

Security Architecture for Intelligent Attachment Device Keying Material Ordering Guide

August 27, 2010

- *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 © 2010 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	References	4
2	Introduction.....	4
3	Licensed objects distributed by SAFIA License Group	5
3.1	Root Public Key	5
3.2	Device Class Certificates	5
3.3	Device Proper Keys	5
4	Order request process	5
5	Order delivery formats	5
5.1	Structure of a SAFIA Key Set Package.....	5
5.2	Structure of a header of a SAFIA Key Set Package.....	6
5.2.1	Identifier	6
5.2.2	Version	6
5.2.3	Serial number	6
5.2.4	Size	6
5.2.5	Number	6
5.3	Structure of a SAFIA Key Set.....	6
6	Cryptographic protection for orders.....	7
Annex A	Keying material ordering form on Security Architecture for Intelligent Attachment Device	8
Annex B	Common Keying material ordering form on Security Architecture for Intelligent Attachment Device	9

1 References

- 1) ISO/IEC 646,
Information technology, ISO 7-bit coded character set for information interchange, 1991,
(ISO/IEC646)
- 2) ITU-T Recommendation X.680,
Data Networks and Open System Communications OSI Networking and System Aspects -
Abstract Syntax Notation One Information Technology – Abstract Syntax Notation One
(ASN.1): Specification of Basic Notation [X680]
- 3) Security Architecture for Intelligent Attachment Device Specifications
Protocol and Data Structure volume 1 [SAFIA/PDS1]
- 4) Security Architecture for Intelligent Attachment Device Specifications
Protocol and Data Structure volume 2 [SAFIA/PDS2]
- 5) Security Architecture for Intelligent Attachment Device Specifications
Storage Device with AT Attachment interface [SAFIA/SD]
- 6) Security Architecture for Intelligent Attachment Device Specifications
Recording and Playback Device for iVDR - TV Recording Specification [SAFIA/RPD-TV]
- 7) Security Architecture for Intelligent Attachment Device Specifications
Recording and Playback Device for iVDR - Audio Stream Recording [SAFIA/RPD-Audio]

2 Introduction

The Security Architecture for Intelligent Attachment Device Specifications relies on strong cryptographic technologies to provide flexible and robust copy protection for Devices. These cryptographic technologies require an appropriate supportive infrastructure in which it is necessary to generate and distribute Security Architecture for Intelligent Attachment Device keying material consisting of Root Public Key, Device Class Certificate or Common Device Class Certificate, Device Proper Keys or Common Device Proper Keys, and other necessary components described in the Security Architecture for Intelligent Attachment Device Specifications. A packaged data which includes a Device Root Key, a Device Class Certificate or Common Device Class Certificate (in which one of the Device Proper Key, namely Device Class Public Key, is included), and Device Proper Keys or Common Device Proper Keys generated for a specific Device is called as a “SAFIA Key Set.” A set of one or more SAFIA Key Sets ordered by a manufacturer is called as a “SAFIA Key Set Package”.

3 Licensed objects distributed by SAFIA License Group

3.1 Root Public Key

A Root Public Key is included in a SAFIA Key Set.

3.2 Device Class Certificates

The following Device Class Certificates are available from SAFIA Agent. Each Device Class Certificate includes one Device Class Public Key described in Table 3.1.

Table 3.1 Variety of available Device Class Certificates

Device	Stream Type	Device Type Name	Acceptable Usage Pass Type Map	References
Storage Device	–	DRV	FFFFFFFF FFFF0000h	SAFIA/PDS1, SAFIA/SD
Host Device	TV	RP1	02000000 00000000h	SAFIA/PDS1, SAFIA/RPD-TV
	Audio	RP1	04000000 00000000h	SAFIA/PDS1, SAFIA/RPD-Audio
	TV & Audio	RP1	06000000 00000000h	SAFIA/PDS1, SAFIA/RPD-TV, SAFIA/RPD-Audio

A Device Class Certificate is included in a SAFIA Key Set.

3.3 Device Proper Keys

A Device Class Private Key corresponding to a Device Class Public Key in the Device Class Certificate and a pair of a Device Private Key and a Device Public Key are included in a SAFIA Key Set.

4 Order request process

In order to place an order, a licensed manufacturer must complete the form provided in Annex A or Annex B of this document and return it with payment to the SAFIA Agent. Payment must accompany each order, or be received subsequent to order placement, before a request to the signing facility for keys will be processed.

The SAFIA Agent mail address is info@safia-lb.com.

5 Order delivery formats

The SAFIA Agent provides SAFIA Key Sets to the adapter as a format described in this chapter.

5.1 Structure of a SAFIA Key Set Package

Structure of a SAFIA Key Set Package is described in Table 5.1.

Table 5.1 Structure of a SAFIA Key Set Package

Byte point	Size in bytes	Description
0	23	Header
23	594	SAFIA Key Set (1)
617	594	SAFIA Key Set (2)
		...
$23 + 594 \times (N - 1)$	594	SAFIA Key Set (N)

5.2 Structure of a header of a SAFIA Key Set Package

Structure of the Header in a SAFIA Key Set Package is described in Table 5.2.

Table 5.2 Structure of a header of a SAFIA Key Set Package

Byte point	Size in bytes	Field	Value (ex.)
0	5	Identifier	53 41 46 49 41h (fixed)
5	1	Version	01h (fixed)
6	10	Serial number	0100 00000000 00000000h
16	3	Size	252h (fixed)
19	4	Number	FFFFFFFFh

5.2.1 Identifier

This field is always filled with 53 41 46 49 41h, which is “SAFIA” in character cords specified in ISO/IEC646.

