Security Architecture for Intelligent Attachment Device Specifications

– Storage Device with AT Attachment Interface –

Version 1.20

February 2008

- *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 © 2008 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.

© SAFIA License Group, 2008. All rights reserved.

Table of Contents

1 General 1
1.1 Scope 1
1.2 References 1
1.3 Definitions 1
1.3.1 Definitions in ATAPI 1
1.3.2 Definitions in iVDR/IF 1
1.3.3 Definitions in SAFIA/PDS1 2
1.3.4 Definitions in SAFIA/IF 3
1.3.5 Additional definitions 3
1.4 Abbreviations 3
1.4.1 Abbreviations described in SAFIA/PDS1 3
1.4.2 Abbreviations described in SAFIA/IF 3
1.5 Conventions 3
1.5.1 Keywords 3
1.5.2 Numerical values 4
2 Device Class Certificate 4
2.1 Device Type Name 4
2.2 Acceptable Usage Pass Type Map 4
3 Requirements for Usage Pass recording into Qualified Storage 4
4 Rule for modification of Access Condition for Storage Module 4
5 Requirements for protocol implementation 4
6 Rules for log management 5
6.1 Transaction Log 5
6.1.1 UT mode 5
6.1.2 BT mode 6
6.2 Connection Log 7
6.3 Clearance Policy of Transaction Log and Connection Log 7
6.4 Recovery-Allowed Primal Device Indicator 7
6.5 Recovery Permission Indicator 8
Annex A Requirements for implementation of Storage Module 9
A.1 Robustness of Storage Module 9
A.2 Capacity of Qualified Storage 9

© SAFIA License Group, 2008. All rights reserved.

1 General

1.1 Scope

This document describes various obligations as to implement the Storage Device of which interface complies with AT-Attachment Interface. However, interface architecture of the Device equipped with AT Attachment interface shall basically comply with the description described in "Security Architecture for Intelligent Attachment Device: Interface for iVDR", therefore the topic about it is not described in this document.

1.2 References

1) ANSI INCITS 361-2002
Information Technology - AT Attachment with Packet Interface - 6 (ATA/ATAPI-6) [ATAPI]

2) iVDR Hard Disk Drive Consortium,
Interface Specification Version 2.0, April 2006 [iVDR/IF]

3) National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 197,
Advanced Encryption Standard (AES), November 2001 [FIPS197]

4) Security Architecture for Intelligent Attachment Device Specifications;
Interface for iVDR [SAFIA/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]

1.3 Definitions

1.3.1 Definitions in ATAPI

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

- ATA
- AT Attachment

1.3.2 Definitions in iVDR/IF

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

- Channel
- LBAQ
- Qualified Access mode
- Qualified Access Mode Identifier

© SAFIA License Group, 2008. All rights reserved.

- Qualified Space

1.3.3 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
- Connection Log
- Destination
- Device
- Device Class
- Device Class Certificate
- Device Class Private Key
- Device Class Public Key
- Device Private Key
- Device Public Key
- Inceptive
- Primal
- Qualified Storage
- Revoked Device Class List
- SAFIA compliant
- Storage Module (This term was defined as Security Management Module in version 1.0.)
- Session
- Session Key
- Session Status
- Source
- Transaction
- Transaction Log
- Transaction Status
- Unidirectional Transfer
- Usage Pass

© SAFIA License Group, 2008. All rights reserved.

- Usage Pass Identifier
- Usage Pass Transfer

1.3.4 Definitions in SAFIA/IF

The following terms used in this document are defined in section 1.3.4 of SAFIA/IF:

- Device Interface
- Host Interface Unit
- Storage Interface Unit

1.3.5 Additional definitions

The following term used in this document is defined in this section.

- Storage Device
  Storage Device which is SAFIA compliant and of which interface complies with iVDR/IF and SAFIA/IF. It is a Drive defined in version 1.0.

1.4 Abbreviations

1.4.1 Abbreviations described in SAFIA/PDS1

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

- AC
- AC_s
- BT
- SAFIA
- UT

1.4.2 Abbreviations described in SAFIA/IF

The following abbreviations are described in section 1.4.3 of SAFIA/IF:

- $MVB_{[X]}$
- $SN_{[P]}$

1.5 Conventions

1.5.1 Keywords

May and shall follow the description provided in section 1.5.1 of SAFIA/PDS1.

