

Security Architecture for Intelligent Attachment Device Specifications

– Recording and Playback Device for iVDR -
TV Recording Specification –

Version 1.2.2

June 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	General	1
1.1	Scope.....	1
1.2	References.....	1
1.3	Definitions	1
1.3.1	Definitions in iVDR/TVRS.....	1
1.3.2	Definitions in SAFIA/PDS1	2
1.3.3	Definitions in SAFIA/IF	3
1.3.4	Additional definitions	3
1.4	Abbreviations	5
1.4.1	Abbreviations in SAFIA/PDS1	5
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	Operations.....	6
1.6.2	Keys	7
2	Outline of Recording and Playback	8
2.1	Described part.....	8
2.2	Recording Device.....	8
2.3	Playback Device	9
2.4	Outline of recording.....	9
2.5	Outline of playback.....	10
3	Device Class Certificate	12
3.1	Device Type Name.....	12
3.2	Acceptable Usage Pass Type Map	12
4	Requirements for protocol implementation	13
5	Usage Pass	14
5.1	Usage Pass Type Map.....	14
5.2	Usage Pass Identifier	14
5.3	Access Condition for Storage Module (AC _s).....	14
5.3.1	Control Count	14
5.3.2	Move Control for Storage Module.....	14
5.4	Cipher Information of Content	14
5.5	Access Condition for Export Module (AC _e)	16
5.6	Content Identifier.....	17

6	Copy Control Descriptor	18
6.1	Syntax of Copy Control Descriptor	18
6.2	private_data_byte	18
6.3	Descriptor_ID_Specific_Field	19
6.3.1	Descriptor_ID_Specific_Field for Audiovisual Content	19
6.3.2	Descriptor_ID_Specific_Field for Audio Content	20
7	Copy control management	21
7.1	Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio in Recording Device	21
7.2	Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio in Playback Device for Copy and Playback.....	22
7.3	Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio in Playback Device for Move.....	24
8	SAFIA AV Stream	25
8.1	Definition of SAFIA AV Stream	25
8.2	Structure of decrypted SAFIA AV Stream	25
8.3	SAFIA AV Stream and Usage Pass	25
8.3.1	Stream recording.....	25
8.3.2	SAFIA AV Stream splitting.....	26
8.4	Encryption and decryption scheme of Allocation Unit	27
8.4.1	Calculation of Initialization Vector.....	27
8.4.2	Encryption of Allocation Unit.....	27
8.4.3	Decryption of Encrypted Allocation Unit	28
9	Directories and files	29
9.1	Restrictions on file system	29
9.2	Location of directories and files.....	29
9.3	iVDR_TVR	29
9.4	PROGxxxx.AVS	29
9.5	Named stream	29
9.5.1	PlaybackInfo.....	29
9.5.2	iVDR_UCInfo.....	29
10	Playback Information	30
10.1	Playback Information General Information (PBI_GI)	30
10.2	Playback Information Type Specific Data.....	30
10.2.1	Playback Information Type Specific Data General Information (PITSD_GI).....	31
10.2.2	Usage Pass Effective Range Entry (PERE)	31
10.2.3	Restriction to Playback Information Type Specific Data	33
11	iVDR Usage Control Information Stream	34
11.1.1	Restriction of location	34

11.1.2 Restriction of the order of Usage Pass Location Field.....	34
Annex A Recording SAFIA Thumbnail	35
A.1 Definitions	35
A.2 Recording Rules	35
A.3 Structure of decrypted SAFIA Thumbnail.....	35
A.4 Encryption of Thumbnail Aligned Unit	35
A.5 Thumbnail Playback Information Type	36
A.6 Thumbnail Playback Information Type Specific Data	36
Annex B Copy Control Management of Prerecorded Content	37

1 General

1.1 Scope

This document describes how Recording and Playback Device, which are a type of Host Device described in SAFIA/PDS1, records and reproduces AV Content specified in iVDR TV Recording Specification. Recording Device converts AV Content into SAFIA AV Stream when the AV Content is required to be protected.

Furthermore, this document describes the format of SAFIA AV Stream and the file structure of SAFIA AV Stream when it is recorded on the Storage Device. Playback Device converts SAFIA AV Stream into AV Content.

In addition, copy control management about SAFIA AV Stream is also described.

1.2 References

- 1) iVDR Consortium,
TV Recording Specification Version 2.31, May, 2009 [iVDR/TVRS]
- 2) National Institute of Standards Technology (NIST), Federal Information Processing Standards Publication 197,
Advanced Encryption Standard (AES), November 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/TVRS

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

- Allocation Unit
- Recording Packet
- TVRS AV Stream
- ALU ID

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 for Export Module (This term was defined as Access Condition for Export Device in version 1.0.)
- Access Condition for Storage Module (This term was defined as Access Condition for Storage Device in version 1.0.)
- Bidirectional Transfer
- Cipher Information of Content
- Content Identifier
- Content Key
- Destination
- Device
- Device Class Certificate
- Device Public Key
- ECDH Shared Key
- Export
- Export Module (This term was defined as Export Device in version 1.0.)
- Host Device
- Host Management Unit (This term was defined as Host in version 1.0.)
- Import
- Import Module (This term was defined as Import Device in version 1.0.)
- Inceptive
- Primal
- Protected
- Open Storage
- Qualified Storage
- Qualified Storage Controller
- SAFIA Content
- SAFIA Security Domain
- Security Domain
- Session Key
- Source
- Storage Device

- Storage Module (This term was defined as Security Management Module in version 1.0.)
- 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

1.3.3 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 Module
- Host Interface Unit
- Storage Interface Module
- Storage Interface Unit

1.3.4 Additional definitions

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

- Aligned Unit
A unit of Cipher Block Chaining mode of the operation for TVRS AV Stream.
- ALU Number
Numbers assigned to ALUs which are related to a Usage Pass when SAFIA AV Stream is created in Recording Device.
- Audio Content
Content mainly including but not limited to audio data. It may contain other kinds of data such as still picture.
- Audiovisual Content
Content mainly including but not limited to audio visual data. It may contain other kinds of data such as markup language, script, meta data.

- AV Content
Audiovisual Content and / or Audio Content.
- Copy
An action of export. A Host Device receives a Usage Pass from a Storage Device through Usage Pass Copy, decrypts the SAFIA AV 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 (CCI) is an information that represents the copy control status of particular content to recording devices.
- Copy-control-not-asserted
A status of CCI that indicates limitations on copying is not asserted.
- Copy-one-generation
A status of CCI that indicates only one generation of copies may be made of such content.
- Encryption Plus Non-Assertion
A status of CCI indicating that numerical copying restrictions are not asserted over the content and such content is protected using a cipher technology.
- 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 AV 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 CCI 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 AV 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 AV Stream. A Playback Device consists of an Export Module of which functions are obliged by the description provided in this document.
- Recording Device
A type of Host Device to import AV Contents from other Security Domain. A Recording Device consists of an Import Module of which functions are obliged by the description provided in this document.
- SAFIA AV Stream
Encrypted TVRS AV Stream together with Copy Control Descriptor.

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:

- ALU Allocation Unit
- AU Aligned Unit
- AGC Automatic Gain Control
- APS Analog Protection System
- bsbf Bit string, left bit first
- CCI Copy Control Information
- E-ALU Encrypted Allocation Unit
- E-AU Encrypted Aligned Unit
- ECB Electronic Code Book
- EPN Encryption Plus Non-Assertion
- IV Initialization Vector
- PERE Usage Pass Effective Range Entry
- RP Recording Packet
- uimbsf Unsigned integer, most significant bit first

1.5 Conventions

The following conventions are used in this document.

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 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

1.6.2 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.

