

Security Architecture for Intelligent Attachment Device Specifications

– Protocol and Data Structure Volume 1 –

Version 1.21

October 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	2
1.3.1	Definitions in X509	2
1.3.2	Additional definitions	3
1.4	Abbreviations	9
1.5	Conventions	10
1.5.1	Keywords	10
1.5.2	Numerical values	11
1.5.3	Bit and byte ordering	11
1.6	Notations	11
1.6.1	Keys and data	11
1.6.2	Operations	12
2	SAFIA Security Domain descriptions	13
2.1	Information in SAFIA Security Domain	13
2.1.1	Usage Pass	13
2.1.2	SAFIA Content	13
2.1.3	Controlled content	13
2.1.4	Non-controlled content	13
2.2	Supposed total system model	13
2.3	Functional units	14
2.4	Functional modules	15
2.4.1	Storage Module	15
2.4.2	Export Module	15
2.4.3	Import Module	16
2.4.4	Transmit Module	16
2.4.5	Storage Interface Module	16
2.4.6	Host Interface Module	16
2.5	Constitution element	16
2.5.1	Storage Device	16
2.5.2	Host Device	17
3	SAFIA security design policy	17
3.1	Tamper Resistant Module	17
3.2	Usage Pass Transfer Protocol	17
3.3	Revocation	17
3.4	Usage Pass Type	17

4	Cryptographic functions	18
4.1	Hash function	18
4.2	Symmetric cryptography	18
4.3	Asymmetric cryptography	18
4.3.1	Key agreement algorithm	18
4.3.2	Digital signature algorithm	18
4.4	Random / pseudorandom number generator	18
5	Common cryptographic key	19
5.1	Device Proper Keys	19
5.1.1	Device Class Private / Public Key	19
5.1.2	Device Private / Public Key	19
5.2	Root Public Key	19
5.3	Challenge / Session Keys	19
5.4	ECDH Shared Key	19
5.5	Content Key	19
6	Outline of protocol	20
6.1	Unidirectional Transfer (UT) mode	20
6.1.1	Basic steps	20
6.1.1.1	Connection Stage	20
6.1.1.2	Transfer Stage	22
6.1.2	Additional steps	23
6.1.2.1	Reconnection Stage	23
6.1.2.2	Recovery Stage	23
6.1.2.3	Usage Pass Inquiry Stage	24
6.2	Bidirectional Transfer (BT) mode	24
6.2.1	Basic steps	24
6.2.1.1	Connection Stage	25
6.2.1.2	Primal to Inceptive Transfer Stage	26
6.2.1.3	Inceptive to Primal Transfer Stage	27
6.2.2	Additional steps	27
6.2.2.1	Reconnection Stage	28
6.2.2.2	Primal to Inceptive Recovery Stage	28
6.2.2.3	Inceptive to Primal Recovery Stage	29
6.2.2.4	Usage Pass Inquiry Stage	30
7	Usage Pass	31
7.1	Usage Pass Format	31
7.1.1	Name	32
7.1.2	Version	32
7.1.3	Type Map	32
7.2	Usage Pass Identifier	32

7.2.1	Version	33
7.2.2	Type	33
7.2.3	Adapter Number	33
7.2.4	Number	33
7.3	Access Condition for Storage Module (AC _s)	33
7.3.1	Control Count	34
7.3.1.1	Generation Count	34
7.3.1.2	Copy Count.....	37
7.3.1.3	Play Count.....	40
7.3.2	Move Control for Storage Module.....	43
7.3.2.1	MU.....	43
7.3.2.2	MB.....	43
7.4	Cipher Information of Content	43
7.4.1	Cipher Scheme.....	44
7.4.2	Content Key.....	44
7.4.3	Type Specific Cipher Info	44
7.5	Access Condition for Export Device (AC _e)	44
7.6	Content Identifier.....	44
7.6.1	Version	44
7.6.2	Type	44
7.6.3	Adapter Number	45
7.6.4	Number	45
7.7	Copyright Information.....	45
8	Device Class Certificate and Revoked Device Class List	46
8.1	Device Class Certificate	46
8.2	Format of Device Class Certificate.....	46
8.2.1	version.....	47
8.2.2	serialNumber	47
8.2.3	signature	47
8.2.4	issuer.....	47
8.2.4.1	Country Name	48
8.2.4.2	Organization Name.....	48
8.2.5	validity	48
8.2.6	subject.....	49
8.2.6.1	Country Name	51
8.2.6.2	Organization Name.....	51
8.2.6.3	Device Name	51
8.2.6.4	Device Type Name	51
8.2.6.5	Acceptable Usage Pass Type Map.....	51
8.2.7	subjectPublicKeyInfo	52

8.2.8	signatureAlgorithm	52
8.2.9	signatureValue	52
8.3	Revoked Device Class List	52
8.3.1	Length of Revoked Device Class List.....	52
8.4	Format of Revoked Device Class List	52
8.4.1	version.....	53
8.4.2	signature	53
8.4.3	issuer.....	53
8.4.4	thisUpdate	54
8.4.5	revokedCertificates.....	54
8.4.6	signatureAlgorithm	55
8.4.7	signatureValue	55
9	Log management.....	56
9.1	Unidirectional Transfer (UT) mode	56
9.1.1	Transaction Log.....	56
9.1.1.1	Usage Pass Identifier.....	56
9.1.1.2	Type Map.....	56
9.1.1.3	Inceptive Device Public Key	57
9.1.1.4	Inceptive Session Key	57
9.1.1.5	Session Status.....	57
9.1.1.6	Original Access Condition.....	57
9.1.1.7	Usage Pass Location.....	58
9.1.2	Transaction Status	58
9.1.3	Recovery condition.....	58
9.2	Bidirectional Transfer (BT) mode	59
9.2.1	Connection Log	59
9.2.1.1	Type Map.....	60
9.2.1.2	Partner Device Public Key	60
9.2.1.3	Self Session Key	60
9.2.1.4	Partner Session Key	60
9.2.1.5	Partner Message Version	60
9.2.1.6	Primal Device Specifier.....	60
9.2.2	Transaction Log.....	60
9.2.2.1	Usage Pass Identifier.....	61
9.2.2.2	Transfer Type	61
9.2.2.3	Original Access Condition.....	61
9.2.2.4	Original Usage Pass.....	61
9.2.2.5	Usage Pass Location.....	61
9.2.3	Recovery-Allowed Primal Device Indicator.....	61
9.2.4	Recovery Permission Indicator.....	62
9.2.5	Transaction Status	62

9.2.6 Recovery condition.....	62
Annex A ECDH Algorithm.....	64
A.1 Encryption.....	64
A.2 Decryption.....	64
Annex B ECDSA Algorithm	65
B.1 Digital signature creation.....	65
B.2 Digital signature verification	65

1 General

1.1 Scope

“Security Architecture for Intelligent Attachment Device Specifications” determines the technology to protect content by encrypting and Usage Pass including the Content Key used to decrypt the content. User authentication, charging system to consumers and so forth are excluded because they are not directly related to these specifications.

