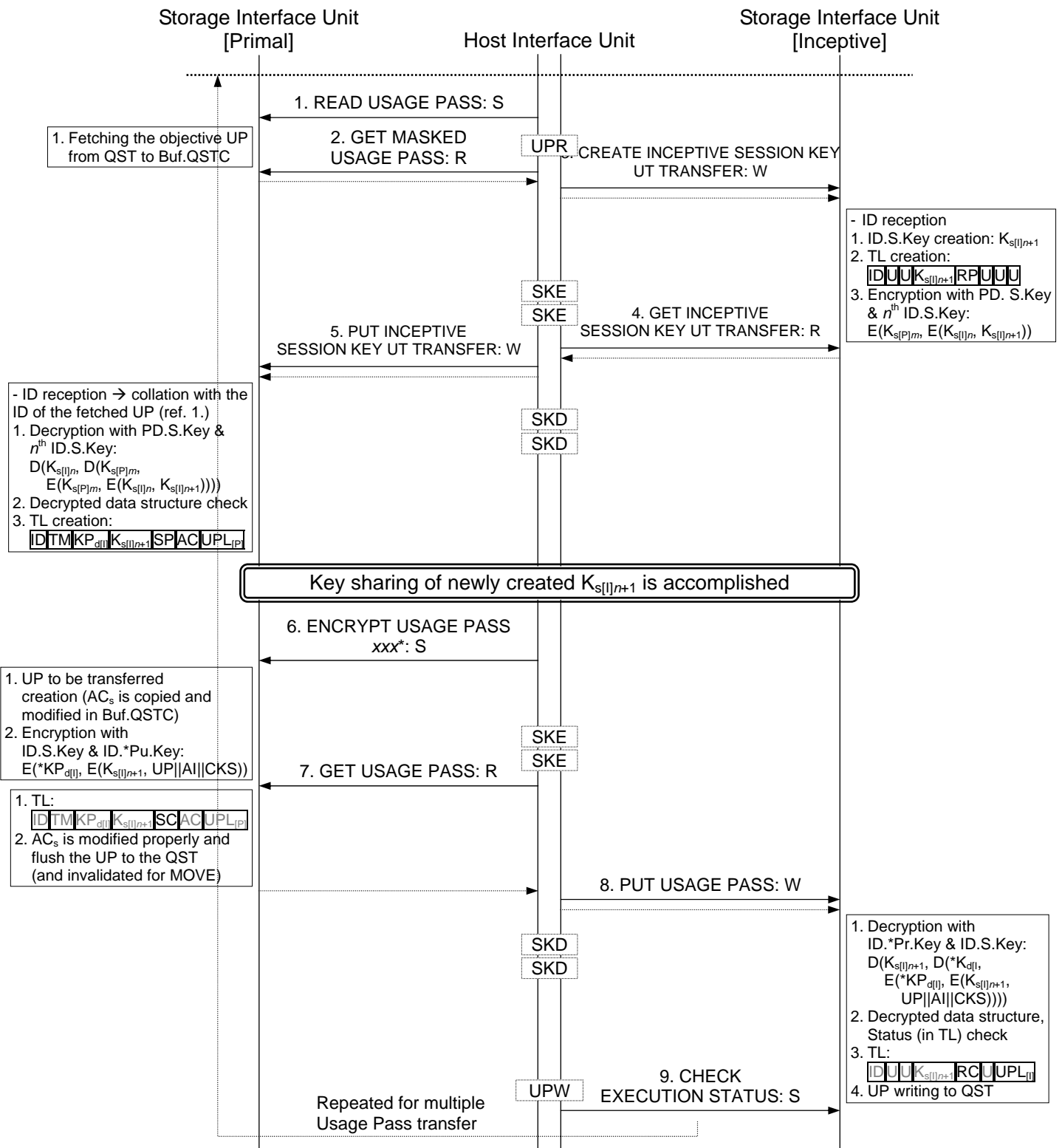


Figure 8.9 Subcommand execution sequence on Reconnection Stage (UT mode)

8.2.6.4 Transfer Stage

A sequence example of Transfer Stage on Device Interface is shown in Figure 8.10.