2 Outline of Recording and Playback

2.1 Described part

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

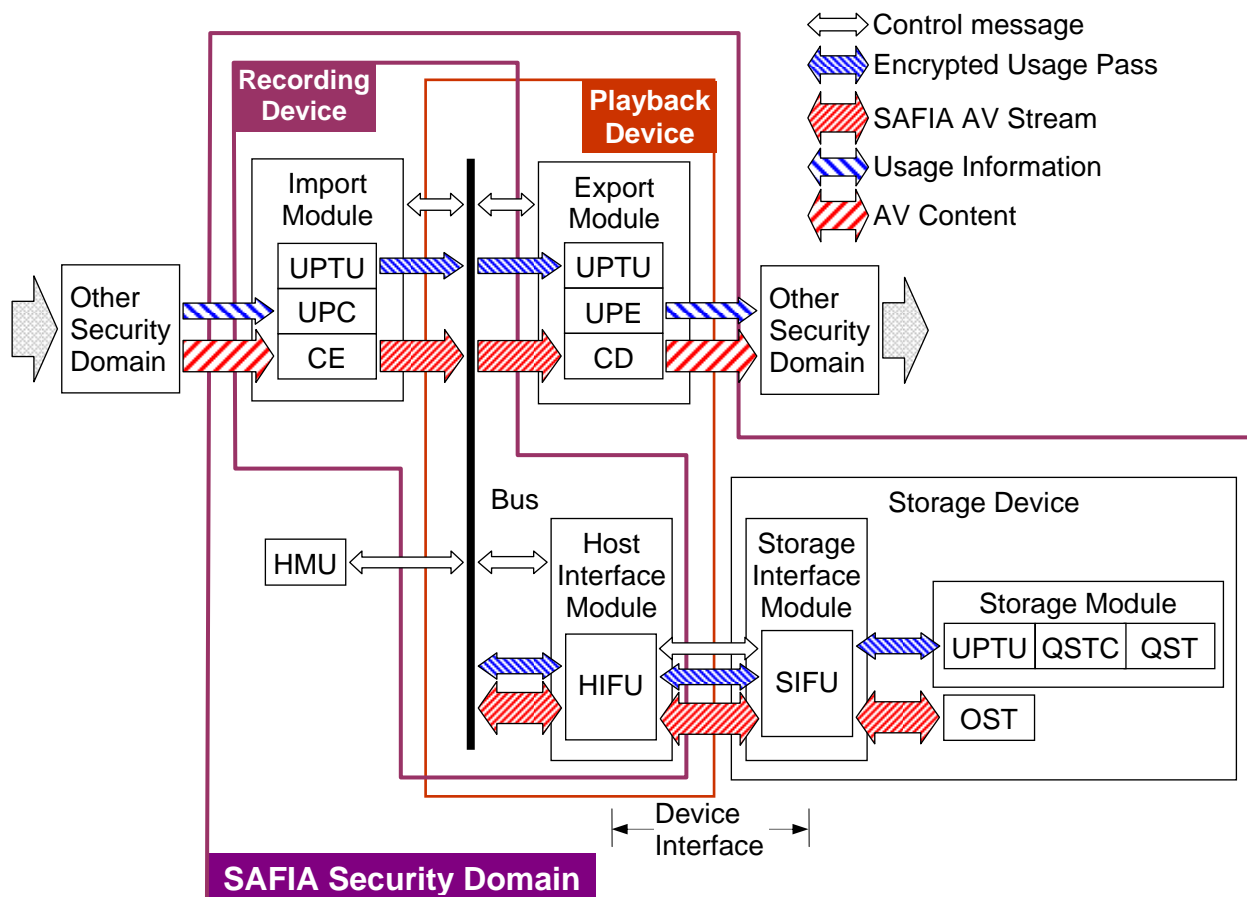


Figure 2.1 Recording Device and Playback Device

2.2 Recording Device

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

- CE

Functions of CE are described in section 2.3 of SAFIA/PDS1. In addition to that, CE has a function to convert AV Content to TVRS AV Stream. Then CE inserts the Copy Control Descriptor, which is sent from UPC, to the TVRS AV Stream and encrypts the Stream. The encrypted result becomes SAFIA AV Stream.
- HIFU

Functions of HIFU are described in SAFIA/IF.
- UPC

Functions of UPC are described in section 2.3 of SAFIA/PDS1. In addition to that, UPC has a

function to create Copy Control Descriptor from Copy Control Information. The created Copy Control Descriptor is sent to CE in Recording Device.

- 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 AV Stream. Function units in Playback Device have following features.

- CD

Functions of CD are described in section 2.3 of SAFIA/PDS1. In addition to that, CD has functions to decrypt SAFIA AV Stream and get Copy Control Descriptor from the decrypted SAFIA AV Stream. After that, CD sends the Copy Control Descriptor to UPE.

- HIFU

Functions of HIFU are described in SAFIA/IF.

- UPE

Functions of UPE are described in section 2.3 of SAFIA/PDS1. In addition to that, UPE determines whether the decrypted SAFIA AV Stream is allowed to be output to outside of SAFIA Security Domain in accordance with the Copy Control Descriptor sent from CD. As the result of the determination, if output of the decrypted SAFIA AV Stream is prohibited, UPE discards the decrypted SAFIA AV Stream.

- 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 Copy / Move / Play as Destination and sends it to UPE.

2.4 Outline of recording

Figure 2.2 shows outline of block diagram for recording. In this figure, SAFIA CCI means Copy Control Descriptor which SAFIA CCI visual or SAFIA CCI audio is included in. To record TVRS AV Stream, a Recording Device may take 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. The structure is described in chapter 5.
- Creates and inserts Copy Control Descriptor to TVRS AV Stream. The details of Copy Control Descriptor are described in chapter 6 and copy control management is described in chapter 7.
- Encrypts TVRS AV Stream with Content Key in the Usage Pass and record the result as SAFIA AV Stream to Open Storage. The details are described in chapter 8.
- Makes Playback Information and record it. Its structure is described in chapter 10.

- Makes iVDR Usage Control information Stream and record it. It is described in chapter 11.
- Records the Usage Pass.

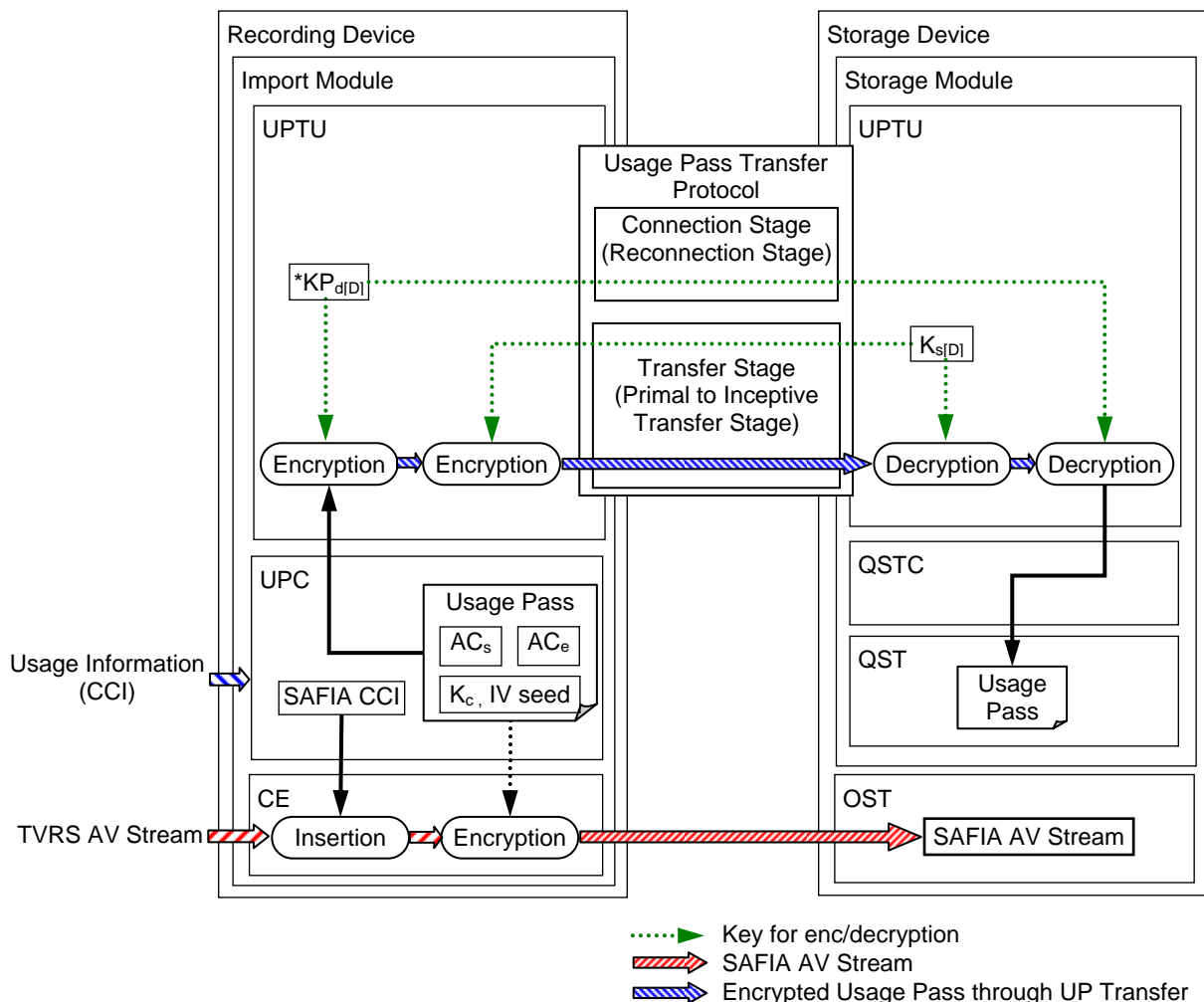


Figure 2.2 Outline of block diagram for recording

2.5 Outline of playback

Figure 2.3 shows outline of block diagram for playback. In this figure, SAFIA CCI means Copy Control Descriptor which SAFIA CCI visual or SAFIA CCI audio is included in. For playback a SAFIA AV Stream, a Playback Device takes 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 10, then gets Usage Pass Identifier related to the playback range in the SAFIA AV Stream.
- Reads iVDR Usage Control information Stream described in chapter 11, then gets location of Usage Pass related to the Usage Pass Identifier described in Playback Information.
- Reads the Usage Pass. The structure is described in chapter 5.