© SAFIA License Group, 2008. All rights reserved.

1.5.2 Numerical values

Decimal numbers are represented as decimal digits 0 to 9. Binary numbers are represented as binary digits 0 and 1 followed by the symbol “b”.

2 Device Class Certificate

A Device Class Certificate installed in the Storage Module and a Revoked Device Class List recorded in the Storage Module is described in this chapter. Other than the fields described in this chapter, the fields of them shall be described as being described in chapter 8 of SAFIA/PDS1.

2.1 Device Type Name

This value is “DRV”.

2.2 Acceptable Usage Pass Type Map

Bits from AT0 to AT47 shall be set to 1b and bits from AT48 to AT63 shall be set to 0b.

Recording a Usage Pass into Qualified Storage is allowed, even if a Storage Module receives a Usage Pass of which Usage Pass Type is not supported by the Storage Device in terms of Acceptable Usage Pass Type Map.

3 Requirements for Usage Pass recording into Qualified Storage

When recording a Usage Pass into Qualified Storage, comparison of Usage Pass Type which the Storage Device received and Acceptable Usage Pass Type Map in the Device Class Certificate installed in the Storage Device shall not be executed in the Usage Pass Transfer Unit, but verification of AC_s shall be executed in the Qualified Storage Controller. Conditions to record Usage Pass into Qualified Storage are described in section 9.2.2 of SAFIA/PDS1.

4 Rule for modification of Access Condition for Storage Module

Access Condition for Storage Module shall be modified and updated as described in section 7.3 of SAFIA/PDS1 when the Qualified Storage Controller records the received Usage Pass into Qualified Storage or the Usage Pass Transfer Unit outputs a Usage Pass to other Device through the Storage Interface Unit.

5 Requirements for protocol implementation

The Storage Interface Unit and the Storage Module in the Storage Device shall implement the functions for both UT and BT mode. As for UT mode, functions which are necessary to execute all

© SAFIA License Group, 2008. All rights reserved.

stages shall be implemented on the Storage Interface and the Storage Module. Meanwhile, as to BT mode, functions which are necessary to execute all stages as the Primal shall not be implemented and all stages as the Inceptive shall be implemented.

6 Rules for log management

This chapter describes the format of Transaction Log and Connection Log when they are recorded and Transaction Status in BT mode. In the Table described in this chapter, “E/I” means “External or Internal”, “P/I” means “Primal Device or Inceptive Device”.

6.1 Transaction Log

6.1.1 UT mode

Transaction Log is recorded in Storage Module only in UT mode. In addition to the information of Transaction Log described in section 9.1.1 of SAFIA/PDS1, two kinds of information inherent to the Storage Device are recorded into the log as Usage Pass Location. Details are shown in Table 6.1.

Transaction Log has the following characteristics:

- The Storage Module shall equip the area to record at least four Transaction Logs per a Channel.
- In Usage Pass Transfer, when a new Session Key is generated (which means that the Storage Interface Unit and the Storage Module is Inceptive) or a new Session Key is received (which means that the Storage Interface Unit and the Storage Module is Primal), a new Transaction Log shall be generated. Rigorous recording and updating timing of the each field is described in SAFIA/PDS2.

© SAFIA License Group, 2008. All rights reserved.