This document describes the Security Domain where content is protected (SAFIA Security Domain), the requirements for the Devices located in the domain, the protocols to transfer a Usage Pass securely, Usage Pass, Device Class Certificate and Revoked Device Class List.

1.2 References

- 1) ANSI X9.31,
Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry, 1998 [ANSI/X9.31]
- 2) ANSI X9.62,
Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998 [ANSI/X9.62]
- 3) ANSI X9.63,
Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, 2001 [ANSI/X9.63]
- 4) Network Working Group, Request for Comment 3279,
Category: Standard Track, W. Polk (NIST), R. Housley (RSA Laboratories), L. Bassham (NIST), Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002 [RFC3279]
- 5) Network Working Group, Request for Comment 3280,
Category: Standard Track: R. Housley (RSA Laboratories), W. Polk (NIST) W. Ford (VeriSign), D. Solo (Citigroup), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002 [RFC3280]
- 6) IEEE 1363-2000,
Standard Specifications for Public-Key Cryptography [IEEE/P1363]
- 7) Internet-Draft, R. Housley (Vigil Security),
Additional Algorithms and Identifiers for use of Elliptic Curve Cryptography with PKIX (Explicit Identification of One-Way Hash Functions) <draft-housley-pkix-ecc-pkalg-ecdsa-00.txt>, January 2005 [ID/ECDSA-00]
- 8) ISO/IEC 646,
Information technology, ISO 7-bit coded character set for information interchange, 1991 [ISO/IEC646]
- 9) ISO 3166,

- Codes for the representation of name of countries and their subdivisions, 1997 [ISO3166]
- 10) ITU-T Recommendation X.509 (1997 E),
Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 [X509]
 - 11) ITU-T Recommendation X.680,
Data Networks and Open System Communications OSI Networking and System Aspects - Abstract Syntax Notation One, Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation [X680]
 - 12) ITU-T Recommendation X.690,
Data Networks and Open System Communications OSI Networking and System Aspects - Abstract Syntax Notation One, Information Technology -ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) [X690]
 - 13) National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 180-2,
Secure Hash Standard (SHS), August 2002 [FIPS180-2]
 - 14) National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 186-2 (+Change Notice),
Digital Signature Standard (DSS), January 2000 [FIPS186-2]
 - 15) National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 197,
Advanced Encryption Standard (AES), November 2001 [FIPS197]
 - 16) National Institute of Standards and Technology (NIST), Special Publication 800-22,
Errata for A Statistical Test Suite for Random and Pseudorandom Number Generators, May 2001 [SP800-22]
 - 17) National Institute of Standards and Technology (NIST), Special Publication 800-38A,
Recommendation for Block Cipher Modes of Operation, 2001 [SP800-38A]
 - 18) Security Architecture for Intelligent Attachment Device Specifications;
Interface for iVDR, [SAFIA/IF]

1.3 Definitions

As far as specific meaning is not given, the following terms have the meanings described below in this document.

1.3.1 Definitions in X509

The following terms used in this document are defined in X509.

- Certificate
- Certification authority

1.3.2 Additional definitions

The following terms are used in this document.

- Access Condition
Usage Information specified by content providers, for controlling the use of content in the SAFIA Security Domain.
- Access Condition for Export Module
Access Conditions to be controlled for exporting in Export Module. Exporting of content from a Host Device is executed according to this condition. This term was defined as Access Condition for Export Device in version 1.0.
- Access Condition for Storage Module
Access Conditions to be controlled in Storage Module. Output of a Usage Pass from a Storage Device is executed according to this condition. This term was defined as Access Condition for Storage Device in version 1.0.
- Bidirectional Transfer
Usage Pass Transfer in which Usage Passes are allowed to transfer bidirectionally between a Primal Device and an Inceptive Device.
- Challenge Key
Temporary key of symmetric key cryptosystem. The key is generated in a Usage Pass Transfer Unit and is shared with the other Usage Pass Transfer Unit in Usage Pass Transfer.
- Cipher Information of Content
Information to decrypt an encrypted SAFIA Content. A Content Key shall be included in it.
- Connection
Procedure to share the first Session Keys and Device Public Keys between a Primal Device and an Inceptive Device.
- Connection Log
Log information in which progress of a Connection between a Primal Usage Pass Transfer Unit and an Inceptive Usage Pass Transfer Unit in Usage Pass Transfer is recorded.
- Content Decryptor
Functional unit to decrypt content.
- Content Encryptor
Functional unit to encrypt content.
- Content Identifier
Identifier uniquely assigned to every content.
- Content Key
Key to be used to decrypt an encrypted content. It is the key of the symmetric key cryptosystem.
- Data concatenation
Concatenating two distinct bit string data into a bit string data.

- Destination
A subject that receives a Usage Pass.
- Device
SAFIA compliant entity to handle Usage Pass. Storage Device, Host Device and so forth are included.
- Device Class
A Device Class indicates a set of Devices. Every Device belonging to a Device Class has a same Device Class Certificate.
- Device Class Certificate
Certificate for the Device Class Public Key.
- Device Class Private Key
A key embedded commonly in every Device belonging to a Device Class. The key is kept inside the Device secretly.
- Device Class Public Key
A public key corresponding to a Device Class Private Key.
- Device Interface
Specifications of connection and transmission of data among plural Devices. The detailed definition is provided in SAFIA/IF. This term was defined as Storage Device Interface in version 1.0.
- Device Private Key
A key embedded uniquely in every Device. The key is kept inside the Device secretly.
- Device Proper Keys
Generic name of four keys; Device Class Private Key, Device Class Public Key, Device Private Key and Device Public Key.
- Device Public Key
A public key corresponding to a Device Private Key.
- Domicile
Position of Usage Pass written or to be written in Qualified Storage.
- Entry Pointer
Pointer to designate the entry of Connection Log recorded in an Inceptive Device.
- ECDH Shared Key
Temporary key of symmetric key cryptosystem. The key is agreed with a Device Public Key and a Device Private Key through ECDH between a Usage Pass Transfer Unit and another Usage Pass Transfer Unit in Usage Pass Transfer.
- Export
Action to throw out content and Usage Information from the inside of SAFIA Security Domain to the outside of the SAFIA Security Domain executed by a Device.
- Export Module

Functional module to export content and Usage Information of the content from the inside of SAFIA Security Domain to the outside of SAFIA Security Domain. It is comprised of Usage Pass Transfer Unit, Usage Pass Extractor and Content Decryptor. This term was defined as Export Device in version 1.0.