- Reads the SAFIA AV Stream from Open Storage.
- Decrypts the SAFIA AV Stream with Content Key in the Usage Pass. The details are described in chapter 8.
- Outputs AV Content conformed to AC_s and the Copy Control Descriptor. The details of Copy Control Descriptor are described in chapter 6 and copy control management is described in chapter 7.

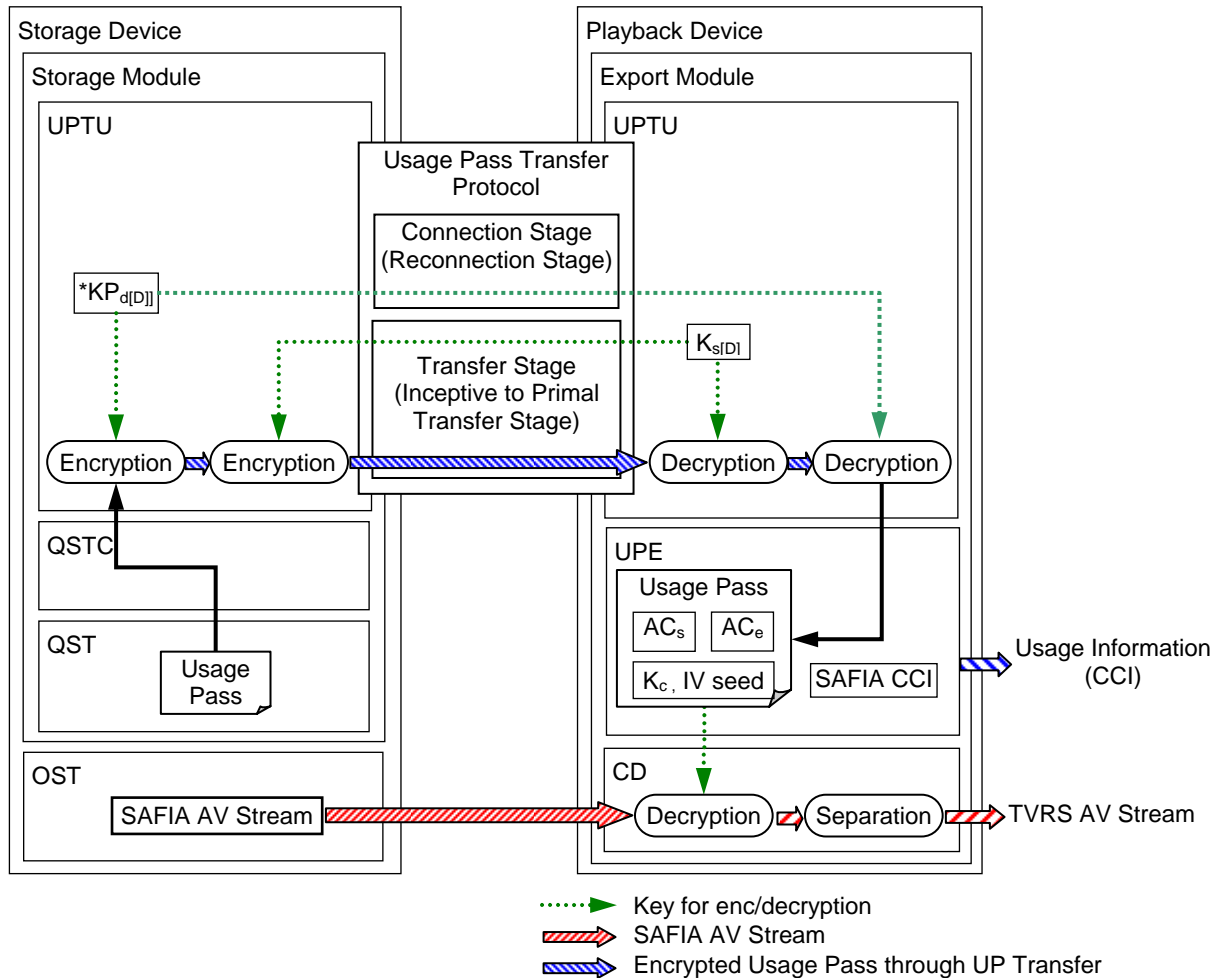


Figure 2.3 Outline of block diagram for playback

3 Device Class Certificate

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

3.1 Device Type Name

This value is “RP1”. Other Device Type Names defined in version 1.0 are deleted.

3.2 Acceptable Usage Pass Type Map

AT1 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 transfer stages of each mode are described in SAFIA/PDS1 and 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			Allowed (Optional)
	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 SAFIA/PDS1. This chapter describes only the information and obligation, which are specific to video recording and playback.

5.1 Usage Pass Type Map

Usage Pass Type is type1. Therefore, Type Map of Usage Pass Format shall be set to 0200 0000 0000 0000h.

5.2 Usage Pass Identifier

Type of Usage Pass Identifier shall be set to 01h. Version shall be set to 1h.

5.3 Access Condition for Storage Module (AC_s)

5.3.1 Control Count

Generation Count and Copy Count are permitted. Therefore, FM of Control Count shall be set to 00b or 01b. The details of copy control management using Control Count are described in chapter 7.

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 not prohibited, these bits shall be set to 0.

5.4 Cipher Information of Content

Table 5.1 shows the structure of CIC of Usage Pass Type 1. 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 1

Bit BP	7	6	5	4	3	2	1	0
0	(MSB) Cipher Scheme							(LSB)
1	(MSB) Content Key (K_c)							(LSB)
...								
16								
17	(MSB) IV Seed							(LSB)
...								
32								
33	VSALN	Reserved						
34	(MSB) Start ALU Number (SALN)							(LSB)
...								
37								
38	VNAUS	(MSB)	Number of AUs in Start ALU (NAUS)				(LSB)	
39								(LSB)
40	VEALN	Reserved						
41	(MSB) End ALU Number (EALN)							(LSB)
...								
44								
45	VNAUE	(MSB)	Number of AUs in End ALU (NAUE)				(LSB)	
46								(LSB)
47								(LSB)
...								
64	Reserved							

- **Cipher Scheme**
This value is 2Eh.
- **Content Key**
This value is a 16-byte random number described in section 5.5 SAFIA/PDS1.
- **IV Seed**
This value indicates the seed of IV to encrypt Contents and a 16-byte random number generated in a Recording Device.
- **VSALN**
This value indicates the validity of Start ALU Number (SALN).
0b: Start ALU Number (SALN) is invalid. In this case, the number of the first ALU is 1.
1b: Start ALU Number (SALN) is valid
- **Start ALU Number**
This value indicates the number of the first ALU managed by this Usage Pass.
- **VNAUS**
This value indicates the validity of Number of AUs in Start ALU (NAUS).
0b: Number of AUs in Start ALU (NAUS) is invalid. In this case, the number of AUs in the first ALU is 512.

1b: Number of AUs in Start ALU (NAUS) is valid

- Number of AUs in Start ALU (NAUS)

This value indicates the number of AUs in the first ALU managed by this Usage Pass.

- VEALN

This value indicates the validity of End ALU Number (EALN).

0b: End ALU Number (EALN) is invalid

1b: End ALU Number (EALN) is valid

- End ALU Number

This value indicates the number of the final ALU managed by this Usage Pass.

- VNAUE

This value indicates the validity of Number of AUs in End ALU (NAUE).

0b: Number of AUs in End ALU (NAUE) is invalid. In this case, the number of AUs in the final ALU is 512.

1b: Number of AUs in End ALU (NAUE) is valid

- Number of AUs in End ALU (NAUE)

This value indicates the number of AUs in the final ALU managed by this Usage Pass.

