

Security Architecture for Intelligent Attachment Device Specifications

– Recording and Playback Device
for iVDR - Audio Stream Recording –

Version 2.00

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>.

Table of Contents

| | | |
|----------|--|-----------|
| 1 | General | 1 |
| 1.1 | Scope..... | 1 |
| 1.2 | References..... | 1 |
| 1.3 | Definitions | 1 |
| 1.3.1 | Definitions in iVDR/ARS | 1 |
| 1.3.2 | Definitions in SAFIA/IF | 1 |
| 1.3.3 | Definitions in SAFIA/PDS1 | 2 |
| 1.3.4 | Additional definitions | 3 |
| 1.4 | Abbreviations | 4 |
| 1.4.1 | Abbreviations in SAFIA/PDS1 | 4 |
| 1.4.2 | Additional abbreviations | 5 |
| 1.5 | Conventions | 6 |
| 1.5.1 | Keywords..... | 6 |
| 1.5.2 | Numerical values..... | 6 |
| 1.6 | Notations..... | 6 |
| 1.6.1 | Keys | 6 |
| 1.6.2 | Operations..... | 6 |
| 2 | Outline of recording and playback..... | 7 |
| 2.1 | Described part..... | 7 |
| 2.2 | Recording Device..... | 7 |
| 2.3 | Playback Device | 8 |
| 2.4 | Outline of recording..... | 8 |
| 2.5 | Outline of playback..... | 9 |
| 3 | Device Class Certificate | 11 |
| 3.1 | Device Type Name..... | 11 |
| 3.2 | Acceptable Usage Pass Type Map | 11 |
| 4 | Requirements for protocol implementation | 12 |
| 5 | Usage Pass | 13 |
| 5.1 | Usage Pass Type Map..... | 13 |
| 5.2 | Usage Pass Identifier | 13 |
| 5.3 | Access Condition for Storage Module (AC _s) | 13 |
| 5.3.1 | Control Count | 13 |
| 5.3.2 | Move Control for Storage Module..... | 13 |
| 5.4 | Cipher Information of Content | 13 |
| 5.5 | Access Condition for Export Module (AC _e) | 13 |
| 5.6 | Content Identifier..... | 14 |

| | | |
|-----------|---|-----------|
| 6 | Copy control management | 15 |
| 6.1 | Rules of Control Count in Recording Device | 15 |
| 6.2 | Rules of Control Count in Playback Device | 16 |
| 7 | SAFIA Audio Stream | 17 |
| 7.1 | Definition of SAFIA Audio Stream | 17 |
| 7.2 | Structure of SAFIA Audio Stream | 17 |
| 7.3 | SAFIA Audio Stream Entity General Information | 17 |
| 7.3.1 | SAFIA Specific Information Type | 18 |
| 7.3.2 | SAFIA Specific Information | 18 |
| 7.4 | SAFIA Audio Stream Entity and Usage Pass | 19 |
| 7.5 | Encryption and decryption scheme of ARS Track Data | 20 |
| 7.5.1 | Calculation of Initialization Vector | 20 |
| 7.5.2 | Encryption of ARS Track Data | 20 |
| 7.5.3 | Decryption of Encrypted ARS Track Data | 21 |
| 8 | Directories and files | 23 |
| 8.1 | Restrictions on file system | 23 |
| 8.2 | Location of directories and files | 23 |
| 8.3 | iVDR_AUR (Directory) | 24 |
| 8.4 | RT_RAC (Directory) and xx (Directory) under RT_RAC | 24 |
| 8.5 | RACxx.ARS | 24 |
| 8.6 | Named stream | 24 |
| 8.6.1 | PlaybackInfo | 24 |
| 8.6.2 | iVDR_UCInfo | 24 |
| 9 | Playback Information | 25 |
| 9.1 | Playback Information General Information | 25 |
| 9.2 | Playback Information Type Specific Data | 25 |
| 9.2.1 | Playback Information Type Specific Data General Information | 25 |
| 9.2.2 | Usage Pass Effective Range Entry (PERE) | 26 |
| 9.2.3 | Restriction to Playback Information Type Specific Data | 27 |
| 10 | iVDR Usage Control Information Stream | 28 |
| 10.1.1 | Restriction of location | 28 |
| 10.1.2 | Restriction of the order of Usage Pass Location field | 28 |

1 General

1.1 Scope

This document describes the encryption and decryption procedures of Audio Content required to be protected. File structure and format of the Audio Content are specified in iVDR/ARS. So, in this document, file structure and format specific to Protected Audio Content are described. In addition, copy control management about the Protected Audio Content is also described.

1.2 References

- 1) iVDR Hard Disk Drive Consortium,
Audio Recording Specification Version 1.10, January 2007 [iVDR/ARS]
- 2) National Institute of Standards Technology (NIST), Federal Information Processing
Standards Publication 197,
Advanced Encryption Standard (AES), November 26, 2001 [FIPS197]
- 3) National Institute of Standards Technology (NIST), Special Publication 800-38A
Recommendation for Block Cipher Modes of Operation, 2001 [SP800-38A]
- 4) Security Architecture for Intelligent Attachment Device Specifications
File System for iVDR [SAFIA/FS]
- 5) Security Architecture for Intelligent Attachment Device Specifications
Interface for iVDR [SAFIA/IF]
- 6) Security Architecture for Intelligent Attachment Device Specifications
Protocol and Data Structure Volume1 [SAFIA/PDS1]
- 7) Security Architecture for Intelligent Attachment Device Specifications
Protocol and Data Structure Volume2 [SAFIA/PDS2]

1.3 Definitions

1.3.1 Definitions in iVDR/ARS

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

- ARS Audio Stream
- Audio Stream Entity TYPE
- Recorded Audio Contents
- Track Data
- Track Identifier

1.3.2 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
- Host Interface Module
- Storage Interface Unit
- Storage Interface Module

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 for Export Module
- Access Condition for Storage Module
- Bidirectional Transfer
- Cipher Information of Content
- Content Identifier
- Content Key
- Device
- Destination
- Device Class Certificate
- Device Public Key
- ECDH Shared Key
- Export
- Export Module
- Host Device
- Host Management Unit
- Import
- Import Module
- Inceptive
- Open Storage
- Qualified Storage
- Qualified Storage Controller
- Primal
- Protected
- SAFIA Content
- SAFIA Security Domain

- Security Domain
- Session Key
- Source
- Storage Device
- Storage Module
- Unidirectional Transfer
- Usage Information
- Usage Pass
- Usage Pass Copy
- Usage Pass Creator
- Usage Pass Extractor
- Usage Pass Identifier
- Usage Pass Move
- Usage Pass Play
- Usage Pass Transfer
- Usage Pass Transfer Protocol
- Usage Pass Transfer Unit

1.3.4 Additional definitions

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

- ARS Aligned Unit
A unit of Cipher Block Chaining mode of operation for ARS Audio Stream.
- ARS Track Data
Track Data specified in iVDR/ARS.
- Audio Content
Content mainly including but not limited to audio data. It may contain other kinds of data such as still picture.
- Copy
An action of export. A Host Device receives a Usage Pass from a Storage Device through Usage Pass Copy, decrypts the SAFIA Audio Stream with Content Key included in the received Usage Pass and output the decrypted Stream to the outside of SAFIA Security Domain.
- Copy Control Information
Copy Control Information is information that represents the copy control status of particular content to Recording Devices.

- Copy-control-not-asserted
A status of Copy Control Information that indicates limitations on copying is not explicitly asserted.
- Copy-never
A status of Copy Control Information that indicates such content is not to be reproduced.
- Copy-one-generation
A status of Copy Control Information that indicates only one generation of copies may be made of such content.
- Move
An action of export. A Host Device receives a Usage Pass from a Storage Device through Usage Pass Move (as a result, the original Usage Pass in the Storage Device is invalidated), decrypts the SAFIA Audio Stream with Content Key included in the received Usage Pass and output the decrypted Stream to the outside of SAFIA Security Domain.
- No-more-copies
A status of Copy Control Information that indicates such content may have originated as “Copy-one-generation”, but that the version being recorded is that one generation and that therefore no more copies are permitted.
- Playback
An action of export. A Host Device receives a Usage Pass from a Storage Device through Usage Pass Play, decrypts the SAFIA Audio Stream with Content Key included in the received Usage Pass and output the decrypted Stream to the outside of SAFIA Security Domain.
- Playback Device
A type of Host Device to export SAFIA Audio Stream.
- Recording Device
A type of Host Device to import Audio Content from other Security Domain.
- SAFIA Audio Stream
ARS Audio Stream which Track Data is encrypted.
- SAFIA Audio Stream Entity
TYPE 1 Audio Stream Entity which Track Data is encrypted.