- Host Interface Module
Functional module comprised of one or more Host Interface Units.
- Host Interface Unit
Interface Unit included in a Host Device.
- Host Device
Device including Host interface Module and at least one of the functional modules such as Import Module, Export Module and Transmit Module. It includes a Combined Device which was described in version 1.0.
- Host Management Unit
Functional unit to control a Host Device. This term was defined as Host in version 1.0.
- Import
Action to bring in content and Usage Information from the outside of SAFIA Security Domain to the inside of SAFIA Security Domain executed by a Host Device.
- Import Module
Functional module to import content and Usage Information of the content from the outside of SAFIA Security Domain to the inside of SAFIA Security Domain. It is comprised of Usage Pass Transfer Unit, Usage Pass Creator and Content Encryptor. This term was defined as Import Device in version 1.0.
- Inceptive
A subject to output Device Class Certificate in first.
- Interface Unit
Functional unit to interface a Device with another Device physically and logically. It is based on Device Interface.
- Licensee ID
Identifier number uniquely assigned to each adapter. It is four columns of natural number.
- Masked Usage Pass
A Usage Pass of which the Cipher Information of Content is filled with 00h.
- Message Version
Value to specify the structure of Sequence Messages supported by a Usage Pass Transfer Unit.
- Open Storage
Functional unit to record SAFIA Content, user data and so forth.
- Playback
An action of export. Transferred content based on Playback is not allowed to be recorded or stored in the outside of SAFIA Security Domain.

- Primal
A subject to verify Device Class Certificate in first.
- Procedure
A set of processes. The order of execution of the processes is determined strictly.
- Protected
Status in which illegal access is prohibited through technical manners (encryption, scrambling).
- Qualified Storage
Functional unit to record Usage Pass.
- Qualified Storage Controller
Functional unit to mediate Usage Pass between a Usage Pass Transfer Unit and Qualified Storage.
- Revoked Device Class List
List of revoked Device Class(es)
- Root Private Key
A private key kept safely in a certification authority. The key is used to calculate the digital signature included in a Device Class Certificate and a Revoked Device Class List.
- Root Public Key
A public key corresponding to a Root Private Key. The key is used to verify the Device Class Certificate and the Revoked Device Class List.
- SAFIA compliant
Conforming to the regulations specified in this document.
- SAFIA Content
Protected content in SAFIA Security Domain.
- SAFIA Security Domain
SAFIA Compliant Security Domain.
- SAFIA Terminal
Terminal equipment with a Host Device.
- Security Domain
Logical domain protected by a special content protection method. If there are several content protection methods, Security Domain shall be defined to each content protection method individually.
- Sequence Message
Message exchanged between a Primal Usage Pass Transfer Unit and an Inceptive Usage Pass Transfer Unit through Usage Pass Transfer.
- Session
A procedure to be executed while a pair of Session Keys in which two keys are included – one is generated in the Primal Device and the other is generated in the Inceptive Device – are

shared mutually. The procedure is determined strictly.

- Session Key
Temporary key of symmetric key cryptosystem. The key is generated by the one Usage Pass Transfer Unit and is shared with the other Usage Pass Transfer Unit in Usage Pass Transfer. A Usage Pass is encrypted with the latest Session Key generated in the Destination Device.
- Session Status
Information showing the status of the progress of Usage Pass Transfer.
- Source
A subject that sends a Usage Pass.
- Storage Interface Module
Functional module comprised of Storage Interface Unit.
- Storage Interface Unit
Interface Unit included in a Storage Device.
- Storage Device
Device including Storage Module, Storage Interface Module and Open Storage.
- Storage Module
Functional module to store Usage Pass. It is comprised of Usage Pass Transfer Unit, Qualified Storage Controller, and Qualified Storage. This term was defined as Security Management Module in version 1.0.
- Tamper Resistant Module
Software / hardware module having durability against attacks such as analysis, falsification and so forth for the purpose of illegal access of content.
- Transaction
A procedure to complete a Usage Pass Transfer.
- Transaction Log
Log information in which progress of a Transaction between a Primal Usage Pass Transfer Unit and an Inceptive Usage Pass Transfer Unit in Usage Pass Transfer is recorded.
- Transaction Status
Data that is transferred from an Inceptive Usage Pass Transfer Unit to a Primal Usage Pass Transfer Unit so as to resume the interrupted Usage Pass Transfer.
- Transmit
Action to transfer the received Usage Pass from a Storage Device to another one in SAFIA Security Domain.
- Transmit Module
Functional module to transmit Usage Pass from a Storage Device to another one in SAFIA Security Domain. It is comprised of Usage Pass Transfer Unit and Usage Pass Transmitter. This term was defined as Transmit Device in version 1.0.
- Unidirectional Transfer

Usage Pass Transfer in which Usage Passes are allowed to transfer unidirectionally between a Primal Device and an Inceptive Device.