5.5 Access Condition for Export Module (AC_e)

Table 5.2 shows the structure of AC_e, which Usage Pass Type is 1.

Table 5.2 Structure of AC_e of Usage Pass Type 1

Bit BP	7	6	5	4	3	2	1	0
0	(MSB) Content Type (LSB)							
1	MC	Reserved	OC	DOT	ICT	APS		
2	Control Type				Reserved			
3	Reserved							
...								
127								

- Content Type

This value indicates the Content Type as the followings:

00h: Audiovisual Content

01h: 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 7.3.

01b: Move is allowed only to Storage Device in accordance with the rules described in section 7.3.

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

- OC

This value indicates the Output Control as the followings:

0b: DOT, ICT and APS fields are not valid. ICT and APS described in the Copy Control Descriptor are used for output control.

1b: DOT, ICT and APS fields are valid, and ICT and APS described in these fields have priority over the information described in the Copy Control Descriptor.

If Content Type is 1h, this field shall be set to 0b. Even when OC is 1b, information described in the Copy Control Descriptor is valid except ICT and APS.

- DOT

This value indicates the Digital Only Token as the followings:

0b: Output of decrypted content is allowed for Analog and Digital Outputs.

1b: Output of decrypted content is allowed only for Digital Outputs.

- ICT

This value indicates the Image Constraint Token described in section 6.3.1.

- APS

This value indicates the analog copy protection information described in section 6.3.1.

- Control Type

This value indicates the copy control type as the followings:

0h: Type specific rule is not defined.

1h: ISDB Copy Count. Additional rules for ISDB Copy Count content defined in the Compliance Rules are applied.

2h: Copy Count. Additional rules for Copy Count content defined in the Compliance Rules are applied.

Others: Reserved for future extension, and discard entire SAFIA AV Stream.

5.6 Content Identifier

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

6 Copy Control Descriptor

6.1 Syntax of Copy Control Descriptor

Table 6.1 shows the syntax of Copy_control_descriptor.

Table 6.1 Syntax of Copy_control_descriptor

Syntax	bits	Identifier
Copy_control_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
for (i = 0; i < descriptor_length - 2; i++) {		
private_data_byte	8	bslbf
}		
}		

- descriptor_tag
This field shall be set to 88h.
- descriptor_length
This field indicates the number of bytes of the descriptor immediately following the descriptor_length field. This field shall be set to 04h.
- CA_System_ID
This field shall be set to 0FFFh.

6.2 private_data_byte

The definition of the private_data_byte field of the Copy_control_descriptor is given in Table 6.2.

Table 6.2 Syntax of private_data_byte for Copy_control_descriptor

Syntax	bits	Identifier
private_data_byte {		
Descriptor_ID	1	bslbf
Descriptor_ID_Specific_Field	15	bslbf
}		

- Descriptor_ID
This field indicates the Descriptor_ID as the followings:
 0b: Copy control descriptor for Audio Content
 1b: Copy control descriptor for Audiovisual Content

6.3 Descriptor_ID_Specific_Field

6.3.1 Descriptor_ID_Specific_Field for Audiovisual Content

Table 6.3 shows the Syntax of Descriptor_ID_Specific_Field for Audiovisual Content of which Descriptor_ID is 1.

Table 6.3 Syntax of Descriptor_ID_Specific_Field for Audiovisual Content

Syntax	bits	Identifier
Descriptor_ID_Specific_Field {		
reserved	4	bslbf
EPN	1	bslbf
SAFIA_CCI_visual	2	bslbf
reserved	4	bslbf
Analog_Sunset-Token	1	bslbf
Image_Constraint-Token	1	bslbf
APS	2	bslbf
}		

- reserved
All bits of this field shall be set to 1b.
- EPN
This field indicates the value of the EPN as the followings:
0b: EPN-asserted
1b: EPN-not-asserted
- SAFIA_CCI_visual
This field indicates the copy generation management information as the followings:
00b: Copy-control-not-asserted
01b: No-more-copies
10b: Copy-one-generation
11b: This value is not used
- Analog_Sunset-Token
This field indicates the value of the Analog_Sunset-Token as the followings:
0b: AST-asserted
1b: AST-not-asserted
- Image_Constraint-Token
This field indicates the value of the Image_Constraint-Token as the followings:
0b: High Definition Analog Output in the form of Constrained Image
1b: High Definition Analog Output in High Definition Analog Form
- APS
This field indicates the analog copy protection information as the followings:

00b: APS off

01b: Type1 of APS is on (AGC)

10b: Type2 of APS is on (AGC + 2L Colorstripe)

11b: Type3 of APS is on (AGC + 4L Colorstripe)

6.3.2 Descriptor_ID_Specific_Field for Audio Content

Table 6.4 shows the Syntax of Descriptor_ID_Specific_Field for Audio Content of which Descriptor_ID is 0.

Table 6.4 Syntax of Descriptor_ID_Specific_Field for Audio Content

Syntax	bits	Identifier
Descriptor_ID_Specific_Field {		
reserved	5	bslbf
SAFIA_CCI_audio	2	bslbf
Audio_Type	3	bslbf
Reserved	5	bslbf
}		

- reserved

All bits of this field shall be set to 1b.

- SAFIA_CCI_audio

This field indicates the copy generation management information as the followings:

00b: Copy-control-not-asserted

01b: No-more-copies

10b: Copy-one-generation

11b: This value is not used

- Audio_Type

This field shall be set to 000b

7 Copy control management

7.1 Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio in Recording Device

Recording Device converts AV Content to SAFIA AV Stream. If AV Content is Audio Content, Content type of AC_e shall be 01h and Descriptor_ID shall be 0b. If AV Content is Audiovisual Content, Content type of AC_e shall be 00h and Descriptor_ID shall be 1b.

A part, which is related to a Usage Pass, of SAFIA AV Stream may be composed of multiple parts. Each part includes SAFIA_CCI_visual or SAFIA_CCI_audio. In this case, Control Count shall be determined in accordance with the most restrictive SAFIA_CCI_visual or SAFIA_CCI_audio. Table 7.1 and Table 7.2 show the permitted combinations of Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio respectively when a Recording Device transfers a Usage Pass to a Storage Device.

When FM is 00b (Generation Count) and COUNT is 1h (One Generation), the value of COUNT is changed to 0h (No More Copy) in a Storage Module. Therefore, if the most restricted CCI is 01b (No-more copies) or 10b (Copy-one-generation), COUNT is set to 1h. And, the CCI of 10b is allowable in the case of non-cognizant recording, which is the case that valid Copy Control Descriptor is inserted in the imported AV Content and a Recording Device records this AV Content without updating the descriptor.

FM of 01b (Copy Count) is allowed when the Control Type is “ISDB Copy Count”. And, in this case, SAFIA_CCI_visual or SAFIA_CCI_audio shall be set to 01b (No-more-copies).

Table 7.1 Relationship between Control Count and SAFIA_CCI_visual

AC _s Control Count			SAFIA_CCI_visual						
			00b (Copy-control- not-asserted)		01b (No-more- copies)	10b (Copy-one- generation)	11b (Not used)		
			EPN-not- asserted	EPN- asserted					
FM	00b	COUNT	0h (No more copy)	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	
			1h (One generation)	Allowed	Allowed	Allowed	Allowed	Prohibited	
			2h (Two generation)	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	
			Fh (Not asserted)	Allowed	Allowed	Prohibited	Prohibited	Prohibited	
			Others	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	
	01b	COUNT	0h (No more copy)	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	
			1h, ..., 9h (Permitted times = 1, ..., 9)	Allowed	Allowed	Allowed	Prohibited	Prohibited	
			Others	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited	
			10b	Don't care	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
			11b	Don't care	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited

Table 7.2 Relationship between Control Count and SAFIA_CCI_audio

AC _s Control Count				SAFIA_CCI_audio			
				00b (Copy-control- not-asserted)	01b (No-more- copies)	10b (Copy-one- generation)	11b (Not used)
FM	00b	COUNT	0h (No more copy)	Prohibited	Prohibited	Prohibited	Prohibited
			1h (One generation)	Allowed	Allowed	Allowed	Prohibited
			2h (Two generation)	Prohibited	Prohibited	Prohibited	Prohibited
			Fh (Not asserted)	Allowed	Prohibited	Prohibited	Prohibited
			Others	Prohibited	Prohibited	Prohibited	Prohibited
	01b		0h (No more copy)	Prohibited	Prohibited	Prohibited	Prohibited
			1h, ..., 9h (Permitted times = 1, ..., 9)	Allowed	Allowed	Prohibited	Prohibited
			Others	Prohibited	Prohibited	Prohibited	Prohibited
	10b		Don't care	Prohibited	Prohibited	Prohibited	Prohibited
	11b		Don't care	Prohibited	Prohibited	Prohibited	Prohibited

7.2 Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio in Playback Device for Copy and Playback

Playback Device shall export decrypted SAFIA AV Stream to comply with both Table 7.3 and Table 7.4.