5.2.2 Version

This field is filled with 01h, which is a version of the structure of SAFIA Key Set Package.

5.2.3 Serial number

This field is filled with a serial number described in the Device Class Certificate in the first SAFIA Key Set (ref. SAFIA Key Set (1) in Table 5.1). The serial number described in the Device Class Certificate in the N th SAFIA Key Set is $SN_0 + N - 1$, where SN_0 is the serial number described in the Device Class Certificate in the first SAFIA Key Set.

5.2.4 Size

This field is filled with the size in byte of each SAFIA Key Set.

5.2.5 Number

This field is filled with the number of SAFIA Key Sets which are included in this SAFIA Key Set Package.

5.3 Structure of a SAFIA Key Set

The structure of a SAFIA Key Set is described in Table 5.3.

Table 5.3 Structure of a SAFIA Key Set

Byte point	Size in bytes	Field		Value
0	1	tag		30h; Sequence type tag (see X680)
1	3	length		82 02 4Ch (ex.)
4	1	kpr	tag	52h; EccPublicKey type tag (see SAFIA/PDS2)
5	1		length	40h
6	64		data	KP_r
70	1	kd	tag	54h; EccPrivateKey type tag (see SAFIA/PDS2)
71	1		length	20h
72	32		data	K_d
104	1	kpd	tag	52h; EccPublicKey type tag (see SAFIA/PDS2)
105	1		length	40h
106	64		data	KP_d
170	1	kdc	tag	54h; EccPrivateKey type tag (see SAFIA/PDS2)
171	1		length	20h
172	32		data	K_{dc}
204	M	dcc		Device Class Certificate (see SAFIA/PDS1)
$204 + M$	$594 - (204 + M)$	-		Padded with zeros

6 Cryptographic protection for orders

A robust, commercially available hybrid cryptographic system is used to protect the integrity of device packages transported via common carrier between SAFIA License Group and the manufacturer. The protection is necessary to ensure the authenticity and confidentiality of the order. Network Associates' PGP is the product which has been chosen to protect each order during distribution.

It can be obtained from PGP Corporation (www.pgp.com).

Manufacturers must obtain a copy of PGP and generate a public/private key pair of type Diffie-Hellman/DSS with a size of 2048. Prior to placing an order with SAFIA License Group, manufacturers will provide their public key in an authenticated manner (as part of the Activation Notice) with SAFIA License Group.

The SAFIA License Group Signing Facility fills the order, encrypting the contents of the order using PGP with the manufacturer's public key prior to writing it to CDROM media.

When the manufacturer receives the CDROM containing the order from SAFIA License Group, the manufacturer can decrypt the order using their private key prior installing the cryptographic materials in Devices.

If for some reason a manufacturer cannot use PGP, they should contact SAFIA License Group to see if an alternative delivery option can be arranged.

The CDROM typically contains a file "SAFIA_DCC_Order_JJJJ.bin.pgp" that contains the keying material in format as described in section 5.

Annex A Keying material ordering form on Security Architecture for Intelligent Attachment Device

Manufacturer (Company Name): _____

Licensee ID:

Addressee Name (please print): _____

Title: _____

Delivery address: _____

Phone: _____

Fax: _____

E-mail: _____

Comment: _____

Order Format: Please fill out the blanks. See SAFIA/PDS1, SAFIA/SD, SAFIA/RPD-TV and SAFIA/RPD-Audio in detail. And select only ONE Device check box either 1 or 2 in the following. If you select 2 (Host Device), please also select either i or ii or both:

- 1. Storage Device (DRV)
- 2. Host Device (RP1)
 - i. TV Stream Recording
 - ii. Audio Stream Recording

Quantity of SAFIA Key Sets (maximum number is 1,000,000):

Authorized signature: _____

Name (please print): _____

Title: _____

Date: _____

PGP Key Name: _____

PGP fingerprint: _____

All orders, Devices, Root Public Key, Device Class Certificates and Device Proper Keys are subject to compliance with the terms of manufacturer's License Agreement with the SAFIA License Group.

Please allow at least ten (10) business days for the processing of orders after an acceptable order form is received by SAFIA License Group and applicable payment is made. Actual turn around time for order fulfillment may vary depending on the volume of Devices being ordered, the number of pending orders and shipping time.

Annex B Common Keying material ordering form on Security Architecture for Intelligent Attachment Device

Manufacturer (Company Name): _____

Licensee ID:

Addressee Name (please print): _____

Title: _____

Delivery address: _____

Phone: _____

Fax: _____

E-mail: _____

Comment: _____

Order Format: Please fill out the blanks. See SAFIA/RPD-TV in detail. And select only ONE check box of a maximum number of units or copies:

1. Host Device (RP1) TV Stream Recording

- i. Up to 100,000 units or copies
- ii. Up to 1,000,000 units or copies
- iii. Up to 10,000,000 units or copies
- iv. Over 10,000,000 units or copies

Quantity of SAFIA Key Sets (maximum number is 10):

Authorized signature: _____

Name (please print): _____

Title: _____

Date: _____

PGP Key Name: _____

PGP fingerprint: _____

All orders, Devices, Root Public Key, Device Class Certificates and Device Proper Keys are subject to compliance with the terms of manufacturer's License Agreement with the SAFIA License Group.

Please allow at least ten (10) business days for the processing of orders after an acceptable order form is received by SAFIA License Group and applicable payment is made. Actual turn around time for order fulfillment may vary depending on the volume of Devices being ordered, the number of pending orders and shipping time.