In the above Figure, xxx* is whether COPY, MOVE or PLAY

Figure 8.10 Subcommand execution sequence on Transfer Stage (UT mode)

Though CHECK EXECUTION STATUS is placed as No.9, this subcommand is not necessary to be executed here.

8.2.6.5 Recovery Stage

A sequence example of Recovery Stage on Device Interface is shown in Figure 8.11.

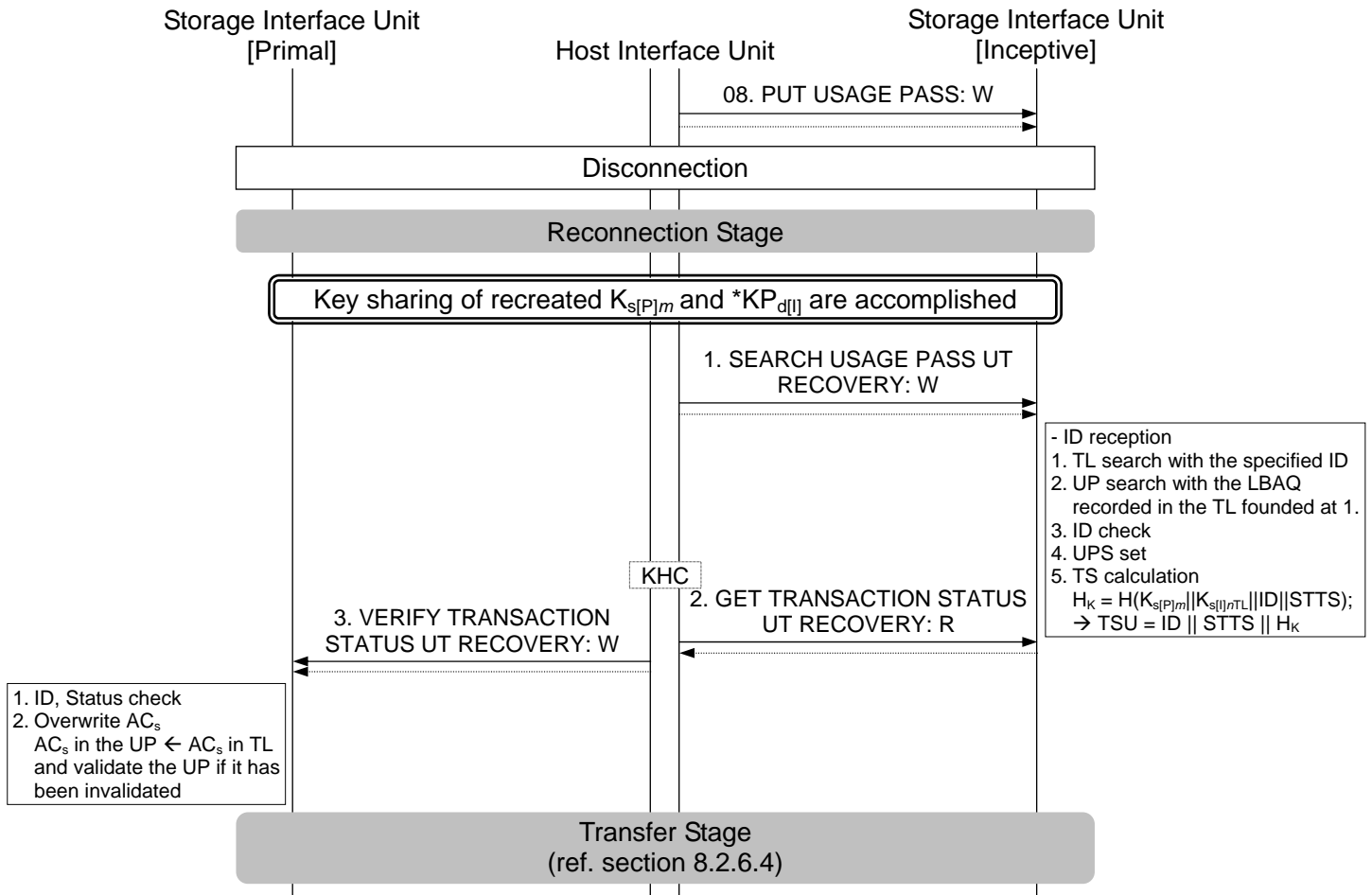


Figure 8.11 Subcommand execution sequence on Recovery Stage (UT mode)

8.2.7 The sequence examples for Usage Pass transfer under BT mode

In this section, subcommand execution sequences for BT mode are described. In this case, Storage Device is always Inceptive.