Table 7.3 Rule of Content Type and Descriptor_ID in Copy Control Descriptor

		Descriptor_ID	
		0b (Audio)	1b (Audiovisual)
Content Type in AC _e	00h (Audiovisual)	Copy Control Descriptor is invalid	Available for processing
	01h (Audio)	Available for processing	Copy Control Descriptor is invalid
	Others	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream

Table 7.4 Rule of Control Count and SAFIA_CCI_visual or SAIFA_CCI_audio in Playback Device for Copy and Playback

AC _s Control Count			SAFIA_CCI_visual or SAFIA_CCI_audio				
			00b (Copy-control-not-asserted)	01b (No-more-copies)	10b (Copy-one-generation)	11b (Not used)	
FM	00b	COUNT	0h (No more copy)	Available for processing ^{*1}	Available for processing	*2	*2
			1h (One generation)	Available for processing ^{*1}	*2	Available for processing ^{*4}	*2
			2h (Two generation)	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}
			Fh (Not asserted)	Available for Processing	*2	*2	*2
			Others	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}
	01b		0h (No more copy)	Available for processing ^{*1}	Available for processing	*2	*2
			1h, ..., Eh	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}	Discard entire SAFIA AV Stream ^{*3}
			Fh (Not asserted)	Available for Processing	*2	*2	*2
	10b		0h, ..., Eh	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream
			Fh (Not asserted)	Available for Processing	*2	*2	*2
	11b		Don't care	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream

*1: A stream can be treated as copy control status of "Copy-control-not-asserted".

*2: A stream shall be treated in accordance with the status of Control Count.

*3: This status does not exist in normal case. A stream may be treated as copy control status of "No-more-copies".

*4: See additional rules for Copy Count content defined in the Compliance Rules.

7.3 Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio in Playback Device for Move

Playback Device shall export SAFIA AV Stream to comply with both Table 7.3 and Table 7.5.

Table 7.5 Rule of Control Count and SAFIA_CCI_visual or SAIFA_CCI_audio in Playback Device for Move

AC _s Control Count				SAFIA_CCI_visual or SAFIA_CCI_audio			
				00b (Copy-control-not-asserted)	01b (No-more-copies)	10b (Copy-one-generation)	11b (Not used)
FM	00b	COUNT	0h (No more copy)	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream
			1h (One generation)	Available for processing	Available for processing	Available for processing	*1
			2h (Two generation)	Available for processing	*1	Available for processing	*1
			Fh (Not asserted)	Available for processing	*1	*1	*1
			Others	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream
	01b		0h (No more copy)	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream
			Others	Available for processing	Available for processing	Available for processing	*1
	10b		Don't care	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream
	11b		Don't care	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream	Discard entire SAFIA AV Stream

*1: A stream shall be treated in accordance with the status of Control Count.

8 SAFIA AV Stream

8.1 Definition of SAFIA AV Stream

SAFIA AV Stream is a SAFIA Content which complies following:

- The SAFIA AV Stream shall be the encrypted TVRS AV Stream.
- The PMT of the TVRS AV Stream shall contain the Copy_control_descriptor in the PMT 1st loop.

8.2 Structure of decrypted SAFIA AV Stream

A decrypted SAFIA AV Stream consists of Allocation Units (ALUs). An ALU consists of 512 Aligned Units (AUs) as shown in Figure 8.1. The size of each ALU shall be 1.5M-byte. An AU consists of 16 Recording Packets (RPs) as shown in Figure 8.1. An RP is defined as 4-byte RP header and 188-byte Transport Stream (TS) packet. ALU and RP are specified in iVDR/TVRS. The size of each AU shall be 3072-byte other than that of the last AU of the Stream and the first AU of the split Stream described in 8.3.2. The size (3072-byte) corresponds to 6 sectors if physical sector size is 512-byte.

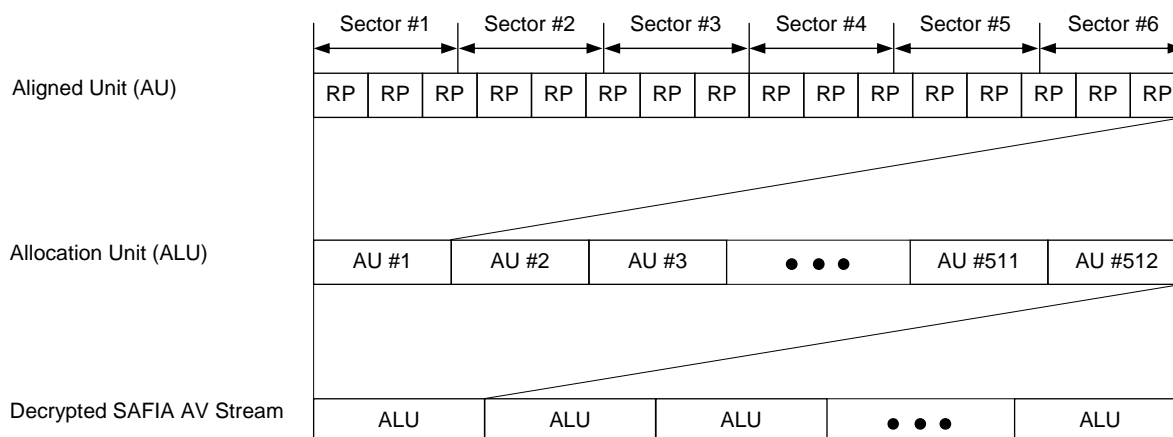


Figure 8.1 Relation among AU, ALU and decrypted SAFIA AV Stream

8.3 SAFIA AV Stream and Usage Pass

8.3.1 Stream recording

A SAFIA AV Stream relates to one or more Usage Passes. A Usage Pass relates to a continuous region in the SAFIA AV Stream. The continuous region consists of plural Encrypted ALUs (E-ALUs). The relations between E-ALU and Usage Pass are described in Usage Pass Effective Range Entry as shown in section 10.2.2. Figure 8.2 shows an example of relations between E-ALUs and Usage Passes. E-ALUs related to a Usage Pass is numbered in ascending order from value "1" as ALU Number and guaranteed its uniqueness in E-ALUs related to the Usage Pass as shown in Figure 8.2. Maximum number of E-ALU related to a Usage Pass shall be FFFFFFFFh.

- First E-ALUs part

In this case, all E-ALUs are left as it is. The Start ALU Number (SALN), Number of AUs in Start ALU (NAUS), End ALU Number (EALN) and Number of AUs in End ALU (NAUE) in the CIC of the Usage Pass #m' are set to 1, 512, k and p respectively.

- Second E-ALUs part

In this case, all E-ALUs are left as it is, which means that ALU Number reassignment is not logically executed. However, the Start ALU Number (SALN), Number of AUs in End ALU (NAUE), End ALU Number (EALN) and Number of AUs in End ALU (NAUE) in the CIC of the Usage Pass #m" are set to k, 512 - p, n and 512 respectively.

8.4 Encryption and decryption scheme of Allocation Unit

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

8.4.1 Calculation of Initialization Vector

The IV used in encryption of every AU is 16-byte different value for each ALU. AES block cipher algorithm with 128-bit key is used for calculation of IV as shown in Figure 8.4. AES is specified in FIPS197. Its calculation is represented by the following equation

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

The iv_seed is a 16-byte IV Seed included in the Usage Pass related to this ALU and it is used as AES key. The alu_number is 16-byte value of which most significant 12-byte is 00000000 00000000 00000000h and the rest 4-byte is ALU Number. Therefore IVs of different AUs included in different ALUs are different value in spite of corresponding to same Usage Pass and IVs of different AUs in same ALU are same value.

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

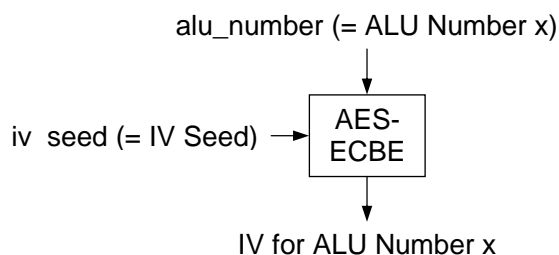


Figure 8.4 Calculation of Initialization Vector

8.4.2 Encryption of Allocation Unit

AES in CBC mode of operation shall be used for encryption of each AU. Its calculation is represented by the following equation

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

Here, the K_c is a 16-byte Content Key used as 16-byte AES key, IV is a 16-byte Initialization Vector, AU is 16 RPs data to be encrypted, and AES-CBCE returns 3072-byte E-AU. K_c is included in the Usage Pass related to this E-AU. 512 AUs included in an ALU shall be encrypted by using the above function AES-CBCE() similarly. Figure 8.5 shows AES based CBC encryption of ALU. The same value shall be used about IV of 512 AUs included in the same ALU. The value of IV corresponding to each AU is specified in section 8.4.1.