1.4 Abbreviations

1.4.1 Abbreviations in SAFIA/PDS1

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

- AC_e
- AC_s
- AES
- BP

- BT
- CBC
- CD
- CE
- CIC
- HIFU
- HMU
- MSB
- LSB
- OST
- QST
- QSTC
- SAFIA
- SIFU
- UPC
- UP Copy
- UPE
- UP Move
- UP Play
- UP Transfer
- UPTU
- UT

1.4.2 Additional abbreviations

The following abbreviations used in this document are defined in this section:

- AAU ARS Aligned Unit
- ATD ARS Track Data
- bsbf Bit string, left bit first
- CCI Copy Control Information
- E-AAU Encrypted ARS Aligned Unit
- E-ATD Encrypted ARS Track Data
- ECB Electronic Code Book
- IV Initialization Vector

- PERE Usage Pass Effective Range Entry
- uimsbf Unsigned integer, most significant bit first

1.5 Conventions

1.5.1 Keywords

Mandatory, may, not used, optional, shall, should and reserved follow the description provided in section 1.5.1 of SAFIA/PDS1.

1.5.2 Numerical values

Numerical values follow the description provided in section 1.5.2 of SAFIA/PDS1.

1.6 Notations

The following notations are used in this document.

1.6.1 Keys

- K_c Content Key
- $K_{s[D]}$ Session Key which is generated to receive a Usage pass in a Destination Device
- $*KP_{d[D]}$ ECDH Shared Key which is symmetric key agreed with a Destination Device Public Key and random / pseudorandom number generated in a Source Device.

1.6.2 Operations

- AES-CBCD(x, y, z) Decrypting data z with a key x and an IV y through AES in CBC mode, and the decrypted result. CBC mode of operation using AES is specified in NIST SP800-38A.
- AES-CBCE(x, y, z) Encrypting data z with a key x and an IV y through AES in CBC mode, and the encrypted result. CBC mode of operation using AES is specified in NIST SP800-38A.
- AES-ECBE(x, y) Encrypting data y with a key x through AES in ECB mode, and the encrypted result. ECB mode of operation using AES is specified in NIST SP800-38A.
- + Addition
- ++ Increment by one
- - Subtraction
- = Assignment
- < Less than

2 Outline of recording and playback

2.1 Described part

Figure 2.1 shows Recording Device and Playback Device in SAFIA Security Domain.

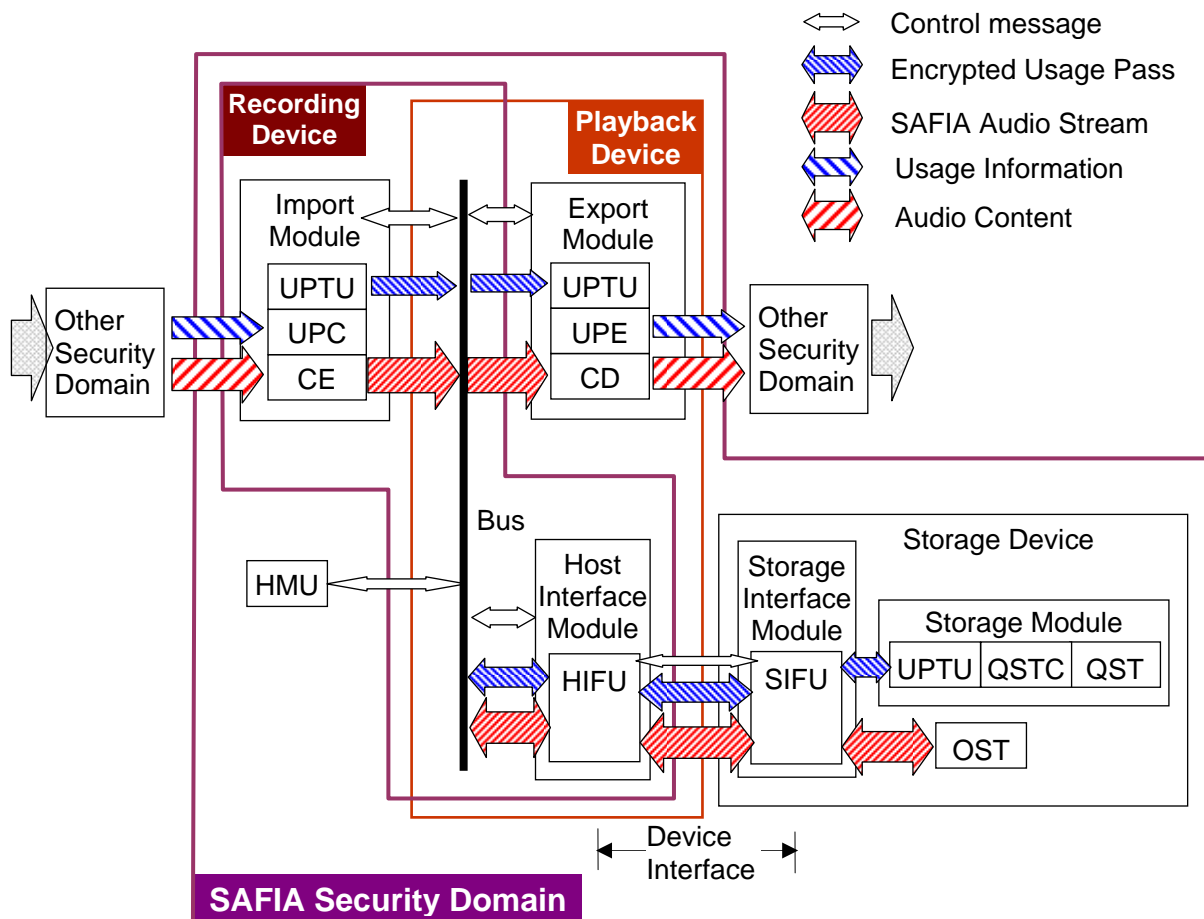


Figure 2.1 Recording Device and Playback Device

2.2 Recording Device

A Recording Device shall be a Host Device which has an Import Module to import Audio Content. Function units in Recording Device have following features.

- CE
 Functions of CE are described in section 2.3 of SAFIA/PDS1.
- HIFU
 Functions of HIFU are described in SAFIA/IF.
- UPC
 Functions of UPC are described in section 2.3 of SAFIA/PDS1.
- UPTU

Functions of UPTU are described in section 2.3 of SAFIA/PDS1. UPT of Recording Device receives a Usage Pass from UPC and sends it to a Storage Device through Usage Pass Transfer as Source.

2.3 Playback Device

A Playback Device shall be a Host Device which has an Export Module to export SAFIA Audio Stream. Function units in Playback Device have following features.

- CD

Functions of CD are described in section 2.3 of SAFIA/PDS1.

- HIFU

Functions of HIFU are described in SAFIA/IF.

- UPE

Functions of UPE are described in section 2.3 of SAFIA/PDS1.

- UPTU

Functions of UPTU are described in section 2.3 of SAFIA/PDS1. UPT of Playback Device receives a Usage Pass from a Storage Device through Usage Pass Play as Destination and sends it to UPE.

2.4 Outline of recording

Figure 2.2 shows outline of block diagram for recording. To record Audio Content, a Recording Device may take the following steps:

- Makes connection with Storage Device. The required Device Class Certificate and protocol are described in chapter 3 and chapter 4.
- Creates a Usage Pass. Its structure is described in chapter 5. And creation rule of AC_s is described in chapter 6.
- Encrypts ARS Audio Stream with Content Key in the Usage Pass and record the result as SAFIA Audio Stream to Open Storage. The details are described in chapter 7.
- Makes Playback Information and record it. Its structure is described in chapter 9.
- Makes iVDR Usage Control Information Stream and record it. It is described in chapter 10.
- Records the Usage Pass.