8.2.7.1 Connection Stage

A sequence example of Connection Stage on Device Interface is shown in Figure 8.12.

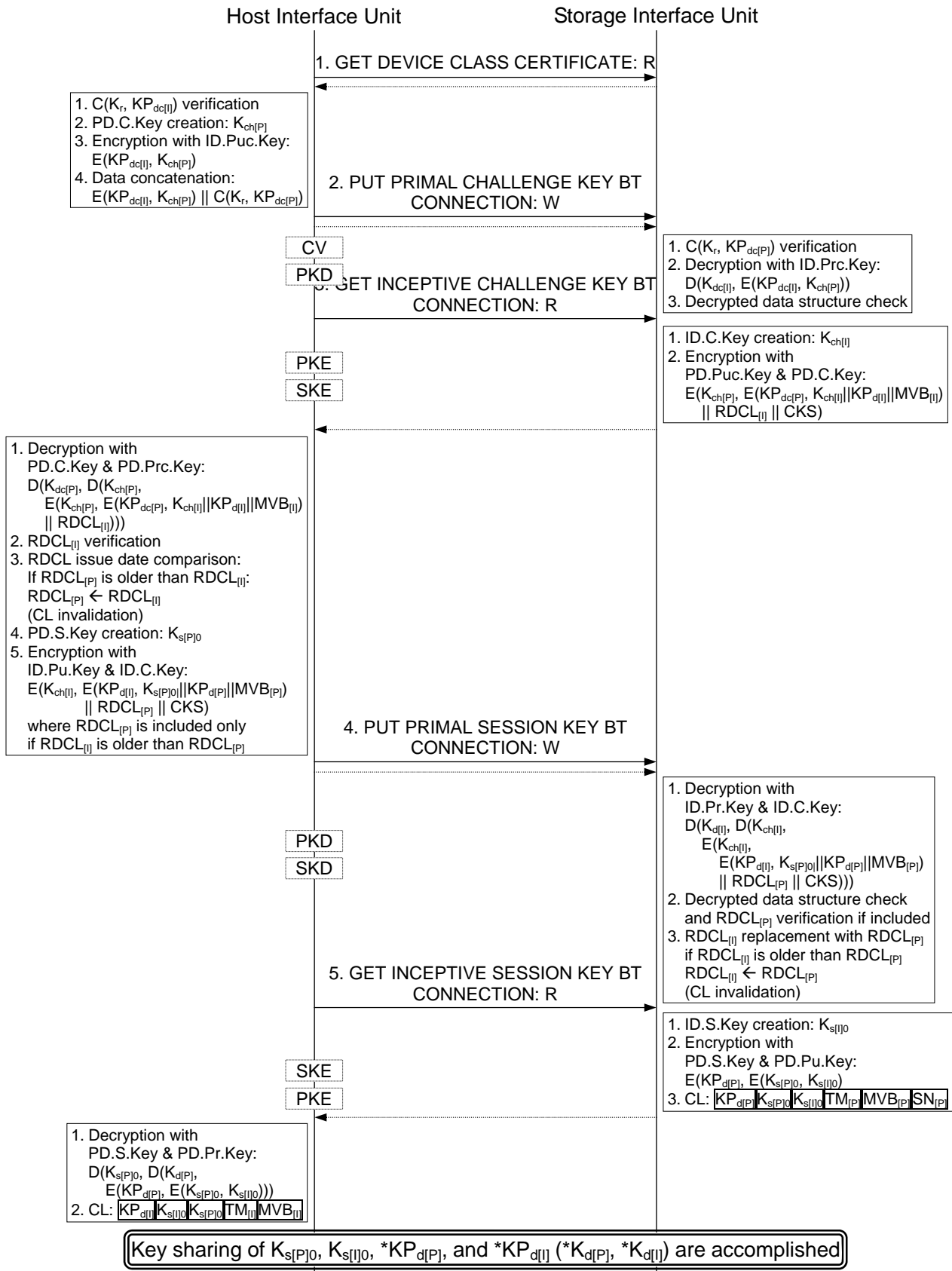


Figure 8.12 Subcommand execution sequence on Connection Stage (BT mode)

8.2.7.2 Reconnection Stage

A sequence example of Reconnection Stage on Device Interface is shown in Figure 8.13.