- Usage Information
Signal or digital information specifying content usage regulations approved by the right holder. This information includes copy control information.
- Usage Pass
Data in which Content Key and Access Condition are packaged conforming to the format specified in this document.
- Usage Pass Copy
Usage Pass Transfer to copy a Usage Pass from a Storage Device. Access Condition for Storage Module may be modified and the Usage Pass remains in the Source Storage Device.
- Usage Pass Creator
Functional unit to create Usage Pass when a Device imports Usage Information.
- Usage Pass Extractor
Functional unit to extract Usage Pass when a Device exports Usage Pass.
- Usage Pass Identifier
Identifier assigned uniquely to each Usage Pass
- Usage Pass Move
Usage Pass Transfer to move a Usage Pass from a Storage Device. After this transaction, the Usage Pass in the Source Storage Device shall be deleted or invalidated.
- Usage Pass Play
Usage Pass Transfer to execute Playback at Destination Device from a Storage Device. Access Condition for Storage Module may be modified and the Usage Pass remains in the Source Storage Device.
- Usage Pass Recovery
A procedure to restore the Usage Pass in a Source Device to pre-transferred one, if the sent Usage Pass has not been recorded in properly a Destination Device.
- Usage Pass Status
Information showing the status of existence of a Usage Pass in Qualified Storage.
- Usage Pass Transfer
Generic expression for the action to send and receive Usage Pass between two Devices.
- Usage Pass Transfer Protocol
A procedure for a Usage Pass Transfer.
- Usage Pass Transfer Unit
Functional unit equipped in all Devices to transfer Usage Pass conforming to Usage Pass Transfer Protocol.
- Usage Pass Transmitter
Functional unit to transmit a Usage Pass from a Storage Device to another one in SAFIA

Security Domain.

1.4 Abbreviations

As far as specific meaning is not given, the following terms are used as the abbreviations in this document.

- AES Advanced Encryption Standard
- AC Access Condition
- AC_e Access Condition for Export Module
- AC_s Access Condition for Storage Module
- ASN.1 DER Distinguished Encoding Rules of Abstract Syntax Notation One
- BP Byte position starting within a descriptor or information, starting with 0
- BT Bidirectional Transfer
- CBC Cipher Block Chaining
- CD Content Decryptor
- CE Content Encryptor
- CIC Cipher Information of Content
- CID Content Identifier
- CLOG, CL Connection Log
- ECC Elliptic Curve Cryptography
- ECDH Elliptic Curve Diffie-Hellman
- ECDSA Elliptic Curve Digital Signature Algorithm
- HIFU Host Interface Unit
- HMU Host Management Unit
- LSB Least Significant Bit
- MSB Most Significant Bit
- OID Object Identifier
- OST Open Storage
- QST Qualified Storage
- QSTC Qualified Storage Controller
- RDCL Revoked Device Class List
- SAFIA Security Architecture for Intelligent Attachment Device
- SIFU Storage Interface Unit
- SHA Secure Hash Algorithm

- SS Session Status
- TLOG, TL Transaction Log
- TRM Tamper Resistant Module
- UP Usage Pass
- UPC Usage Pass Creator
- UP Copy Usage Pass Copy
- UPE Usage Pass Extractor
- UPID Usage Pass Identifier
- UPL Usage Pass Location
- UP Move Usage Pass Move
- UP Play Usage Pass Play
- UPS Usage Pass Status
- UPT Usage Pass Transmitter
- UP Transfer Usage Pass Transfer
- UPTU Usage Pass Transfer Unit
- UT Unidirectional Transfer

1.5 Conventions

The following conventions are used in this document.

1.5.1 Keywords

- Mandatory Indicates actions and features to be implemented as defined by this document.
- May Indicates an action or feature that is optional.
- Not used Indicates bits, bytes, field, and code values are not used in this document. A bit, byte or field is usually filled with 0b unless particular requirement is given. A bit, byte or field as not used shall not be checked.
- Optional Indicates actions and features that are not required by this document. However, if any optional action or feature defined by this document is implemented, it shall be implemented in the way defined by this document.
- Shall Indicates an action or feature that is mandatory and must be implemented conforming to this document.
- Should Indicates an action or feature that is optional, but it is strongly recommended to be implemented.
- Reserved Indicates bits, bytes, field and code values are reserved for future use. A reserved bit, byte or field shall be filled with 0b unless particular requirements

are given.

1.5.2 Numerical values

The following numerical values are used in this document. Decimal numbers are represented as decimal digits 0 to 9. Hexadecimal numbers are represented as hexadecimal digits 0 to 9 and A to F suffixed by the symbol “h”. Binary numbers are represented as binary digits 0 to 1 suffixed by the symbol “b”.

1.5.3 Bit and byte ordering

Certain data values or parts of data values are interpreted as an array of bits. Unless explicitly noted otherwise, bit positions within an n-bit data value are numbered such that the least significant bit is numbered 0 and the most significant bit is numbered n-1. Unless otherwise specified, big-endian ordering is used for multiple byte values, meaning that byte 0 is the most significant byte.

1.6 Notations

The following notations are used in this document.

1.6.1 Keys and data

- K_c Content Key.
- K_r Root Private Key.
- KP_r Root Public Key.
- K_{dc} Device Class Private Key.
- $Kdc[x]$ Device Class Private Key installed in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- KP_{dc} Device Class Public Key.
- $KP_{dc[x]}$ Device Class Public Key installed in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- K_d Device Private Key.
- $K_{d[x]}$ Device Private Key installed in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- KP_d Device Public Key.
- $KP_{d[x]}$ Device Public Key installed in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- $KP_{d[x]CL}$ Device Public Key $KP_{d[x]}$ recorded in Connection Log of the partner Device on BT mode.
- $KP_{d[I]TL}$ Device Public Key $KP_{d[I]}$ recorded in Transaction Log of Primal Device on UT

- mode.
- K_{ch} Challenge Key.
- $K_{ch[x]}$ Challenge Key generated in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- K_s Session Key.
- $K_{s[x]}$ Session Key generated in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- $K_{s[x]CL}$ Session Key $K_{s[x]}$ recorded in Connection Log on BT mode.
- $K_{s[x]TL}$ Session Key $K_{s[x]}$ recorded in Transaction Log on UT mode.
- $*KP_{d[x]}$ ECDH Shared Key which is symmetric key agreed through ECDH key exchange with $KP_{d[x]}$ and $K_{d[x]}$.
- $RDCL_{[x]}$ Revoked Device Class List kept in x Device. x is whether “I” which means Inceptive or “P” which means Primal.
- AC_{sTL} Original AC_s recorded in Transaction Log of Primal Device.