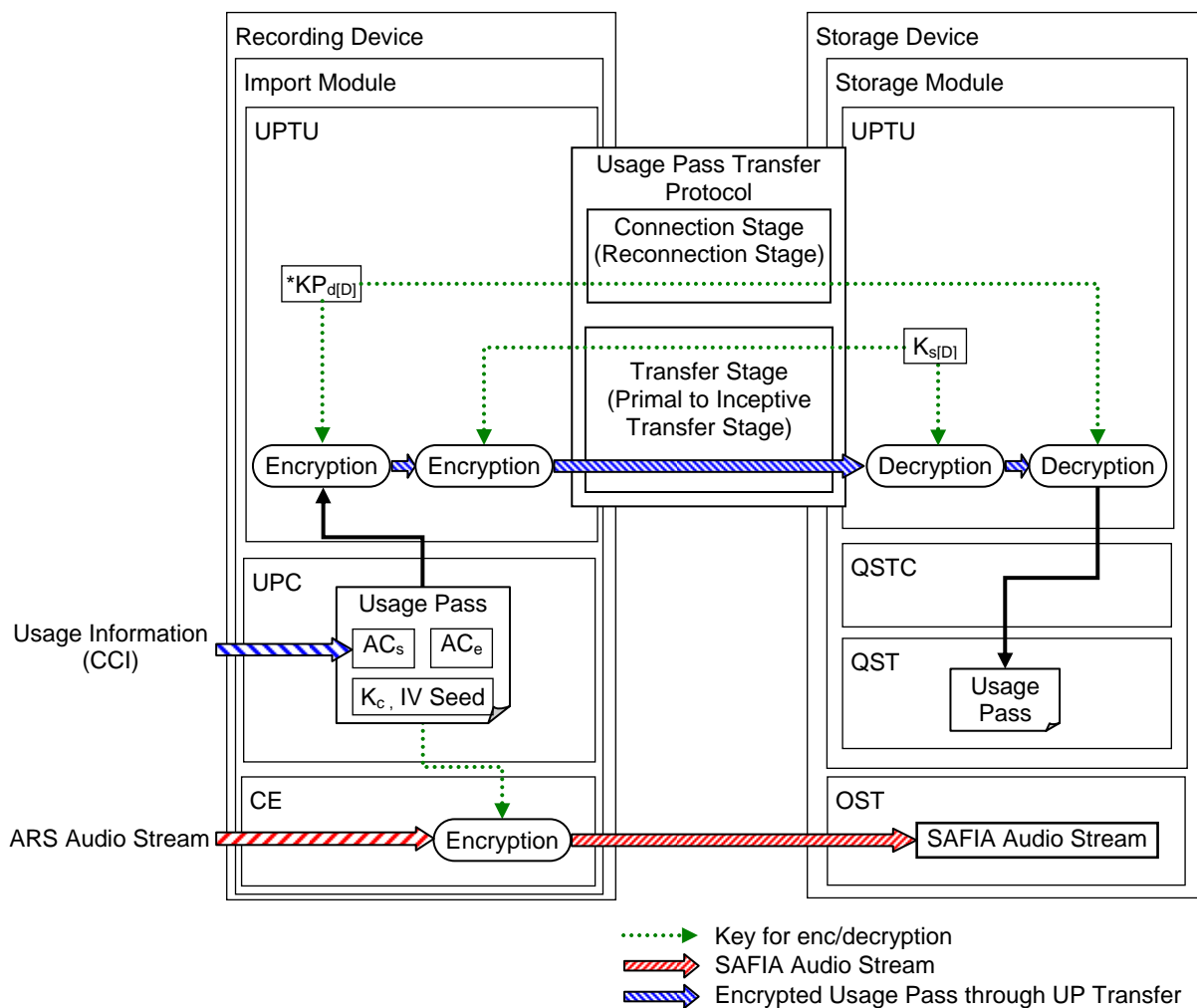


Figure 2.2 Outline of block diagram for recording

2.5 Outline of playback

Figure 2.3 shows outline of block diagram for playback. For playback a SAFIA Audio Stream, a Playback Device may take the following steps:

- Makes connection with Storage Device. The required Device Class Certificate and protocol are described in chapter 3 and chapter 4.
- Reads Playback Information described in chapter 9, then gets Usage Pass Identifier related to the playback range in the SAFIA Audio Stream.
- Reads iVDR Usage Control Information Stream described in chapter 10, then gets location of Usage Pass related to the Usage Pass Identifier described in Playback Information.
- Reads the Usage Pass. Its structure is described in chapter 5.
- Reads the SAFIA Audio Stream from Open Storage.
- Decrypts the SAFIA Audio Stream with Content Key in the Usage Pass. The details are described in chapter 7.

- Outputs Audio Content conformed to AC_s . Output rule of Audio Content is described in chapter 6.

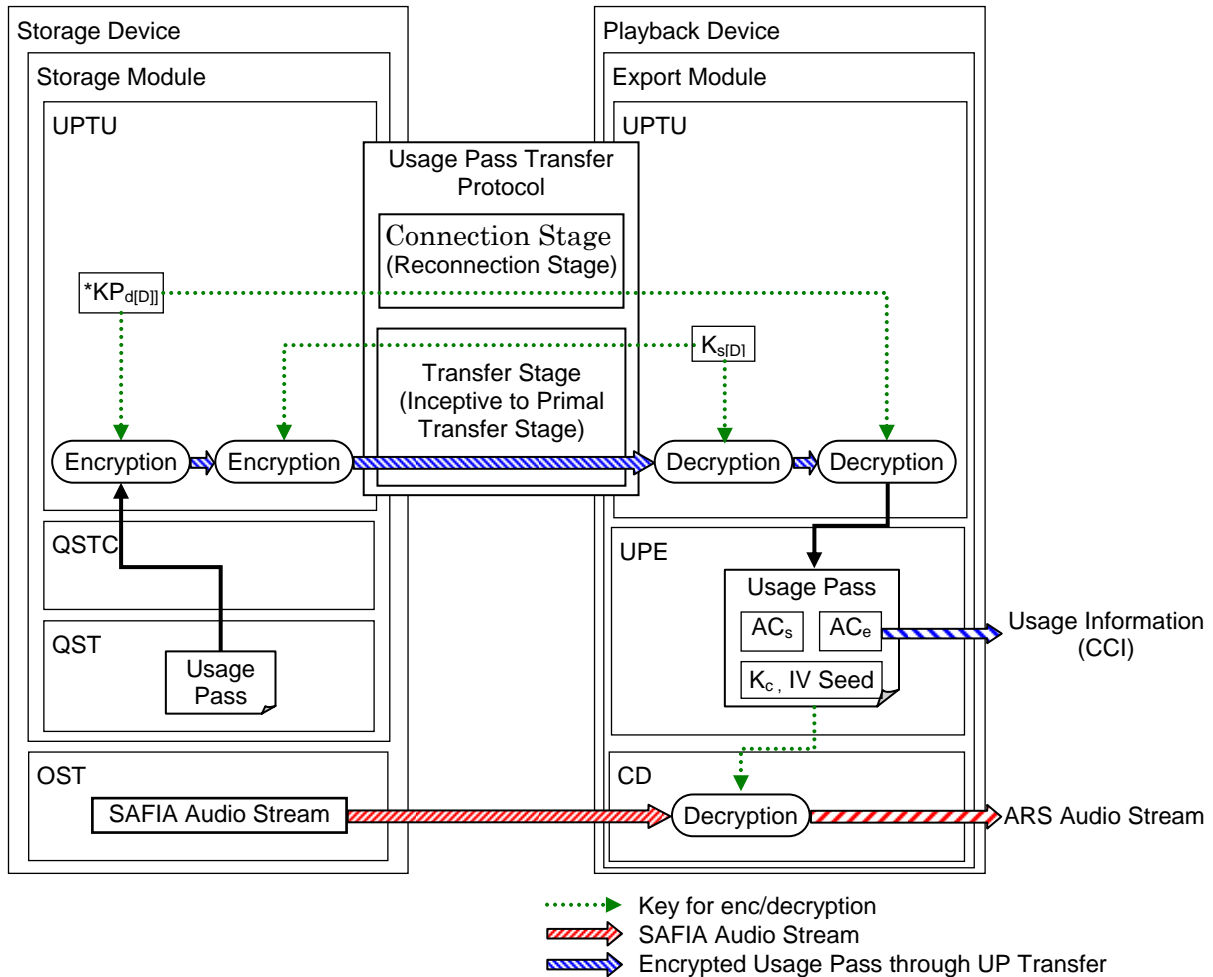


Figure 2.3 Outline of block diagram for playback

3 Device Class Certificate

Device Class Certificate is described in chapter 8 of SAFIA/PDS1. And this section describes the information of Device Class Certificate specific to Recording and Playback Device for Audio Content recording and playback.