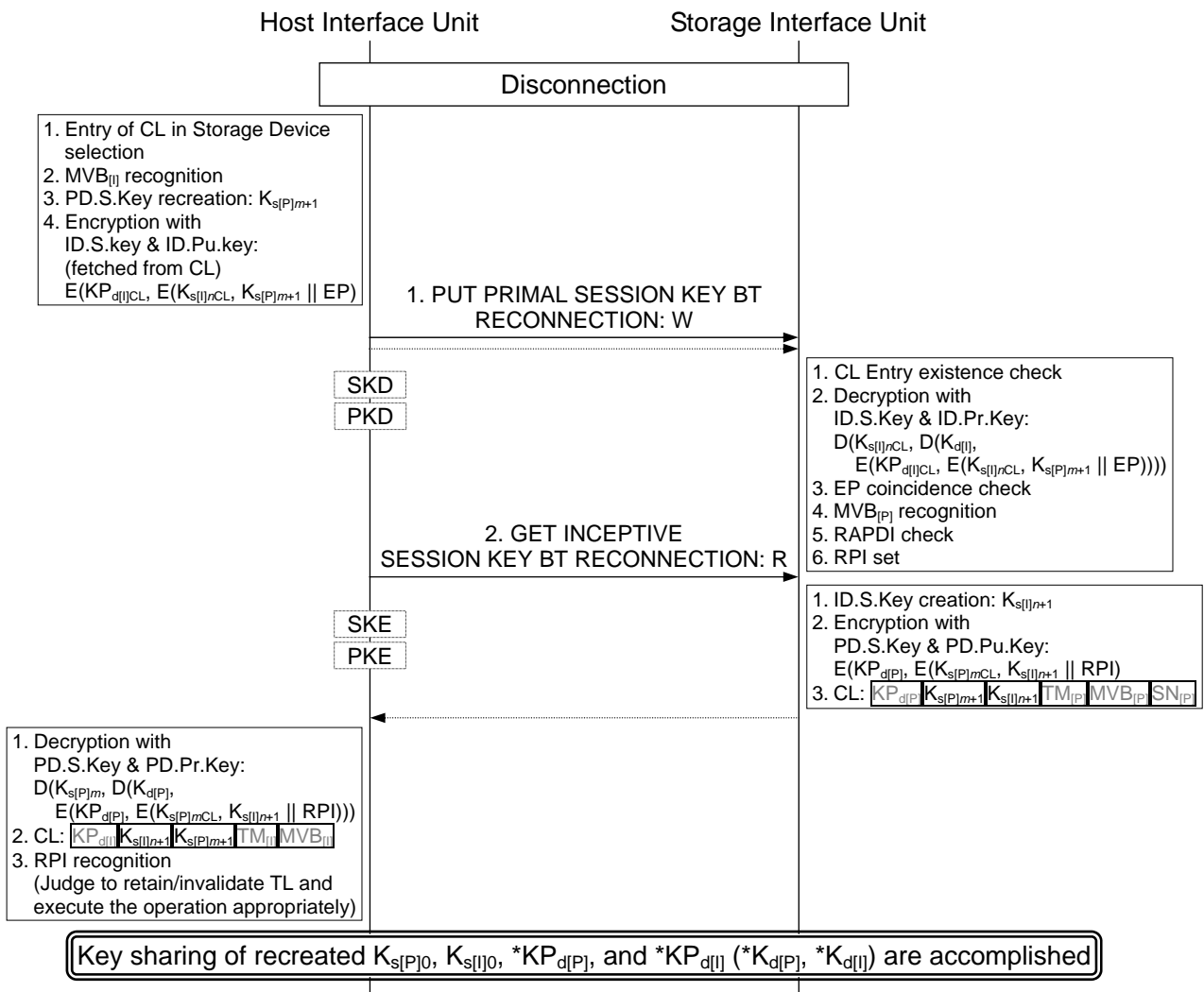


Figure 8.13 Subcommand execution sequence on Reconnection Stage (BT mode)

8.2.7.3 Transfer Stage

A sequence example of Transfer Stage on Device Interface is shown in Figure 8.14 and Figure 8.15.