1.6.2 Operations

- $A ::= B$ Definition to make the content of information. B as information A.
- $E(K,D)$ Result of encrypting data D with key K.
- $C(K_r, KP_x)$ Certificate of a public key KP_x .
- $H(D)$ Hash value of Information D.
- P-Enc Process for agreeing ECDH Shared Key $*KP_x$ with ECC public key KP_x through ECDH and encrypting data with the key $*KP_x$.
- P-Dec Process for agreeing ECDH Shared Key $*KP_x$ with ECC private key K_x through ECDH and decrypting encrypted data with the key $*KP_x$.
- S-Enc Process for encrypting data with a key of symmetric key cryptosystem.
- S-Dec Process for decrypting encrypted data with a key of symmetric key cryptosystem.
- R-Gen Process for generating key of symmetric key cryptosystem.
- + Addition.
- – Subtraction.
- \times Multiplication, scalar multiplication.
- || Concatenation.
- | Choice.
- = Assignment, equal to.
- \leq Less than or equal to.

2 SAFIA Security Domain descriptions

This chapter describes SAFIA Security Domain.

2.1 Information in SAFIA Security Domain

In the SAFIA Security Domain, Usage Pass and SAFIA Content may be handled separately.

2.1.1 Usage Pass

Usage Pass is necessary information to use content. Usage Pass shall include Content Key K_c to decrypt SAFIA Content and AC. Usage Pass is recorded in TRM so that it is protected from illegal access.

2.1.2 SAFIA Content

SAFIA Content is data encrypted with Content Key K_c . It can be read and copied without restrictions from a Storage Device to another. However, it is encrypted so that it is impossible to use without Usage Pass.

2.1.3 Controlled content

Content with restrictions on usage provided by the right holder. When importing such content from other Security Domain to SAFIA Security Domain, it shall be converted into SAFIA Content.

Controlled content shall be encrypted with Content Key K_c and Usage Information of controlled content converts it into AC.

2.1.4 Non-controlled content

Content without restrictions on usage. As for such content, it shall not be converted into SAFIA Content as far as it is not admitted by SAFIA License Group.

2.2 Supposed total system model

Figure 2.1 shows the SAFIA Security Domain.

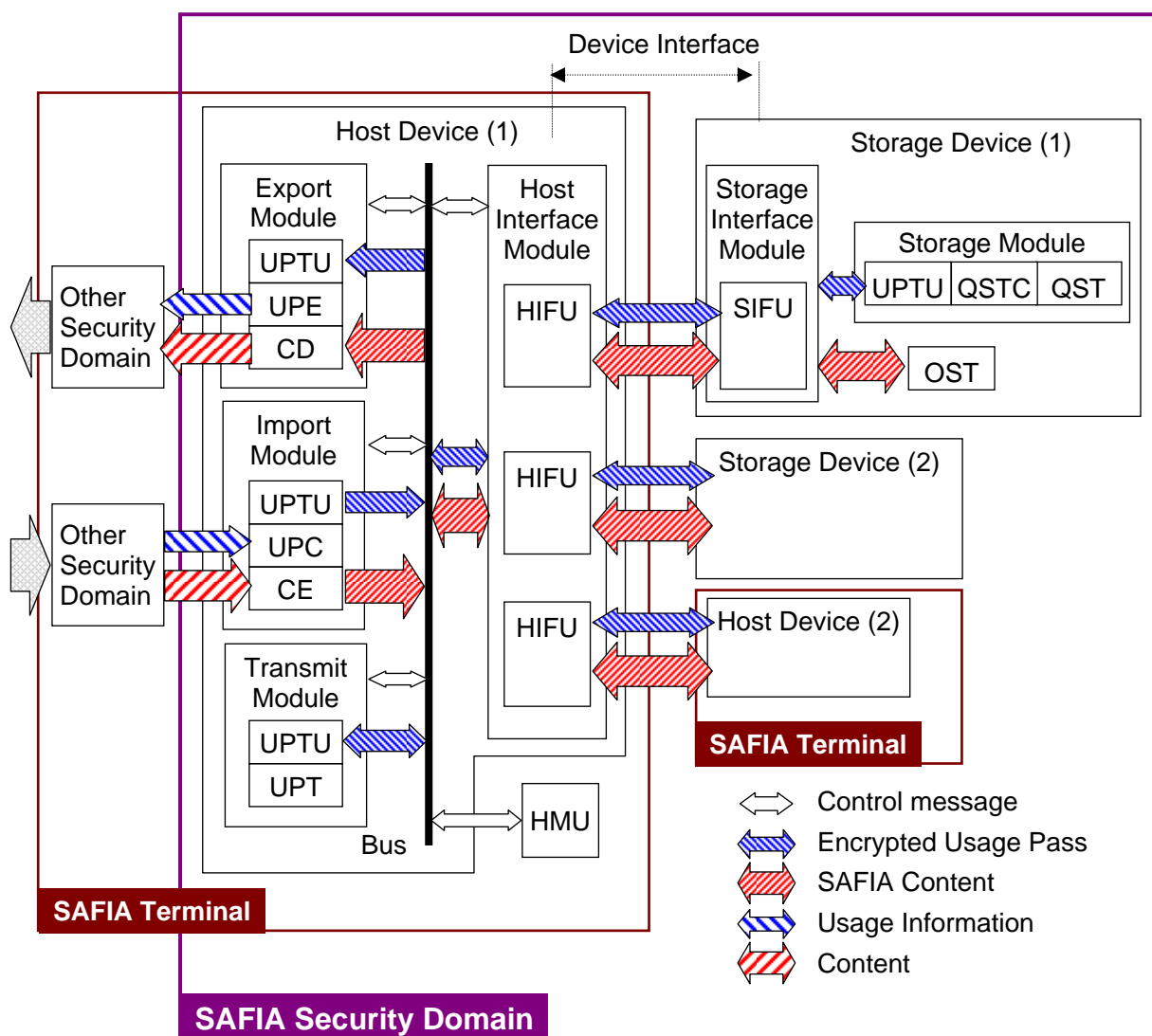


Figure 2.1 SAFIA Security Domain

2.3 Functional units

In this section, respective functional units in the SAFIA Security Domain shown in Figure 2.1 are described.

- CD (Content Decryptor)
 Functional unit to decrypt content. By using of K_c received from UPE, this unit decrypts the objective content.
- CE (Content Encryptor)
 Functional unit to encrypt content. This unit encrypts content brought in from other Security Domain with K_c created in UPC, and converts it into SAFIA Content.
- HIFU (Host Interface Unit)
 Functional unit to interface the Host Device included itself with another Device physically and logically. The Host Device shall transfer Usage Pass and SAFIA Content through HIFU.