3.1 Device Type Name

This value is “RP1”.

3.2 Acceptable Usage Pass Type Map

AT2 bit of Acceptable Usage Pass Type Map is 1b.

4 Requirements for protocol implementation

In this chapter, protocol implementation rules for each stage are described. Recording Device and Playback Device shall implement either UT mode or BT mode at least. The details of stages of each mode are described in chapter 6 of SAFIA/PDS1 and chapter 5 of SAFIA/PDS2. If the appliance implements UT mode, it shall comply with the rule described in Table 4.1. Meanwhile, if the appliance implements BT mode, it shall comply with the rule described in Table 4.2

Table 4.1 Protocol implementation rule for Recording / Playback Device in UT mode

| Location | Stage | | Rule | |
|--------------------|--------------------|--------------------------------------|---------------------|---------------------|
| | | | Recording Device | Playback Device |
| Primal | Connection | | Allowed (Mandatory) | Prohibited |
| | Transfer | UP Transfer to Storage* ¹ | | |
| | | UP Copy | | |
| | | UP Move | | |
| | | UP Play | | |
| | Reconnection | | Allowed (Optional) | |
| | Recovery | | | |
| Usage Pass Inquiry | | | | |
| Inceptive | Connection | | Prohibited | Allowed (Mandatory) |
| | Transfer | | | |
| | Reconnection | | | |
| | Recovery | | | |
| | Usage Pass Inquiry | | | |

*1: UP Transfer from Import Module to Storage Module

Table 4.2 Protocol implementation rule for Recording / Playback Device in BT mode

| Location | Stage | | Rule | |
|-----------|------------------------------|--|---------------------|---------------------|
| | | | Recording Device | Playback Device |
| Primal | Connection | | Allowed (Mandatory) | Allowed (Mandatory) |
| | Primal to Inceptive Transfer | | | Prohibited |
| | Inceptive to Primal Transfer | | Prohibited | Allowed (Mandatory) |
| | Usage Pass Inquiry | | Allowed (Optional) | Allowed (Optional) |
| | Reconnection | | | |
| | Primal to Inceptive Recovery | | | Prohibited |
| | Inceptive to Primal Recovery | | Prohibited | Allowed (Optional) |
| Inceptive | - | | Prohibited | Prohibited |

5 Usage Pass

Usage Pass is described in chapter 7 of SAFIA/PDS1. This chapter describes only the information and obligation, which are specific to audio recording and playback.

5.1 Usage Pass Type Map

Usage Pass Type is type 2. Therefore, Type Map of Usage Pass Format shall be set to 0400 0000 0000 0000h.

5.2 Usage Pass Identifier

Type of Usage Pass Identifier shall be set to 02h. Version shall be set to 1h.

5.3 Access Condition for Storage Module (AC_s)

5.3.1 Control Count

Only Generation Count shall be used. Therefore, FM of Control Count shall be set to 00b. The details of copy control management using Control Count are described in chapter 6.

5.3.2 Move Control for Storage Module

MU and MB control the Move in UT and/or BT mode. In case Move of content is prohibited, these bits shall be set to 1b.

5.4 Cipher Information of Content

Table 5.1 shows the structure of CIC of Usage Pass Type 2. A Recording Device shall not output CIC except in the case of Usage Pass Transfer.

Table 5.1 Structure of CIC of Usage Pass Type 2

| BP \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|----------|-------------------------------|---|---|---|---|---|---|-------|
| 0 | (MSB) Cipher Scheme | | | | | | | (LSB) |
| 1 | (MSB) | | | | | | | |
| ... | Content Key (K _c) | | | | | | | |
| 16 | | | | | | | | (LSB) |
| 17 | (MSB) | | | | | | | |
| ... | IV Seed | | | | | | | |
| 32 | | | | | | | | (LSB) |
| 33 | | | | | | | | |
| ... | Reserved | | | | | | | |
| 64 | | | | | | | | |

- Cipher Scheme
This value is 20h.
- Content Key

This value is a 16-byte random number described in section 5.5 of SAFIA/PDS1.

- IV Seed

This value indicates the seed of IV to encrypt ARS Audio Stream and is a 16-byte random number generated in a Recording Device.

5.5 Access Condition for Export Module (AC_e)

Table 5.2 shows the structure of AC_e, which Usage Pass Type is 2.

Table 5.2 Structure of AC_e of Usage Pass Type 2

| BP \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|----------|--------------------------|---|----------|---|---|---|---|---|
| 0 | (MSB) Content Type (LSB) | | | | | | | |
| 1 | MC | | Reserved | | | | | |
| 2 | Reserved | | | | | | | |
| 3 | | | | | | | | |
| ... | | | | | | | | |
| ... | | | | | | | | |
| 127 | | | | | | | | |

- Content Type

This value indicates the Content Type as the followings:

0h: Audio Content

Others: Reserved for future extension

- MC

This value is valid when MB in AC_s is 0b, and indicates the Move Control as the followings:

00b: Move is allowed in accordance with the rules described in section 6.2.

01b: Move is allowed only to Storage Device in accordance with the rules described in section 6.2.

Others: Reserved for future extension, and Move is prohibited in this version.

5.6 Content Identifier

The value of Content Identifier shall be same as the value of Usage Pass Identifier.

6 Copy control management

6.1 Rules of Control Count in Recording Device

Recording Device shall create ACs of Usage Pass to comply with Table 6.1.

Table 6.1 Rules of Control Count in Recording Device

| AC _s Control Count | | | Permission | |
|----------------------------------|-----|-------|---------------------|-----------------------|
| FM | 00b | COUNT | 0h (No more copy) | Prohibited |
| | | | 1h (One generation) | Allowed* ¹ |
| | | | 2h (Two generation) | Prohibited |
| | | | Fh (Not asserted) | Prohibited |
| | | | Others | Prohibited |
| | 01b | | Don't care | Prohibited |
| | 10b | | Don't care | Prohibited |
| | 11b | | Don't care | Prohibited |

*1: As described in section 7.3.1.1 of SAFIA/PDS1, Storage Device records it as “No more copy”.

6.2 Rules of Control Count in Playback Device

Playback Device shall export SAFIA Audio Stream to comply with Table 6.2.

Table 6.2 Rules of Control Count in Playback Device

| AC _s Control Count | | | Purpose of Usage Pass Transfer | | | |
|----------------------------------|-----|------------|-----------------------------------|---|---|-----------------------------------|
| | | | Copy | Playback | Move | |
| FM | 00b | COUNT | 0h (No more copy) | Discard entire SAFIA Audio Stream | Available for processing | Discard entire SAFIA Audio Stream |
| | | | 1h (One generation) | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream ^{*1} | Available for processing |
| | | | 2h (Two generation) | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream ^{*1} | Discard entire SAFIA Audio Stream |
| | | | Fh (Not asserted) | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream ^{*1} | Discard entire SAFIA Audio Stream |
| | | Others | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream ^{*1} | Discard entire SAFIA Audio Stream | |
| | 01b | Don't care | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream ^{*1} | Discard entire SAFIA Audio Stream | |
| | 10b | Don't care | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream | |
| | 11b | Don't care | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream | Discard entire SAFIA Audio Stream | |

*1: This status does not exist in normal case. A stream may be treated as Control Count status of "No more copy"

7 SAFIA Audio Stream

7.1 Definition of SAFIA Audio Stream

SAFIA Audio Stream is a SAFIA Content which complies following:

- Data format of SAFIA Audio Stream shall comply with ARS Audio Stream.
- Audio Stream Entity TYPE of SAFIA Audio Stream shall be TYPE 1 Audio Stream Entity specified in iVDR/ARS.
- When ARS Audio Stream is converted to SAFIA Audio Stream, ARS Track Data of the ARS Audio Stream shall be encrypted.