8.2.7.3.1 PI Transfer Stage

On PI Transfer Stage, the Import Module in the Host Device is Source Module and the Storage Module in the Storage Device is Destination Module.

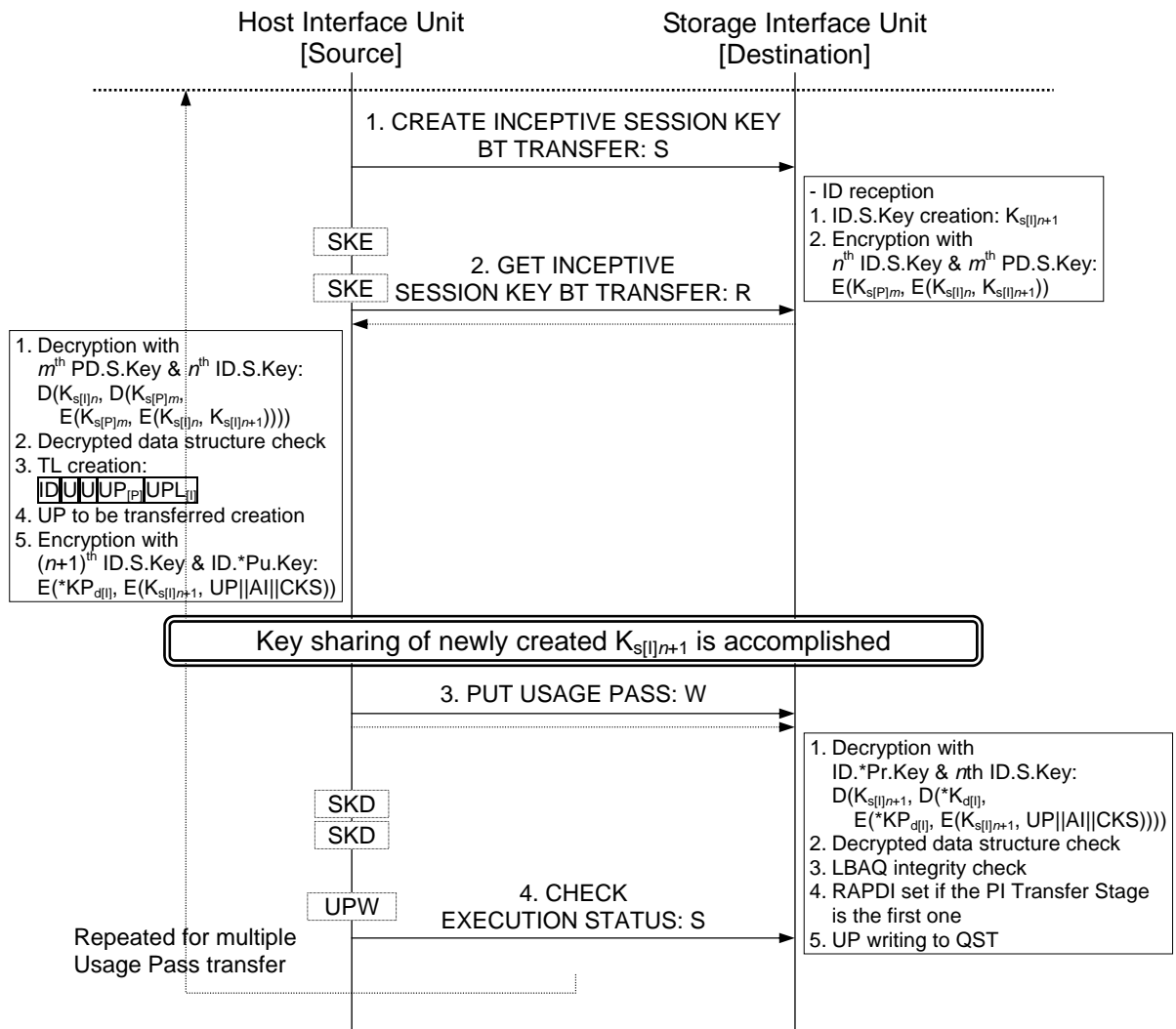
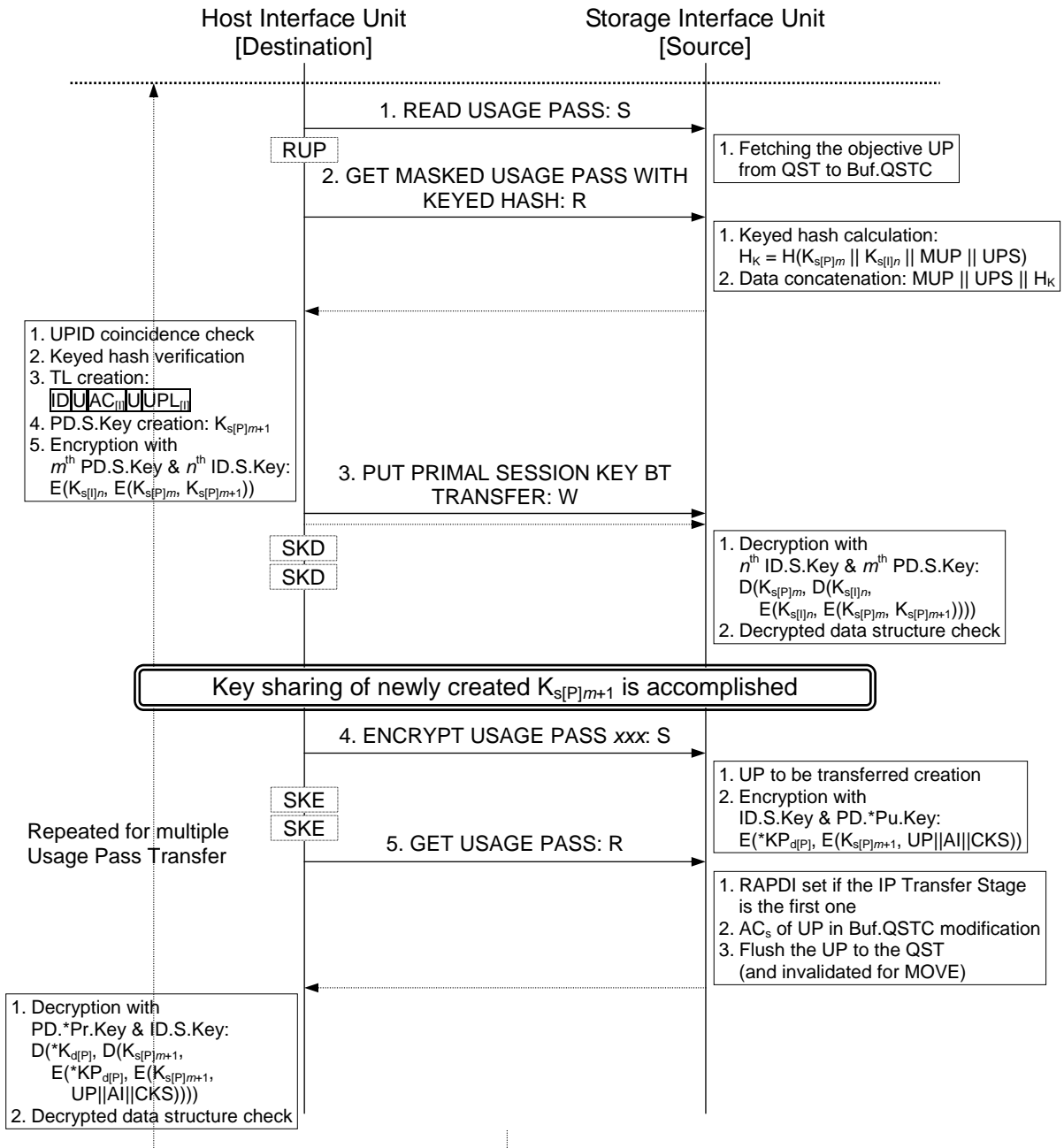