- OST (Open Storage)
Storage to record SAFIA Content (encrypted content). Access to this unit is not restricted by this document.
- SIFU (Storage Interface Unit)
Functional unit to interface the Storage Device included itself with another Device physically and logically. The Storage Device shall transfer Usage Pass and SAFIA Content through SIFU.
- QST (Qualified Storage)
Storage to record Usage Pass. Access to this unit is possible only through UPTU and QSTC.
- QSTC (Qualified Storage Controller)
Functional unit to mediate Usage Pass information between a Usage Pass Transfer Unit and Qualified Storage.
- UPC (Usage Pass Creator)
Functional unit to create Usage Pass. This unit receives Usage Information from other Security Domain, and converts it into AC, and creates K_c to encrypt the objective content, and sends the key to CE.
- UPE (Usage Pass Extractor)
Functional unit to extract Usage Pass and interpret AC. This unit sends K_c to CD and controls content throwing out from CD to other Security Domain conforming to AC in Usage Pass.
- UPT (Usage Pass Transmitter)
Functional unit to relay Usage Pass in SAFIA Security Domain. This unit does not change Usage Pass on transmit. This unit sends back received Usage Pass from a UPTU to it.
- UPTU (Usage Pass Transfer Unit)
Functional unit to control Usage Pass Transfer.

2.4 Functional modules

In this section, individual functional modules in the SAFIA Security Domain shown in Figure 2.1 are specified.

2.4.1 Storage Module

A functional module to record Usage Pass. This module comprises QSTC, QST and UPTU. When this module behaves as a Destination, the QSTC receives a Usage Pass from a Source Device through the UPTU in the same module, and records the Usage Pass to QST. When this module behaves as a Source, the QSTC appropriately judges whether a Usage Pass output is allowed or not according to AC_s . If it is allowed, the QSTC sends the Usage Pass to a Destination Device through the UPTU. This module shall be implemented as TRM.

2.4.2 Export Module

A functional module to export content and Usage Information from SAFIA Security Domain to other Security Domain. This module comprises UPE, CD and UPTU. The UPE receives a Usage

Pass from a Source Device through the UPTU in the same functional module. Then the UPE extracts and interprets AC_s and AC_e in Usage Pass, and judges whether content output is allowed or not. If it is allowed, the UPE converts AC_s and AC_e into the Usage Information conforming to other Security Domain, and sends K_c to the CD. The CD decrypts SAFIA Content with K_c . This module shall be implemented as TRM. Additional rules are described in SAFIA Specification for each application.

2.4.3 Import Module

A functional module to import content and Usage Information from other Security Domain to SAFIA Security Domain. This module comprises UPC, CE and UPTU. The UPC generates K_c , and sends it to the CE, converts Usage Information conforming to other SAFIA Security Domain into AC, and creates a Usage Pass from the K_c and AC. Then the UPC transfers the created Usage Pass to a Destination Device through the UPTU in the same functional module. The CE encrypts input content into SAFIA Content with K_c and transfers the SAFIA Content to the Destination Device. This module shall be implemented as TRM. Additional rules are described in SAFIA Specification for each application.

2.4.4 Transmit Module

A functional module to relay Usage Pass between two Storage Devices. This module comprises UPT and UPTU. The UPT receives a Usage Pass from a Storage Device through the UPTU in the same module. Then the UPT extracts and interprets Usage Pass Format and AC_s in the Usage Pass, and judges whether Usage Pass is sent to another Storage Device is allowed or not. If it is allowed, the UPT sends Usage Pass which is not changed to the other Storage Device through the UPTU. This module shall be implemented as TRM.

2.4.5 Storage Interface Module

A functional module comprised of one or more SIFUs

2.4.6 Host Interface Module

A functional module comprised of one or more HIFUs.

2.5 Constitution element

In this section, individual structural components in the SAFIA Security Domain shown in Figure 2.1 are described.

2.5.1 Storage Device

A Device for recording SAFIA Content and Usage Pass. It implements Storage Module, OST and Storage Interface Module. SAFIA Content and Usage Pass shall be received and transferred through Storage Interface Module.

2.5.2 Host Device

A Device implements a functional module or plural functional modules among three functional modules described above, namely Export, Import and Transmit Module. In addition, it implements Host Interface Module.

3 SAFIA security design policy

3.1 Tamper Resistant Module

Storage Module, Import Module, Export Module and Transmit Module in the SAFIA Security Domain shall be implemented as TRM.

3.2 Usage Pass Transfer Protocol

In the SAFIA Security Domain, Usage Pass Transfer Protocol is determined in consideration of safety. The basic concept for these protocols is the following: the Source and the Destination confirm mutually the validity using Certificate of the counterpart, and only when the validity of them is confirmed, Usage Pass Transfer is executed between the Source UPTU and the Destination UPTU. Since communication between UPTUs is protected by the Usage Pass Transfer Protocol, communication lines including bus shown in Figure 2.1 do not have to be TRM.

3.3 Revocation

The Device of which safety is lost shall be excluded from SAFIA Security Domain.

3.4 Usage Pass Type

Plural Usage Pass Types are defined in response to the differences of content and service. If a Host Device receives a Usage Pass of which Usage Pass Type is not supported, the Device shall not decrypt the objective SAFIA Content. And a Storage Device as Source shall not transfer a Usage Pass to a Destination Device if the Usage Pass Type of the objective Usage Pass is not supported at the Destination Device. Information on the supported Usage Pass Type is included in Device Class Certificate of each Device. Usage Pass Type is described in SAFIA Specification for each application.

4 Cryptographic functions

This chapter describes the common cryptographic functions in the SAFIA Security Domain.

4.1 Hash function

SHA-256 function is used as hash function. The SHA-256 is the algorithm that converts any length data into 256-bit hash value. The details are specified in FIPS180-2.

4.2 Symmetric cryptography

Symmetric cryptographic functions are based on the Advanced Encryption Standard (AES) block cipher algorithm that is specified in FIPS197. Unless some other cryptographic function is particularly provided, the AES algorithm shall be used with 128-bit key. Cipher Block Chaining (CBC) mode of operation specified in SP800-38A shall be adopted as the method of chain between blocks in its encryption and decryption. The initialization vector depends on the particular application.

4.3 Asymmetric cryptography

Asymmetric cryptographic functions are based on the Elliptic Curve Cryptography (ECC) scheme as specified in IEEE/P1363. Elliptic curve is defined over prime finite (256-bit) field. ECC is used for key sharing and digital signature.