7.2 Structure of SAFIA Audio Stream

A SAFIA Audio Stream consists of ARS Audio Stream General Information and SAFIA Audio Stream Entity. ARS Audio Stream General Information is specified in iVDR/ARS. SAFIA Audio Stream Entity consists of SAFIA Audio Stream Entity General Information and a set of Encrypted ARS Track Data (E-ATD). SAFIA Audio Stream Entity General Information is TYPE 1 Audio Stream Entity General Information specified in iVDR/ARS. The E-ATD is the encrypted ARS Track Data (ATD). The size of each E-ATD shall be multiples of 512-byte. An E-ATD consists of Encrypted ARS Aligned Units (E-AAUs) as shown in Figure 7.1. The E-AAU is the encrypted ARS Aligned Unit (AAU). The size of each E-AAU shall be 512-byte.

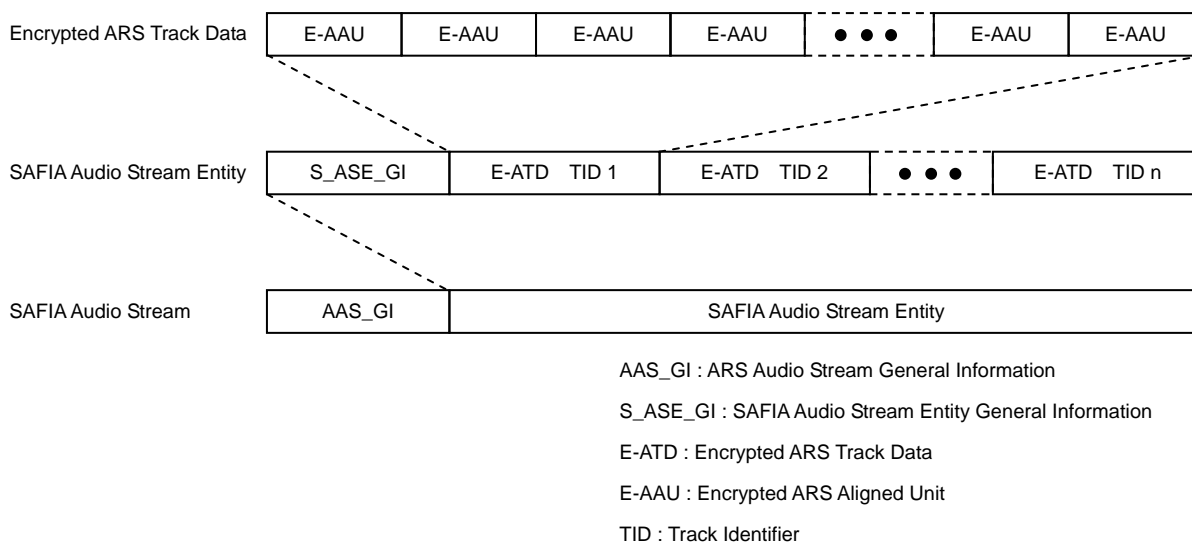


Figure 7.1 Relations among Encrypted ARS Aligned Unit, Encrypted ARS Track Data, SAFIA Audio Stream Entity and SAFIA Audio Stream

7.3 SAFIA Audio Stream Entity General Information

SAFIA Audio Stream Entity General Information is TYPE 1 Audio Stream Entity General Information specified in iVDR/ARS. In this field, Vendor Specific Information Type and Vendor Specific Information are uniquely defined in SAFIA as SAFIA Specific Information Type and SAFIA

Specific Information. This section describes the structure of Vendor Specific Information peculiar to SAFIA. This field is prepared to specify relationship between Track Identifier of ATD and Content Identifier of ATD

7.3.1 SAFIA Specific Information Type

This field is specified in iVDR/ARS as Vendor Specific Information. The value of this field shall be 01h for SAFIA.

7.3.2 SAFIA Specific Information

Figure 7.2 shows the structure of SAFIA Specific Information.

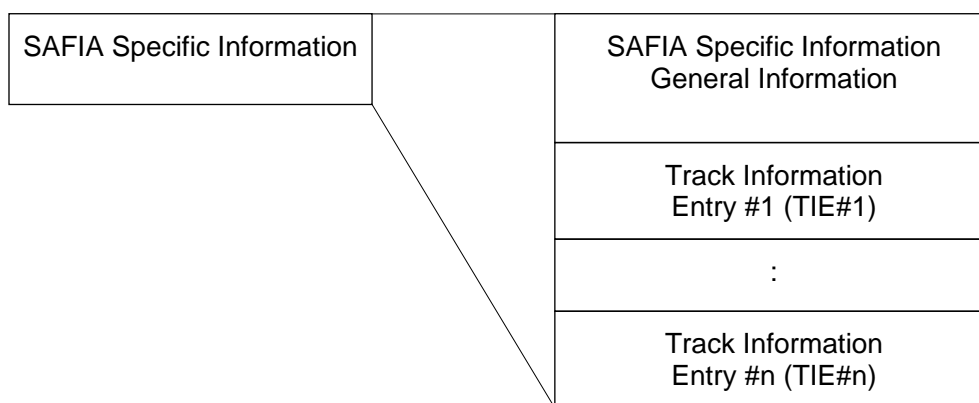


Figure 7.2 Structure of SAFIA Specific Information

7.3.2.1 SAFIA Specific Information General Information

Table 7.1 shows the structure of SAFIA Specific Information General Information.

Table 7.1 Structure of SAFIA Specific Information General Information

| BP | Length | Field name | Contents |
|----|--------|-------------------------------------|----------|
| 0 | 2 | Reserved for Flag | bslbf |
| 2 | 2 | Number of Track Information Entries | uimsbf |

7.3.2.1.1 Reserved for Flag

This field is reserved and shall be filled with zero.

7.3.2.1.2 Number of Track Information Entries

The number of Track Information Entries after SAFIA Specific Information General Information field is stored.

7.3.2.2 Track Information Entries

Table 7.2 shows the structure of Track Information Entry.

Table 7.2 Structure of Track Information Entry

| BP | Length | Field name | Contents |
|----|--------|----------------------|----------|
| 0 | 1 | Reserved for Flag | bslbf |
| 1 | 1 | Length of this Entry | uimsbf |
| 2 | 2 | Track Identifier | uimsbf |
| 4 | 32 | Content Identifier | uimsbf |

7.3.2.2.1 Reserved for Flag

This field is reserved and shall be filled with zero.

7.3.2.2.2 Length of this Entry

The length of Track Information Entry after this field shall be set to this field. The length is 22h and may be changed in the future.

7.3.2.2.3 Track Identifier

Track Identifier is set to this field.

7.3.2.2.4 Content Identifier

Content Identifier of Track Data referred by the Track Identifier described in section 7.3.2.2.3 is set to this field.

7.3.2.3 Restriction to SAFIA Specific Information

In the SAFIA Specific Information, all Track Information Entry shall be located in ascending order as to the value of Track Identifier. And Track Identifier in all Track Information Entry included in the SAFIA Specific Information shall cover all Track Identifier related to E-ATD included in the SAFIA Audio Stream Entity.

7.4 SAFIA Audio Stream Entity and Usage Pass

A SAFIA Audio Stream Entity relates to one or more Usage Passes. A Usage Pass relates to a continuous region in the SAFIA Audio Stream Entity. The continuous region consists of plural E-ATD. The relations between E-ATD and Usage Pass are described in Usage Pass Effective Range Entry as shown in section 9.2.2. Figure 7.3 shows an example of relations between E-ATD and Usage Passes. E-ATD related to a Usage Pass is numbered in ascending order from value "1" as SAFIA Track Number. SAFIA Track Number is 2-byte value and guaranteed its uniqueness in plural E-ATD related to the Usage Pass as shown in Figure 7.3.