Table 6.1 Fields of Transaction Log in UT mode

Field		E/I	P/I	Description
Usage Pass Identifier		E	P	A received Usage Pass Identifier is recorded in this field when a new Transaction Log is created.
			I	A received Usage Pass Identifier is recorded in this field when a new Transaction Log is created.
Type Map		I	P	Acceptable Usage Pass Type Map specified in the received Device Class Certificate is converted into binary values and recorded into this field when a new Transaction Log is created.
			I	Not recorded.
Inceptive Device Public Key		I	P	A received Device Public Key is recorded in this field when a new Transaction Log is created.
		I	I	Not recorded.
Inceptive Session Key		I	P	A received Session Key is recorded into this field when a new Transaction Log is created.
			I	A Session Key generated in the Storage Module is recorded into this field when a new Transaction Log is created.
Session Status		E	P	There are two states: Send Prepared (SP) and Send Completed (SC). SP is set to this field when a Transaction Log is created. The state is updated to SC after the Usage Pass Transfer Unit in Storage Module receives a command to output the objective Usage Pass. After the updating of the state finishes, encryption of the Usage Pass to be output is started.
			I	There are two states: Receive Prepared (RP), Receive Completed (RC). RP is set to this field when a Transaction Log is created. The state is updated to RC after the Usage Pass Transfer Unit in the Storage Module receives the encrypted Usage Pass, decrypts the received data and verifies the structure of it.
Original Access Condition		I	P	Access Condition for Storage Module which has not been modified yet is recorded when a new Transaction Log is created.
			I	Not recorded.
Usage Pass Location	LBAQ	E	P	The value of LBAQ where the Usage Pass to be output is recorded in this field when a new Transaction Log is created.
			I	The value of LBAQ specified by the Host Interface Unit is recorded into this field after the Storage Module receives the encrypted Usage Pass, decrypts the received data and verifies the structure of it.
	Sector Length		P	Sector length of Usage Pass to be output is recorded into this field when LBAQ is recorded into Transaction Log.
			I	Sector length of the received Usage Pass is recorded into this field when LBAQ is recorded into Transaction Log.

6.1.2 BT mode

Transaction Log is not recorded in the Storage Module but may be recorded in the Import, Export or Transmit Module (one of them is selected depending on the purpose of Usage Pass Transfer) in the Primal Device in BT mode. If a Transaction Log is recorded in the Module, LBAQ where objective Usage Pass exists is set to Usage Pass Location field. For other fields, values described in section 9.2.2 of SAFIA/PDS1 shall be set. Rigorous recording and updating timing of

© SAFIA License Group, 2008. All rights reserved.

the each field is described in SAFIA/PDS2.

6.2 Connection Log

Connection Log may be recorded in the Storage Module only in BT mode. Recording of multiple entries of Connection Log is allowed, with the proviso that retaining of valid multiple entries for a Host Device is prohibited. The number of entries which Storage Device records shall be less than or equal 15. An entry of the log includes six fields described in section 9.2.1 of SAFIA/PDS1. All fields of the log shall be recorded at the same time in the Storage Module just after the Storage Module receives and decrypts the encrypted Session Key generated in the Primal Device on Connection Stage. Self Session Key and Partner Session Key shall be updated just after the Storage Module receives and decrypts the encrypted Session Key generated in the Primal Device on Reconnection Stage. Rigorous recording and updating timing of the each field is described in SAFIA/PDS2.

Table 6.2 Fields of a Connection Log

Field	E/I	Description
Self Session Key	I	A Session Key on Connection Stage generated in the Storage Module is recorded into this field.
Partner Session Key	I	A Session Key on Connection Stage generated in the Primal Device and sent from it is recorded into this field.
Partner Device Public Key	I	A Device Public Key installed in the Primal Device and sent from the Device is recorded into this field.
Type Map	I	Acceptable Usage Pass Type Map specified in the Device Class Certificate installed in the Primal Device and sent from the Device is converted into binary values and recorded into this field.
Partner Message Version	I	$MVB_{[P]}$ included in Initlal_PrimalSession sent from the Primal Device is recorded into this field.
Primal Device Specifier	E	Serial Number of Device Class Certificate sent from the Primal Device is recorded into this field.

6.3 Clearance Policy of Transaction Log and Connection Log

The clearance policy of Transaction Log and Connection Log shall follow the description provided in chapter 9 of SAFIA/PDS1.

6.4 Recovery-Allowed Primal Device Indicator

Recovery-Allowed Primal Device Indicator is recorded in the Storage Module only in BT mode. The information described in section 9.2.3 of SAFIA/PDS1 is included in this indicator. The rigorous timing of recording or updating of the indicator is described in SAFIA/PDS2.

Table 6.3 Recovery-Allowed Primal Device Indicator

Field	E/I	Description
Connection Log Entry Pointer	E	Information to designate an entry of Connection Log for the Primal Device is recorded, where most recent Usage Pass Transfer has been executed between the Host Device and this Storage Device.