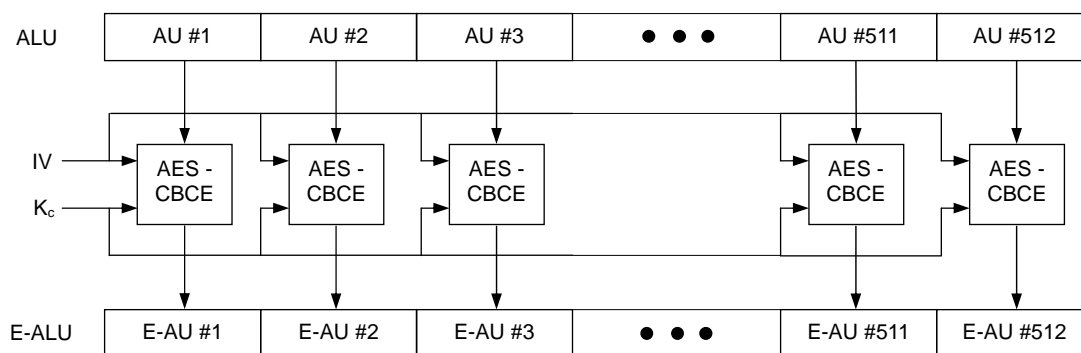


Figure 8.5 Encryption of Allocation Unit

8.4.3 Decryption of Encrypted Allocation Unit

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

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

Here, the K_c is a 16-byte Content Key used as 16-byte AES key, IV is a 16-byte Initialization Vector, E-AU is encrypted 16 RPs data to be decrypted, and AES-CBCD returns 3072-byte decrypted E-AU. 512 E-AUs included in an E-ALU shall be decrypted by using the above function AES-CBCD() similarly. Figure 8.6 shows AES based CBC decryption of E-ALU. IV used at the beginning of each CBC decryption chain shall be the same IV used at the time of encryption of AU.

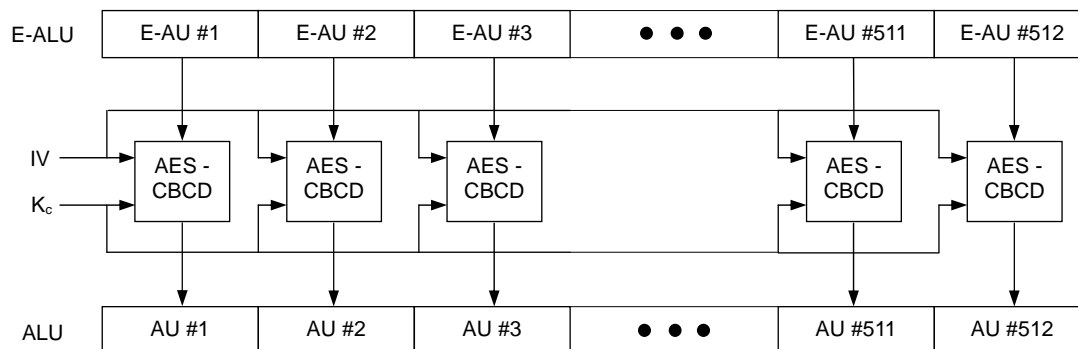


Figure 8.6 Decryption of Encrypted Allocation Unit

9 Directories and files

9.1 Restrictions on file system

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

9.2 Location of directories and files

All directories and files shall be located in accordance with iVDR/TVRS. Figure 9.1 shows the location of directories and files. A directory and file names are changed from version 1.0.

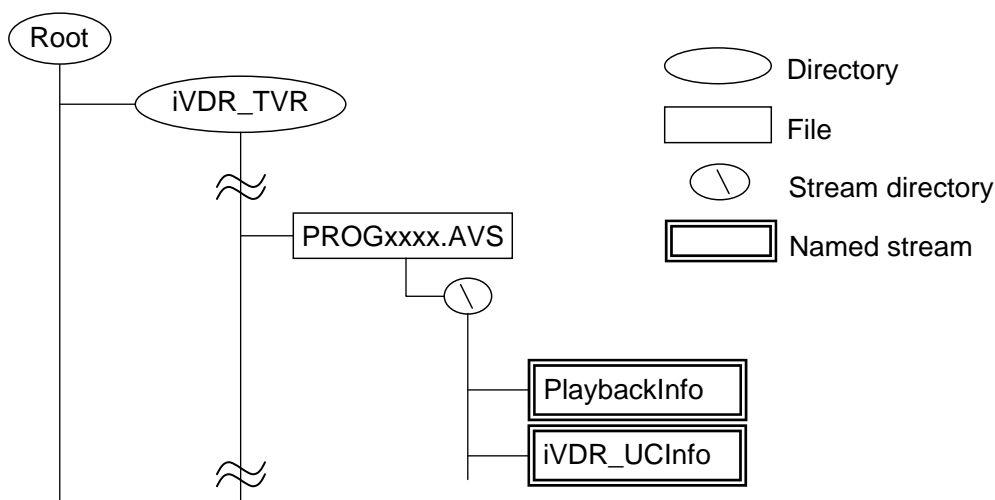


Figure 9.1 Location of directories and files

9.3 iVDR_TVR

It is specified in iVDR/TVRS.

9.4 PROGxxxx.AVS

It is specified in iVDR/TVRS. SAFIA AV Stream described in chapter 8 is stored in it.

9.5 Named stream

Named Streams described in the following sections shall be attributed to PROGxxxx.AVS described in section 9.5.2.

9.5.1 PlaybackInfo

Playback Information described in chapter 10 is stored.

9.5.2 iVDR_UCInfo

iVDR Usage Control Information Stream described in chapter 11 is stored. It shall have all Usage Pass Identifiers related to the stream.

10 Playback Information

Playback Information is specified in iVDR/TVRS. This chapter describes the structure of Playback Information peculiar to SAFIA. This named stream file is prepared to specify relationship between SAFIA AV Stream and Usage Passes. Playback Information consists of Playback Information General Information and Playback Information Type Specific Data as shown in Figure 10.1.

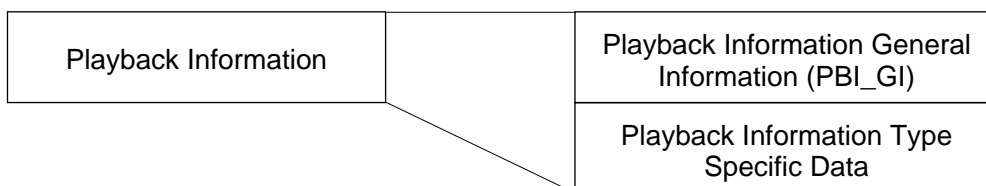


Figure 10.1 Structure of Playback Information

10.1 Playback Information General Information (PBI_GI)

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

10.2 Playback Information Type Specific Data

Figure 10.2 shows the structure of Playback Information Type Specific Data.

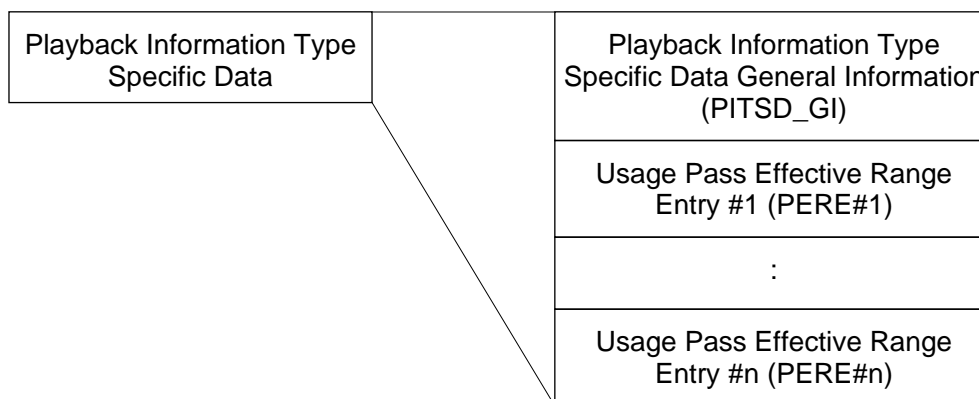


Figure 10.2 Structure of Playback Information Type Specific Data

10.2.1 Playback Information Type Specific Data General Information (PITSD_GI)

Table 10.1 shows the structure of PITSD_GI.