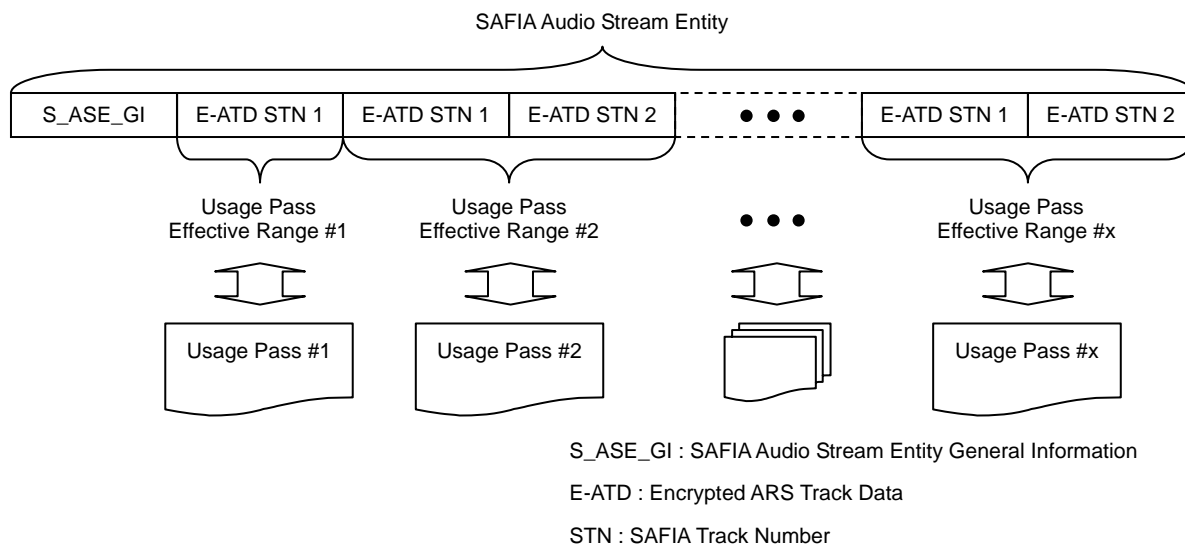


Figure 7.3 Relations between SAFIA Audio Stream Entity and Usage Pass

7.5 Encryption and decryption scheme of ARS Track Data

Each ATD is encrypted with the Content Key and IV calculated from IV Seed. Content Key and IV Seed are stored in Usage Pass related to the ATD. Details are described in section 5.4.

7.5.1 Calculation of Initialization Vector

The IV used in encryption of every AAU is 16-byte different value for each ATD. AES block cipher algorithm with 128-bit key is used for calculation of IV as shown in Figure 7.4. AES is specified in FIPS197. Its calculation is represented by the following equation

$$IV = \text{AES-ECBE}(\text{iv_seed}, \text{st_number}).$$

The *iv_seed* is a 16-byte IV Seed included in the Usage Pass related to the ATD and it is used as AES key. The *st_number* is 16-byte value of which most significant 14-byte is 00000000 00000000 0000h and rest 2-byte is SAFIA Track Number.

The IV used in decryption of E-AAU shall be same value used at the time of encryption of AAU.

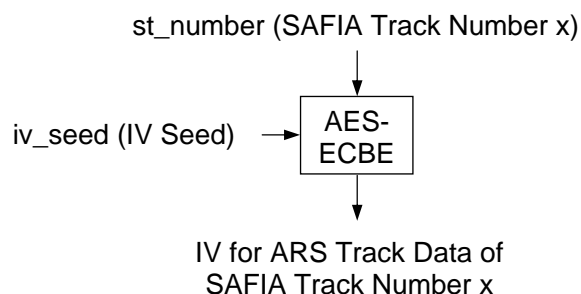


Figure 7.4 Calculation of Initialization Vector

7.5.2 Encryption of ARS Track Data

ATD consists of AAUs as shown in Figure 7.5. The size of each AAU shall be 512-byte. AES in CBC mode of operation shall be used for encryption of each AAU. Its calculation is represented

by the following equation

$$E\text{-AAU} = \text{AES-CBCE}(K_c, IV, \text{AAU}).$$

Here, the K_c is a 16-byte Content Key used as 16-byte AES key, IV is a 16-byte Initialization Vector, AAU is data to be encrypted, and AES-CBCE returns 512-byte E-AAU. K_c is included in the Usage Pass related to the ATD. AAUs included in an ATD shall be encrypted by using above function AES-CBCE similarly. Figure 7.5 shows AES based CBC encryption of ATD. The same value shall be used about IV of AAUs included in the same ATD. The value of IV corresponding to each AAU is described in section 7.5.1.

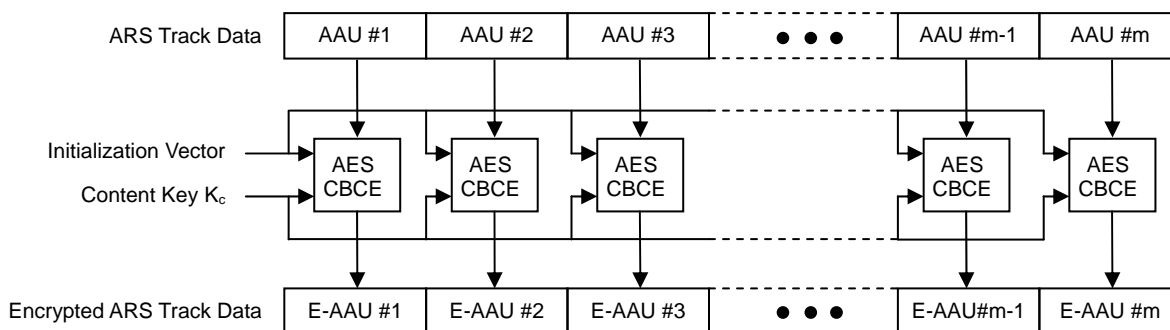


Figure 7.5 Encryption of ARS Track Data

7.5.3 Decryption of Encrypted ARS Track Data

AES in CBC mode of operation shall be used for decryption of each E-AAU. Its calculation is represented by the following equation

$$\text{AAU} = \text{AES-CBCD}(K_c, IV, E\text{-AAU}).$$

Here, the K_c is a 16-byte Content Key used as 16-byte AES key, IV is a 16-byte Initialization Vector described in section 7.5.1, E-AAU is data to be decrypted, and AES-CBCD returns 512-byte AAU. K_c is included in the Usage Pass related to the E-ATD. E-AAUs included in an E-ATD shall be decrypted by using above function AES-CBCE similarly. Figure 7.6 shows AES based CBC decryption of E-ATD. IV used at the beginning of each CBC decryption chain shall be the same IV used at the time of encryption of AAU.

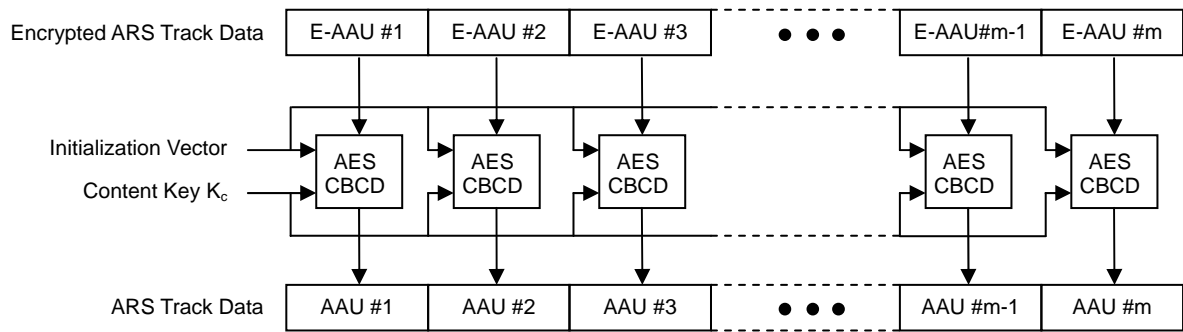


Figure 7.6 Decryption of Encrypted ARS Track Data

8 Directories and files

8.1 Restrictions on file system

All directories and files shall be recorded on the file system format described in chapter 2 of SAFIA/FS and shall be recorded only in iVDR partition.

8.2 Location of directories and files

All directories and files shall be located in accordance with iVDR/ARS. Figure 8.1 shows the location of directories and files.