© SAFIA License Group, 2008. All rights reserved.

The Figure 6.1 illustrates the relation between Connection Log and Recovery-Allowed Primal Device Indicator.

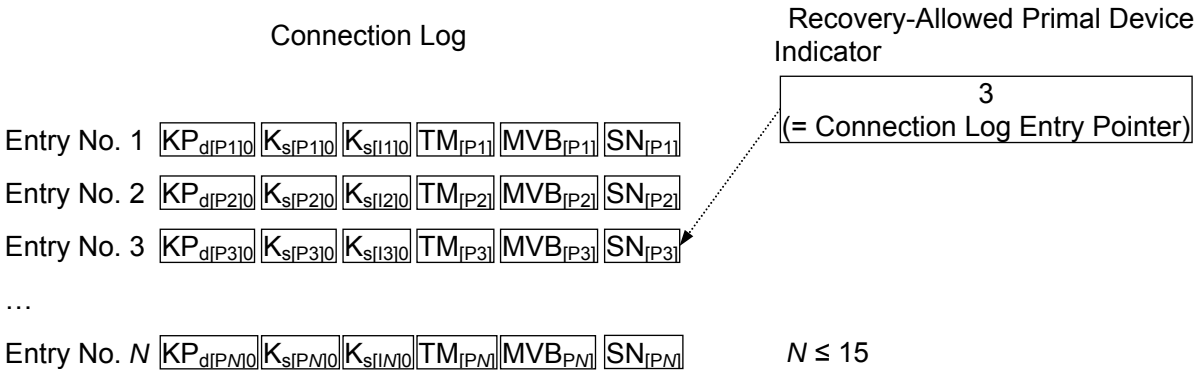

Figure 6.1 Connection Log and Recovery-Allowed Primal Device Indicator in Storage Device

In the situation where Recovery-Allowed Primal Device Indicator designates the entry to be overwritten with the information as to different Host Device (it corresponds to a case where entry whose number is 3 is overwritten in Figure 6.1), the information recorded in Recovery-Allowed Primal Device Indicator shall be cleared. It means that the indicator shall not designate any entry of Connection Log.

When the Partner Message Version, which is recorded in the entry of Connection Log, is 0000h, only Reconnection Stage execution with the entry of Connection Log designated by Recovery-Allowed Primal Device Indicator is allowed in the Storage Module.

6.5 Recovery Permission Indicator

When the following conditions are satisfied, Recovery Permission Indicator is allowed to be set to 0001h by the Inceptive UPTU in the Storage Device. In other case, the Indicator shall be set to 0000h.

- The entry of Connection Log, which is designated by Recovery-Allowed Primal Device Indicator, is selected to execute Reconnection Stage and the Recovery_PrimalConnection message is verified.

© SAFIA License Group, 2008. All rights reserved.

Annex A Requirements for implementation of Storage Module

A.1 Robustness of Storage Module

Storage Module shall be implemented so as to satisfy the following conditions.

- Methods to access to Storage Module through the Device Interface do not exist other than the one by the execution sequences of the subcommands defined in Qualified Access mode of which identifier is 0 (subcommands included in SAFIA UT feature set) and 1 (subcommands included in SAFIA BT feature set) described in iVDR/IF and SAFIA/IF. In this sense, Qualified Storage is logically built as a part of Qualified Space defined in iVDR/IF.
- In case where Qualified Storage is built on magnetic recording medium, all data recorded in it shall be encrypted. The example of cryptosystem is AES of which key length is 128-bit. The algorithm is specified in FIPS197.
- The key with which the encryption described above is executed shall be implemented in compliance with the Robustness Rules.
- In case where Qualified Storage is not built on magnetic recording medium, it shall be implemented in compliance with the Robustness Rules.
- The key with which the encryption described above is executed shall be unique for every Storage Module that a manufacturer produces.
- A Device Class Certificate, a Device Class Private Key, a Device Public Key and a Device Private Key that are installed in each Device shall be implemented in compliance with the Robustness Rules.

A.2 Capacity of Qualified Storage

Capacity of Qualified Storage in a Storage Device shall be larger than 0.1 % of the capacity of Open Storage.

© SAFIA License Group, 2008. All rights reserved.