4.3.1 Key agreement algorithm

Elliptic Curve Diffie-Hellman (ECDH) scheme specified in ANSI/X9.63 is generally used as a method to share a key between two Devices. The shared key is a key for symmetric cryptographic operation. The shared key obtained through ECDH is used to encrypt and decrypt various messages.

4.3.2 Digital signature algorithm

Elliptic Curve Digital Signature Algorithm (ECDSA) specified in ANSI/X9.62 is used as a signature algorithm. SHA-1 is used as a signature algorithm in ECDSA. However, SHA-256 is used instead of SHA-1 in this document.

4.4 Random / pseudorandom number generator

Random number or pseudorandom number generator is required to generate values such as cryptographic keys. The generator shall satisfy one of the following features; (1) Pseudorandom number generator is designed according to the description in ANSI/X9.31 (2) Pseudorandom number generator is designed according to the description in FIPS180-2 (3) Random number or pseudorandom number generator have equal or higher quality that passes the tests described in SP800-22.

5 Common cryptographic key

5.1 Device Proper Keys

Device Proper Keys are generic name of four keys; Device Class Private Key K_{dc} , Device Class Public Key KP_{dc} , Device Private Key K_d and Device Public Key KP_d . A set of Device Proper Keys is installed to each Device when it is manufactured.

5.1.1 Device Class Private / Public Key

A pair of Device Class Private Key K_{dc} and Public Key KP_{dc} is provided by SAFIA License Group. The Device Class Public Key is included in a Device Class Certificate. If Device is compromised in a way that threatens the integrity of system, the Device Class Public Key is revoked with RDCL. The pair of keys may be either unique per Device or used commonly by multiple Devices. Device Class Private Key is highly confidential. A Device shall not output its Device Class Private Key.

5.1.2 Device Private / Public Key

A pair of Device Private Key K_d and Public Key KP_d is provided by SAFIA License Group or a adaptor. The pair of keys may be unique per Device. The pair of keys is highly confidential. A Device shall not output its Device Private Key. A Device shall not output its Device Public Key in ways except for Usage Pass Transfer.

5.2 Root Public Key

Root Public Key is used for verification of Device Class Certificate and RDCL. The key is installed to each Device when it is manufactured. The key is provided by SAFIA License Group. The key is highly confidential. A Device shall not output the key.

5.3 Challenge / Session Keys

Challenge Keys K_{ch} and Session Keys K_s are random/pseudorandom numbers generated in a Device and exchanged between two Devices in Usage Pass Transfer. A Device shall not output the keys in ways except for Usage Pass Transfer. Two latest Session Keys that are generated in Primal Device and Inceptive Device respectively are shared between the Devices.

5.4 ECDH Shared Key

ECDH Shared Key $*KP_d$ is a value calculated with KP_d and random/pseudorandom number generated in a Device. This key is agreed between two Devices in Usage Pass Transfer. A Device shall not output this key.

5.5 Content Key

A Content Key K_c is random/pseudorandom numbers generated in a Device or provided by a copyright holder. A Device shall not output this key except in the case of Usage Pass Transfer.

6 Outline of protocol

This chapter describes the protocols to send and receive a Usage Pass safely from a Device to another Device in the SAFIA Security Domain.

UPTU is a functional unit to manage Usage Pass Transfer. A Device executing Usage Pass Transfer shall be equipped with the UPTU.

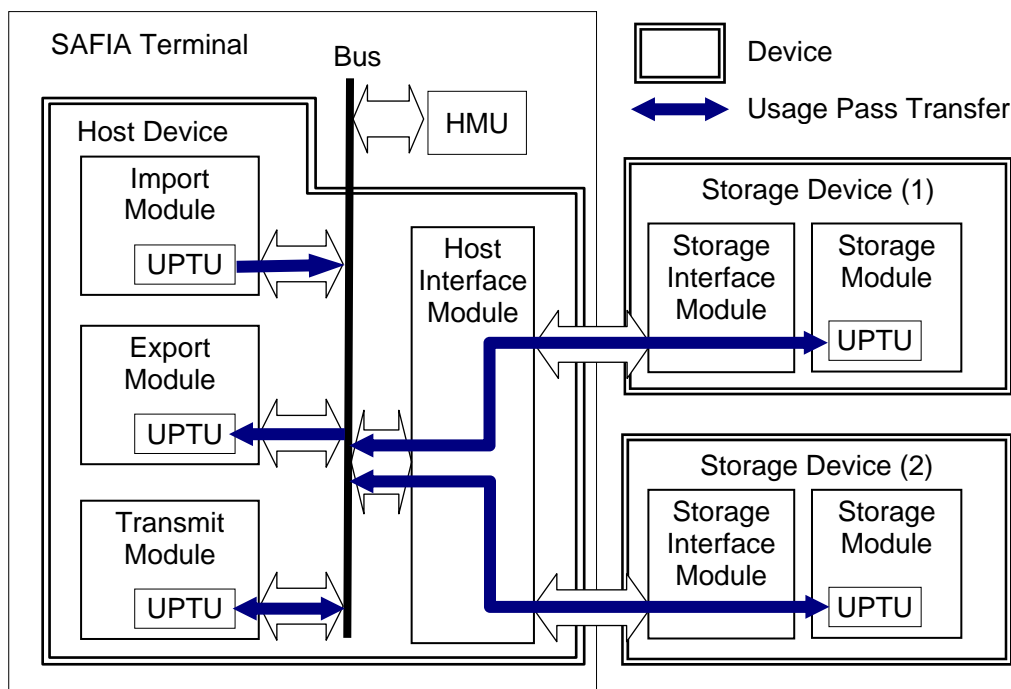


Figure 6.1 Subject of Usage Pass Transfer

6.1 Unidirectional Transfer (UT) mode

The Usage Pass Transfer Protocol on UT mode includes the basic steps and the additional steps to resume interrupted Usage Pass Transfer. A Primal Device shall only be a Source Device and an Inceptive Device shall only be a Destination Device.

A HMU shall manage Usage Pass Transfer Protocol between a Primal UPTU and an Inceptive UPTU.

6.1.1 Basic steps

Basic steps consist of two stages: (1) Connection Stage where a Primal UPTU and an Inceptive UPTU share two Session Keys and an ECDH Shared Key, (2) Transfer Stage where the Primal UPTU sends a Usage Pass to the Inceptive UPTU.