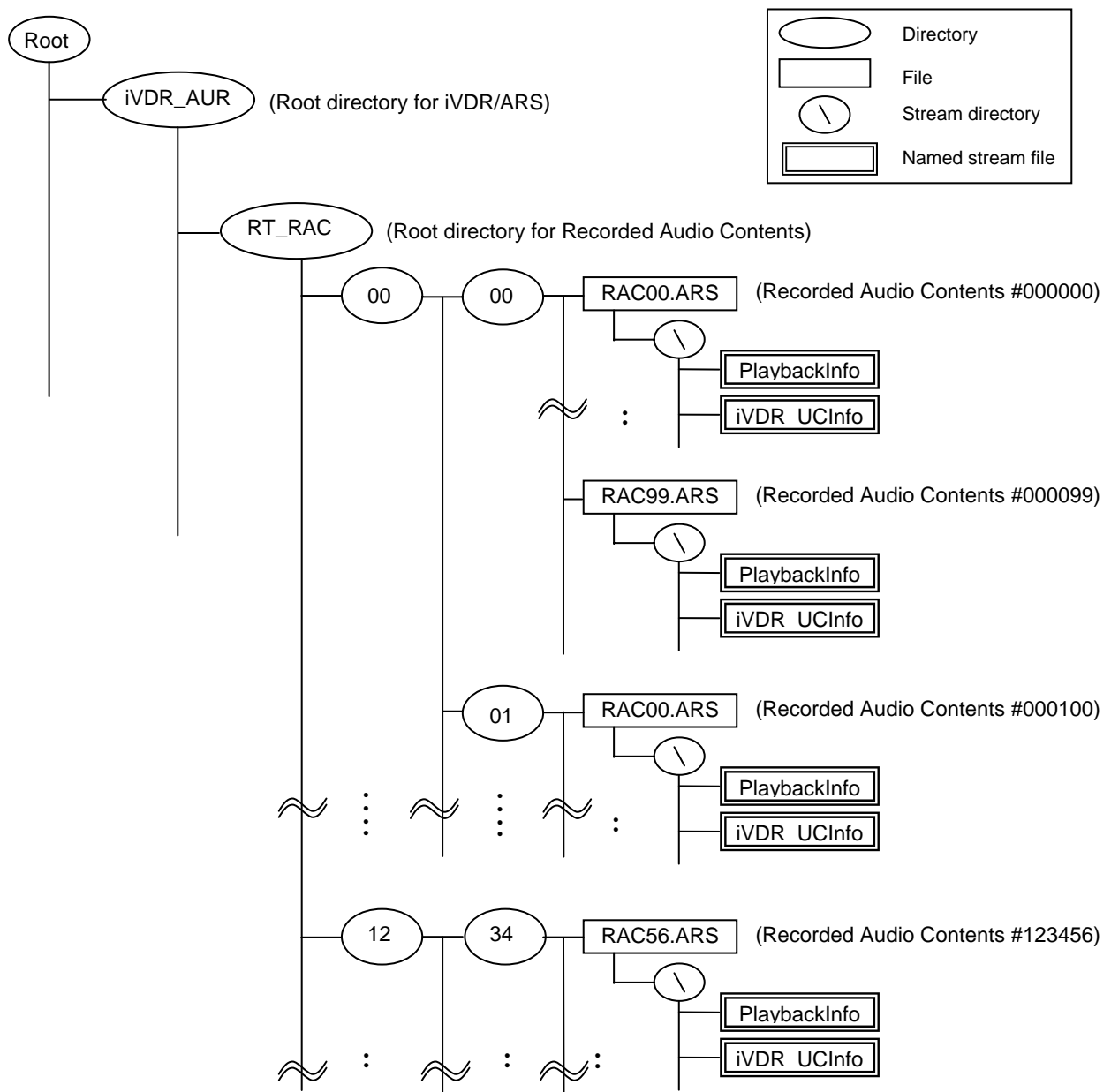


Figure 8.1 Location of directories and files

8.3 iVDR_AUR (Directory)

It is specified in iVDR/ARS.

8.4 RT_RAC (Directory) and xx (Directory) under RT_RAC

It is specified in iVDR/ARS.

8.5 RACxx.ARS

It is specified in iVDR/ARS. SAFIA Audio Stream described in chapter 7 is stored in it. It shall have two named streams; 1) PlaybackInfo, and 2) iVDR_UCInfo. In Figure 8.1, RAC00.ARS, RAC56.ARS and RAC99.ARS represent RACxx.ARS.

8.6 Named stream

8.6.1 PlaybackInfo

Playback Information described in chapter 9 is stored.

8.6.2 iVDR_UCInfo

iVDR Usage Control Information Stream described in chapter 10 is stored.

9 Playback Information

Playback Information is specified in iVDR/ARS. This chapter describes the structure of Playback Information peculiar to SAFIA. This named stream file is prepared to specify relationship between SAFIA Audio Stream and Usage Passes. Playback Information consists of Playback Information General Information and Playback Information Type Specific Data as shown in Figure 9.1.

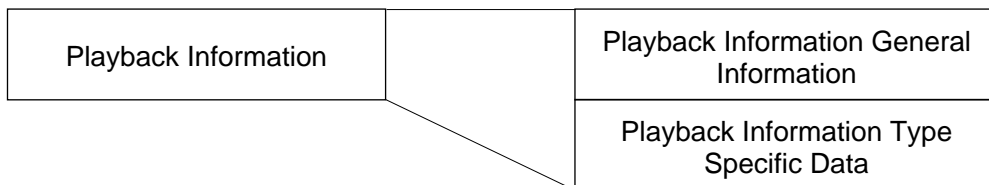


Figure 9.1 Structure of Playback Information

9.1 Playback Information General Information

This field is specified in iVDR/ARS. Playback Information Type of this field shall be 01h for SAFIA. If Playback Information Type is not 01h, corresponding ARS Audio Stream is not SAFIA Audio Stream.

9.2 Playback Information Type Specific Data

Figure 9.2 shows the structure of Playback Information Type Specific Data.

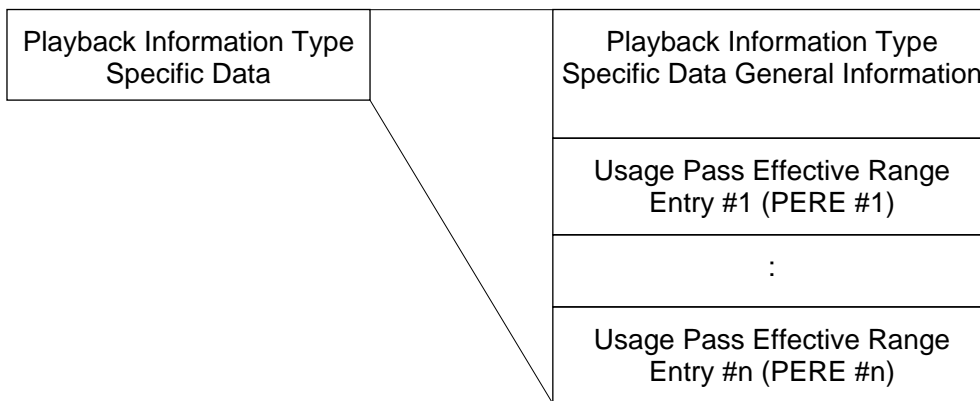


Figure 9.2 Structure of Playback Information Type Specific Data

9.2.1 Playback Information Type Specific Data General Information

Table 9.1 shows the structure of Playback Information Type Specific Data General Information..

Table 9.1 Structure of Playback Information Type Specific Data General Information

| BP | Length | Field name | Contents |
|----|--------|--|----------|
| 0 | 4 | Number of Usage Pass Effective Range Entries | uimsbf |

9.2.1.1 Number of Usage Pass Effective Range Entries

The number of Usage Pass Effective Range Entries after Playback Information Type Specific Data General Information field is stored.

9.2.2 Usage Pass Effective Range Entry (PERE)

Table 9.2 shows the structure of PERE.