Table 10.1 Structure of PITSD_GI

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

10.2.1.1 Number of Usage Pass Effective Range Entries (PERE_N)

The number of Usage Pass Effective Range Entries after PITSD_GI field is stored.

10.2.2 Usage Pass Effective Range Entry (PERE)

Table 10.2 shows the structure of PERE.

Table 10.2 Structure of PERE

BP	Length	Field name	Contents
0	1	Reserved for Flag	bslbf
1	1	Length of this Entry	uimsbf
2	4	Usage Pass Effective Range Start Position	uimsbf
6	4	Usage Pass Effective Range End Position	uimsbf
10	32	Usage Pass Identifier	uimsbf

10.2.2.1 Reserved for Flag

This field is reserved and shall be filled with zero.

10.2.2.2 Length of this Entry

The length of PERE after this field shall be set to this field. The length is 28h and may be changed in the future.

10.2.2.3 Usage Pass Effective Range Start Position

ALU ID of Usage Pass Effective Range Start Position shall be set to this field. Namely, the ALU ID of the first E-ALU among continuous E-ALUs related to a Usage Pass shall be set. ALU ID shall be assigned to E-ALU in ascending order and guaranteed its uniqueness in SAFIA AV Stream as shown in Figure 10.3.

10.2.2.4 Usage Pass Effective Range End Position

ALU ID of Usage Pass Effective Range End Position shall be set to this field. Namely, the ALU ID of the last E-ALU among continuous E-ALUs related to a Usage Pass shall be set.

10.2.2.5 Usage Pass Identifier

Usage Pass Identifier of Usage Pass related to E-ALUs ranging from Usage Pass Effective Range Start Position to Usage Pass Effective Range End Position shall be stored. 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 SAFIA/FS.

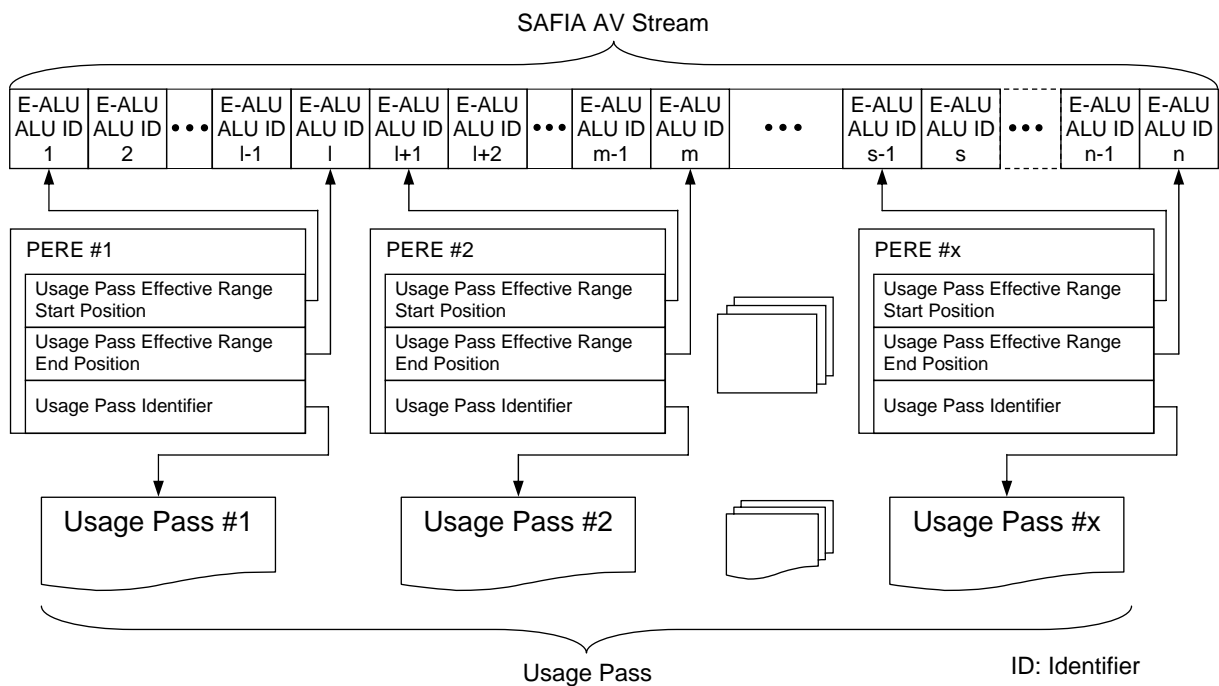


Figure 10.3 Definition of Usage Pass Effective Range Entry

10.2.3 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 Position. It means that the value of ALU ID set in the field of Usage Pass Effective Range Start Position in PERE #i (i = 2, ..., x in Figure 10.3) shall be greater than the value of ALU ID described in the field of Usage Pass Effective Range End Position in PERE #i-1.

As for the value of ALU ID set in the field of Usage Pass Effective Range End Position in PERE #j (i = 1, ..., x in Figure 10.3), it shall be greater than or equal to the value of ALU ID described in the field of Usage Pass Effective Range Start Position in the same PERE (PERE #j).

It is also noted that the value of Usage Pass Effective Range End Position (= q) in PERE #k and the value of Usage Pass Effective Range Start Position (= r) in PERE #(k+1) are not successive if ALUs which ALU IDs from q + 1 to r – 1 are not encrypted and therefore the ALUs are not related to a Usage Pass. An example of this case is shown in Figure 10.4.

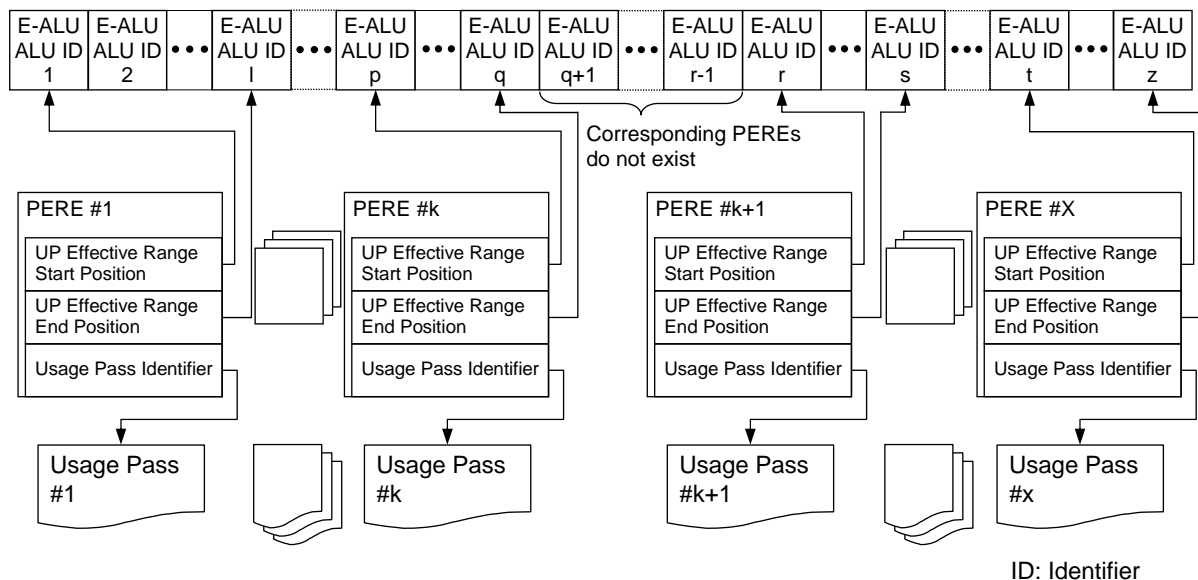


Figure 10.4 Definition of Usage Pass Effective Range Entry

11 iVDR Usage Control Information Stream

iVDR Usage Control Information Stream for SAFIA is described in SAFIA/FS. Figure 11.1 shows the structure of iVDR Usage Control Information Stream Type 1.