Figure 8.14 Subcommand execution sequence on Transfer Stage (BT mode)

CHECK EXECUTION STATUS is placed as No.4, however, this subcommand is not necessary to be executed here.

8.2.7.3.2 IP Transfer Stage

On IP Transfer Stage, the Export Module in the Host Device is Destination Module and the Storage Module in the Storage Device is Source Module.



In the above Figure, xxx* is whether COPY, MOVE or PLAY

Figure 8.15 Subcommand execution sequence on Transfer Stage (BT mode)

8.2.7.4 Recovery Stage

A sequence example of Recovery Stage on Device Interface is shown in Figure 8.16 and Figure 8.17.

8.2.7.4.1 PI Recovery Stage

On PI Recovery Stage, the Import Module in the Host Device is Source Module and the Storage Module in the Storage Device is Destination Module for Usage Pass Transfer in the past. PI Recovery Stage is a recovery procedure of lost Usage Pass for PI Transfer Stage.

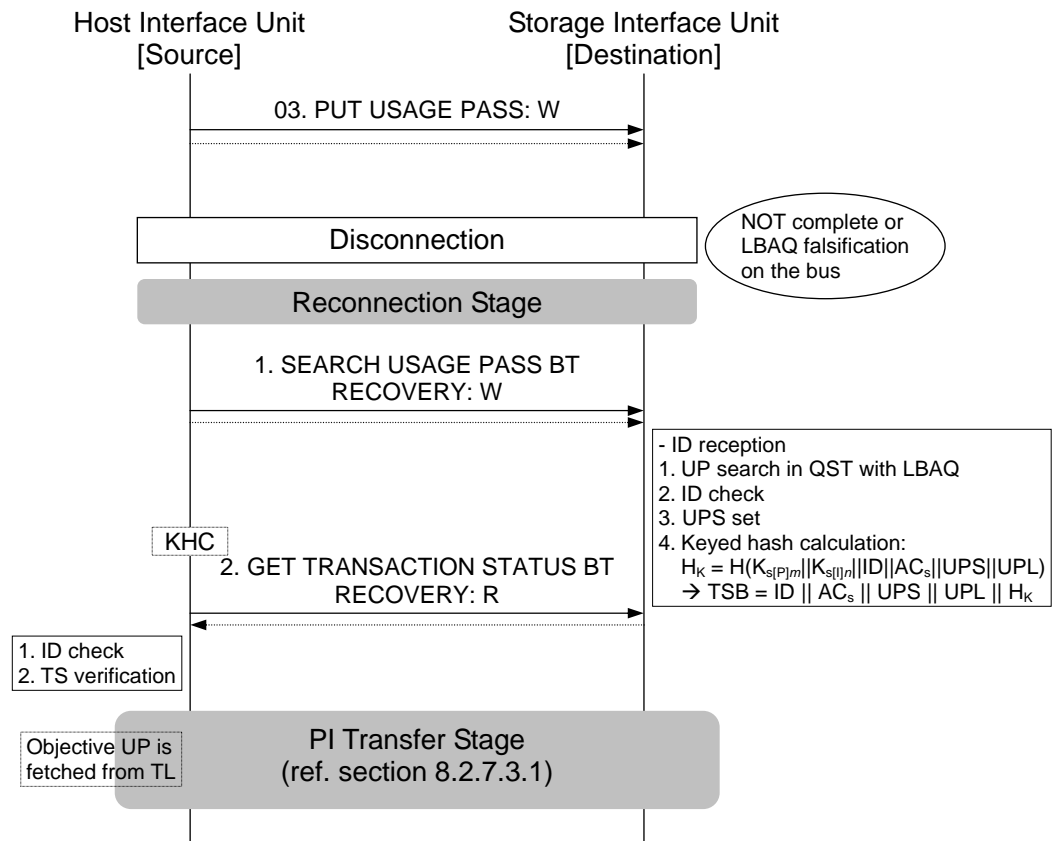
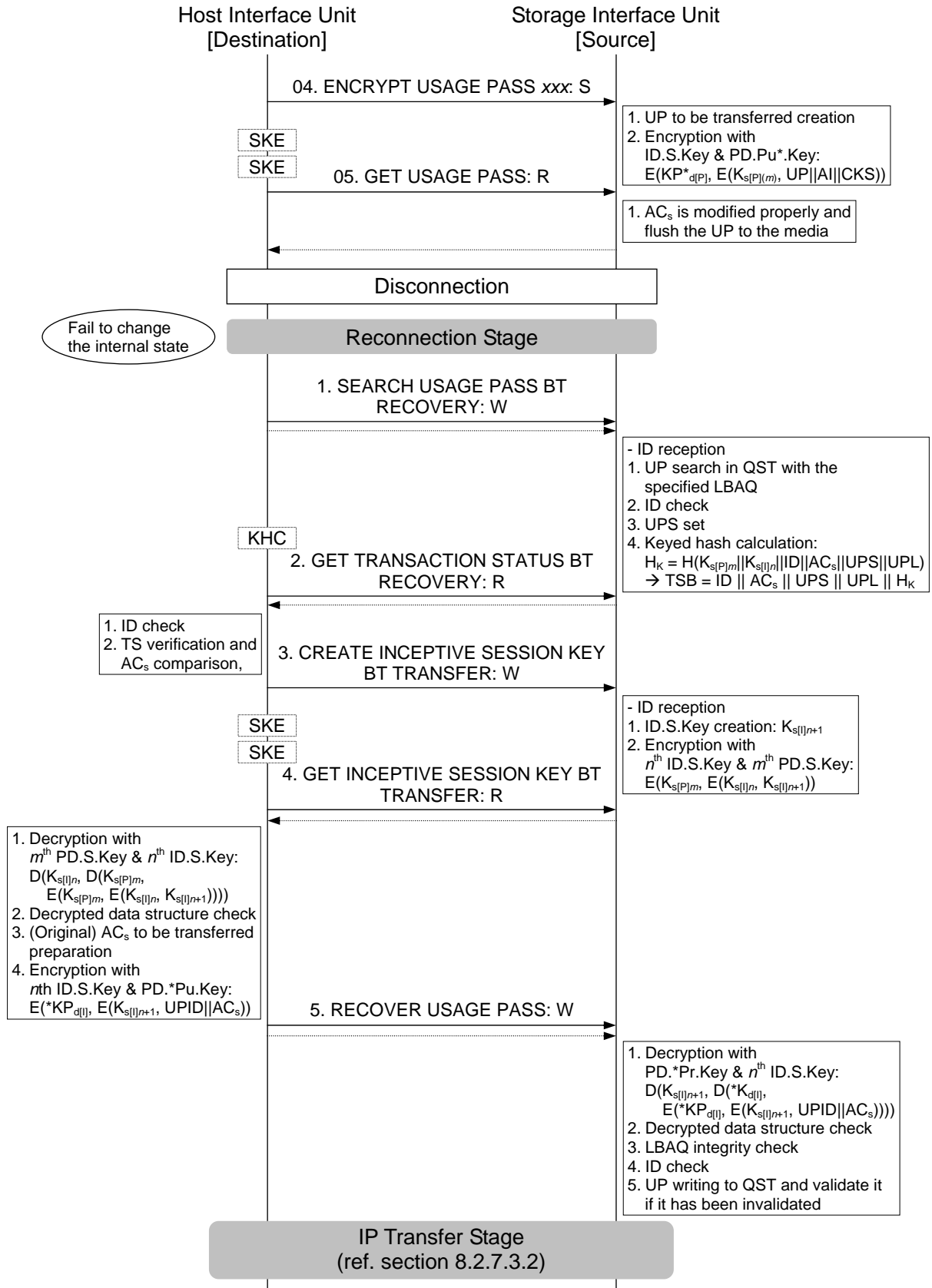


Figure 8.16 Subcommand execution sequence on PI Recovery Stage (BT mode)

8.2.7.4.2 IP Recovery Stage

On IP Recovery Stage, the Export Module in the Host Device is Destination Module and the Storage Module in the Storage Device is Source Module for Usage Pass Transfer in the past. IP Recovery Stage is a recovery procedure of lost Usage Pass for IP Transfer Stage.



In the above Figure, xxx* is whether COPY, MOVE or PLAY

Figure 8.17 Subcommand execution sequence on IP Recovery Stage (BT mode)

Annex A Composition of an HIFU

Composition of an HIFU is either one of the following.

- (1) All the components constituting HIFU are in the Host Device.
- (2) Some of the components constituting HIFU are out of the Host Device but in the SAFIA Terminal, and the rest of the components are in the Host Device. Then, the two set of components, which are in the Host Device and out of the Host Device, are directly connected with just one physical cable, and conformity of the later set of components to the prescription is confirmed.