Table 9.2 Structure of PERE

| BP | Length | Field name | Contents |
|----|--------|---|----------|
| 0 | 1 | Reserved for Flag | bslbf |
| 1 | 1 | Length of this Entry | uimsbf |
| 2 | 2 | Usage Pass Effective Start Track Identifier | uimsbf |
| 4 | 2 | Usage Pass Effective End Track Identifier | uimsbf |
| 6 | 1 | Reserved | bslbf |
| 7 | 1 | Usage Pass Identifier Validity Flag | bslbf |
| 8 | 32 | Usage Pass Identifier | uimsbf |

9.2.2.1 Reserved for Flag

This field is reserved and shall be filled with zero.

9.2.2.2 Length of this Entry

The length of PERE after this field shall be set to this field. The length is 26h and may be changed in the future.

9.2.2.3 Usage Pass Effective Range Start Track Identifier

Track Identifier of Usage Pass effective start ARS Track Data shall be set to this field. Namely, the Track Identifier of the first ARS Track Data among continuous ARS Track Data related to a Usage Pass shall be set. Track identifier is assigned to ARS Track Data in ascending order from 0001h and guaranteed its uniqueness in SAFIA Audio Stream as shown in Figure 9.3.

9.2.2.4 Usage Pass Effective Range End Track Identifier

Track Identifier of Usage Pass effective end ARS Track Data shall be set to this field. Namely, the Track Identifier of the last ARS Track Data among ARS Track Data related to a Usage Pass shall be set.

9.2.2.5 Reserved

This field is reserved and shall be filled with zero.

9.2.2.6 Usage Pass Identifier Validity Flag

This field indicates the validity of the Usage Pass Identifier set to next field.

00h: Usage Pass Identifier set to next field is invalid.

80h: Usage Pass Identifier set to next field is valid.

Others: Reserved for future extension.

9.2.2.7 Usage Pass Identifier

If Usage Pass Identifier Validity Flag described in section 9.2.2.6 is set to 80h, Usage Pass Identifier of Usage Pass related to ARS Track Data ranging from Usage Pass Effective Range Start Track Identifier to Usage Pass Effective Range End Track Identifier shall be set to this field. If Usage Pass Identifier Validity Flag is set to 00h, the value of this field is invalid. Usage Pass Identifier shall be 32-byte and unique in the SAFIA Security Domain. Relations between Usage Pass Identifier and physical locations of Usage Pass are described in section 3.3 of SAFIA/FS.

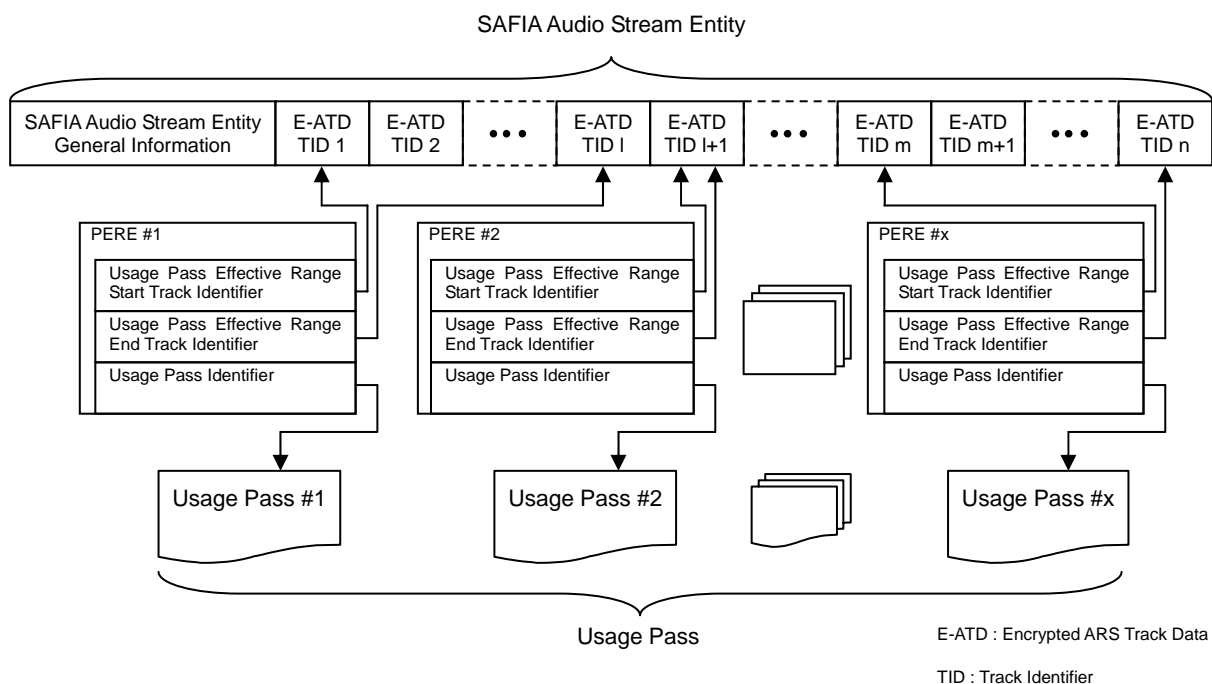


Figure 9.3 Definition of Usage Pass Effective Range Entry

9.2.3 Restriction to Playback Information Type Specific Data

In the Playback Information Type Specific Data, all PEREs shall be located in ascending order as to the value of Usage Pass Effective Range Start Track Identifier. And Track Identifier ranging from Usage Pass Effective Range Start Track Identifier to Usage Pass Effective Range End Track Identifier in all PEREs included in the Playback Information Type Specific Data shall cover all Track Identifier related to Encrypted ARS Track Data included in the SAFIA Audio Stream Entity.

10 iVDR Usage Control Information Stream

iVDR Usage Control Information Stream for SAFIA is described in section 3.3 of SAFIA/FS. Figure 10.1 shows the structure of iVDR Usage Control Information Stream Type 1.

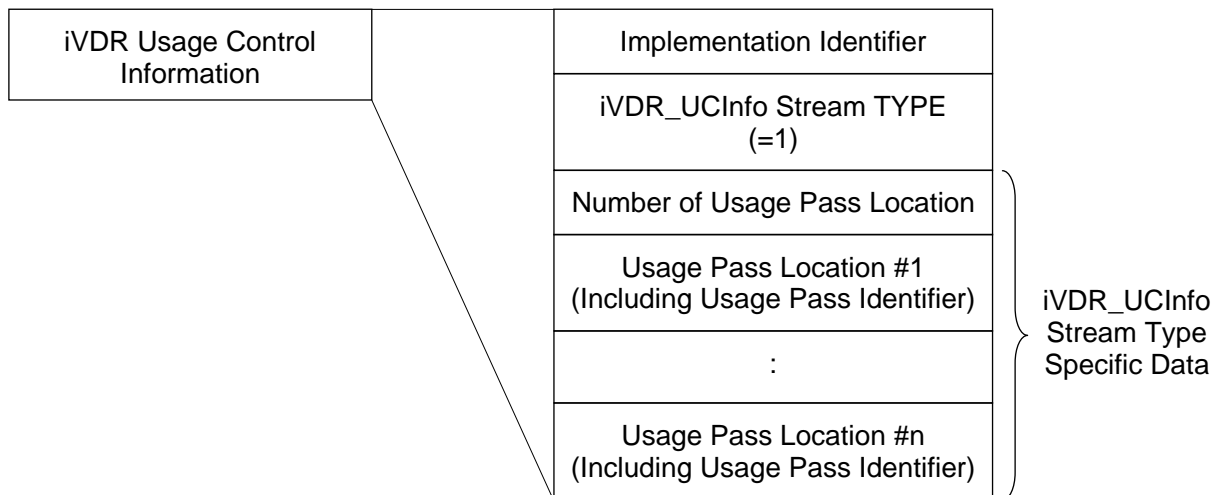


Figure 10.1 The structure of iVDR Usage Control Information Stream Type 1

10.1.1 Restriction of location

The location of iVDR Usage Control Information Stream shall belong to RACxx.ARS.

10.1.2 Restriction of the order of Usage Pass Location field

In the iVDR Usage Control Information Type Specific Data, the order of Usage Pass Locations shall be the same as the order of PEREs in the corresponding Playback Information. (i.e. The Usage Pass Identifier in PERE #n shall equal to the Usage Pass Identifier in Usage Pass Location #n.)