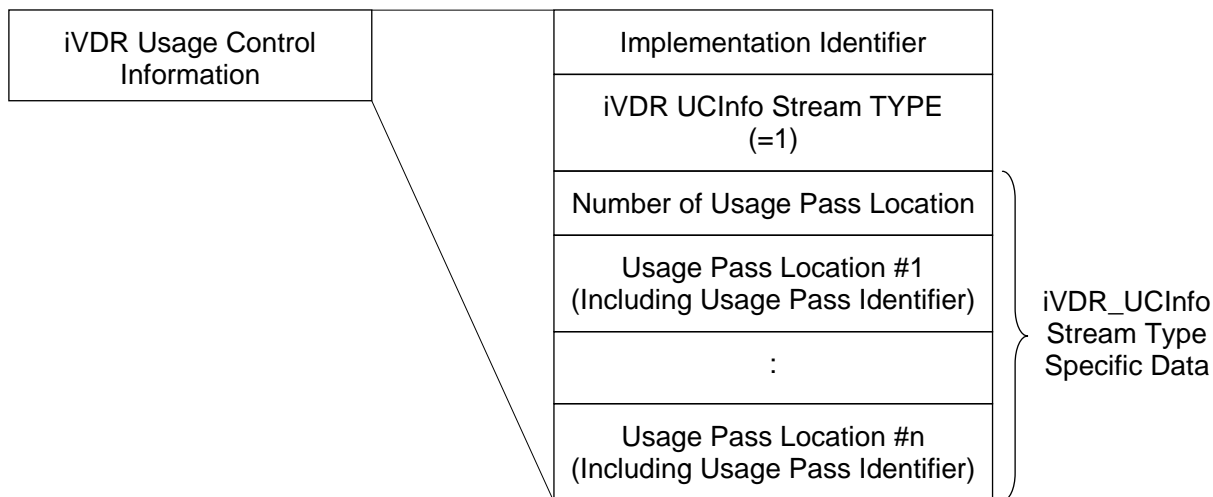


Figure 11.1 The structure of iVDR Usage Control Information Stream Type 1

11.1.1 Restriction of location

The location of iVDR Usage Control Information Stream shall belong to PROGxxxx.AVS.

11.1.2 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.)

Annex A Recording SAFIA Thumbnail

A.1 Definitions

- E-ALU Chunk
E-ALU Chunk consists of continuous E-ALUs related to a Usage Pass.
- SAFIA Thumbnail
SAFIA Thumbnail is the encrypted picture data converted from part of E-ALU Chunks.

A.2 Recording Rules

SAFIA thumbnail may be recorded in the Open Storage when the following conditions are satisfied.

- 1) When the SAFIA thumbnail converted from the part of E-ALU Chunks, it shall have been encrypted with the K_c in the Usage Pass related to the first E-ALU of E-ALU Chunks.
- 2) Encryption algorithm to obtain SAFIA Thumbnail shall be AES and the key length is 16-byte, where the mode of encryption shall be CBC. The details are described in section of A.3.

A.3 Structure of decrypted SAFIA Thumbnail

A decrypted SAFIA Thumbnail consists of Thumbnail Aligned Units (TAUs) as shown in Figure A.1. The size of each TAU shall be 3072-byte other than that of the last TAU (TAU #N in Figure A.1).

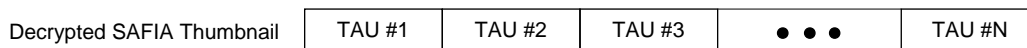


Figure A.1 Relation between TAU and decrypted SAFIA Thumbnail

If the length of the decrypted SAFIA Thumbnail is not the multiples of 16-byte, zeros less than 16-byte are padded at the end such as the length to be multiples of 16-byte.

A.4 Encryption of Thumbnail Aligned Unit

AES in CBC mode of operation shall be used for the encryption of each TAU. Its calculation is represented by the following equation

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

The K_c in the above equation is a 16-byte Content Key described in section of A.2 and IV is a 16-byte Initialization Vector, where IV is calculated as the following equation.

$$IV = \text{AES-ECBE}(\text{iv_seed}, 00000000\ 00000000\ 00000000\ 00000000\text{h}).$$

The *iv_seed* in the above equation is the value specified in the Usage Pass which includes the Content Key K_c .

Each TAU shall be encrypted by using the above function AES-CBCE() similarly. Figure A.2 shows AES based CBC encryption of TAU. The same IV value shall be applied for the encryption of all TAU.

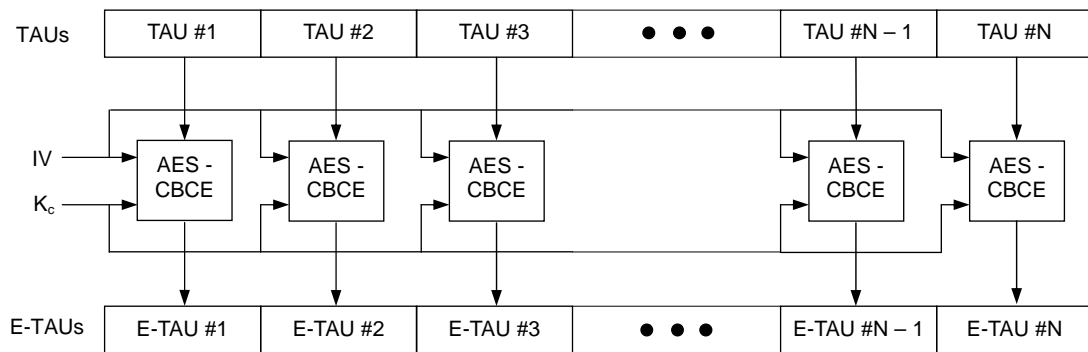


Figure A.2 Encryption of Thumbnail Aligned Units

A.5 Thumbnail Playback Information Type

Thumbnail Playback Information Type specified in iVDR/TVRS shall be set to 01h.

A.6 Thumbnail Playback Information Type Specific Data

Thumbnail Playback Information Type Specific Data specified in iVDR/TVRS shall be set to the Usage Pass Identifier of the Usage Pass which manages the E-ALUs, from which this thumbnail is created.

Annex B Copy Control Management of Prerecorded Content

If AV Content is Audio Content, Content type of AC_e shall be 01h and Descriptor_ID shall be 0b.
 If AV Content is Audiovisual Content, Content type of AC_e shall be 00h and Descriptor_ID shall be 1b.

A part, which is related to a Usage Pass, of SAFIA AV Stream may be composed of multiple parts. Each part includes SAFIA_CCI_visual or SAFIA_CCI_audio. In this case, Control Count shall be determined in accordance with the most restrictive SAFIA_CCI_visual or SAFIA_CCI_audio. Table 7.1 and

Table 7.2 show the permitted combinations of Control Count and SAFIA_CCI_visual or SAFIA_CCI_audio respectively.

Table B.1 Relationship between Control Count and SAFIA_CCI_visual

AC _s Control Count				SAFIA_CCI_visual				
				00b (Copy-control-not-asserted)		01b (No-more-copies)	10b (Copy-one-generation)	11b (Not used)
				EPN-not-asserted	EPN-asserted			
FM	00b	COUNT	0h	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
			1h (0h: No more copy in Sotrage Device)	Allowed	Allowed	Allowed	Prohibited	Prohibited
			2h (1h: One generation in Sotrage Device)	Prohibited	Prohibited	Prohibited	Allowed	Prohibited
			Fh (Not asserted)	Allowed	Allowed	Prohibited	Prohibited	Prohibited
			Others	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
	01b	COUNT	0h (No more copy)	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
			1h, ..., Eh (Permitted times = 1, ..., 14)	Allowed	Allowed	Allowed	Prohibited	Prohibited
			Fh	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
			10b	Don't care	Prohibited	Prohibited	Prohibited	Prohibited
			11b	Don't care	Prohibited	Prohibited	Prohibited	Prohibited

Table B.2 Relationship between Control Count and SAFIA_CCI_audio

AC _s Control Count			SAFIA_CCI_audio				
			00b (Copy-control-not-asserted)	01b (No-more-copies)	10b (Copy-one-generation)	11b (Not used)	
FM	00b	COUNT	0h	Prohibited	Prohibited	Prohibited	Prohibited
			1h (0h: No more copy in Storage Device)	Allowed	Allowed	Prohibited	Prohibited
			2h (1h: One generation in Storage Device)	Prohibited	Prohibited	Allowed	Prohibited
			Fh (Not asserted)	Allowed	Prohibited	Prohibited	Prohibited
			Others	Prohibited	Prohibited	Prohibited	Prohibited
	01b		0h (No more copy)	Prohibited	Prohibited	Prohibited	Prohibited
			1h, ..., Eh (Permitted times = 1, ..., 14)	Allowed	Allowed	Prohibited	Prohibited
			Fh	Prohibited	Prohibited	Prohibited	Prohibited
			10b	Don't care	Prohibited	Prohibited	Prohibited
			11b	Don't care	Prohibited	Prohibited	Prohibited