6.1.1.1 Connection Stage

Basic steps of UT mode for connection are shown in Figure 6.2. As long as both Primal and Inceptive UPTU keep the latest keys, Connection Stage may be skipped.

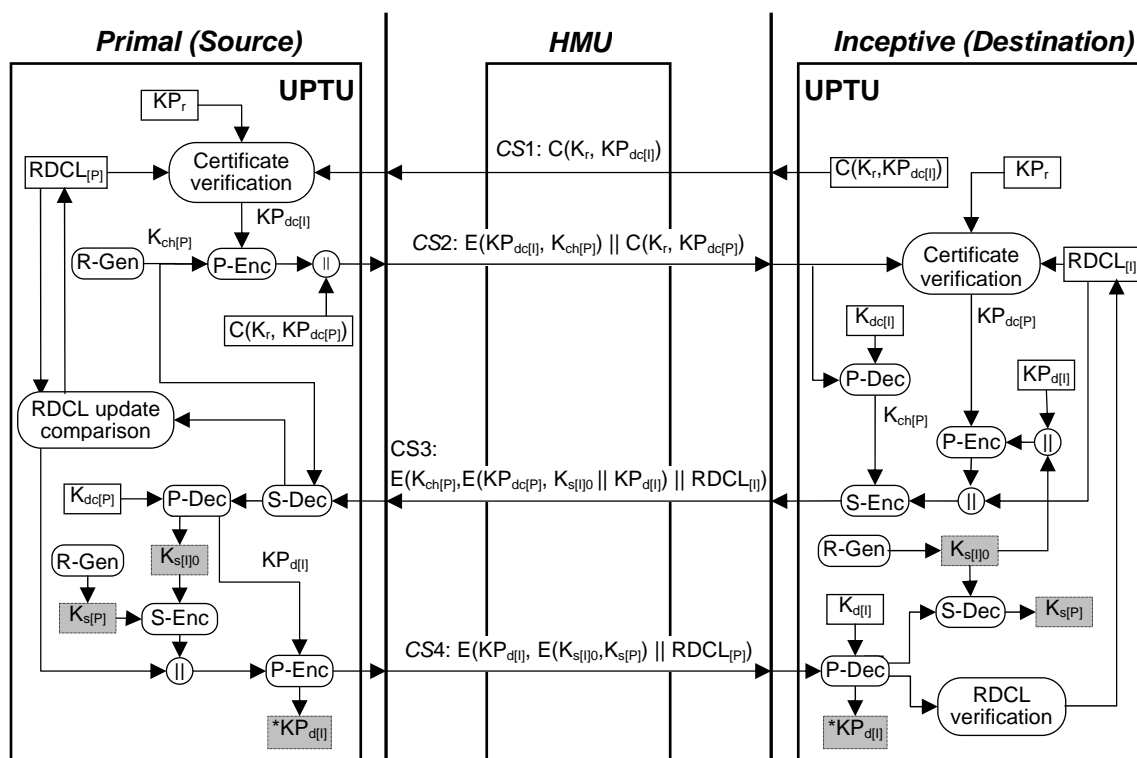


Figure 6.2 Basic steps of UT mode for connection

[Connection Stage]

- CS1 Inceptive UPTU sends its own Device Class Certificate $C(K_r, KP_{dc[I]})$ to Primal Device. After receiving it, the Primal UPTU verifies the certificate sent from the Inceptive UPTU. Root Public Key KP_r is used on the verification. If the verification fails, the Primal UPTU shall quit the Connection Stage.
- CS2 The Primal UPTU generates a Challenge Key $K_{ch[P]}$, and encrypts the Challenge Key $K_{ch[P]}$ with the Device Class Public Key $KP_{dc[I]}$. The Primal UPTU sends its own Device Class Certificate $C(K_r, KP_{dc[P]})$ together with the encrypted Challenge Key to the Inceptive UPTU. After receiving them, the Inceptive UPTU decrypts the encrypted Challenge Key with its own Device Class Private Key $K_{dc[I]}$. Moreover, the Inceptive UPTU verifies the certificate with Root Public Key KP_r . If the verification fails, the Inceptive shall quit the Connection Stage.
- CS3 The Inceptive UPTU generates a Session Key $K_{s[I]0}$. And then, the Inceptive UPTU concatenates it with the Device Public Key $KP_{d[I]}$ and encrypts the data with Device Class Public Key $KP_{dc[P]}$. Moreover, the Inceptive UPTU concatenates the data with $RDCL_{[I]}$ recorded in the Inceptive Device and encrypts it with the Challenge Key $K_{ch[P]}$. After that, the Inceptive UPTU sends it to the Primal UPTU. After receiving the encrypted data, the Primal UPTU decrypts it with the Challenge Key $K_{ch[P]}$ and its own Device Class Private Key $K_{dc[P]}$ consecutively.
- CS4 First off, the Primal UPTU generates a Session Key $K_{s[P]}$, and encrypts it with the Session Key $K_{s[I]0}$. Here, if issue date of $RDCL_{[I]}$ recorded in the Inceptive Device is

older than that of $RDCL_{[P]}$, the Primal UPTU concatenates its own $RDCL_{[P]}$ with the encrypted data mentioned above. Meanwhile, if the date is newer than that of $RDCL_{[P]}$, the Primal UPTU shall replace the $RDCL_{[P]}$ with the received $RDCL_{[I]}$. Next, the Primal UPTU encrypts the data with the Device Public Key $KP_{d[I]}$ and sends it to the Inceptive UPTU. After receiving the encrypted data, the Inceptive UPTU decrypts it with the Device Private Key $K_{d[I]}$ and the Session Key $K_{s[I]0}$ consecutively. If a $RDCL_{[P]}$ is included in the received data, the Inceptive UPTU shall replace the $RDCL_{[I]}$ of its own with the $RDCL_{[P]}$ included in the received data. As a result, both UPTUs share Session Keys $K_{s[P]}$, $K_{s[I]0}$ and ECDH Shared Key $*KP_{d[I]}$.

6.1.1.2 Transfer Stage

Basic steps of UT mode for transfer of Usage Pass from the Primal Device to the Inceptive Device is shown in Figure 6.3. Before entering this stage, Session Keys $K_{s[P]}$, $K_{s[I]n}$ and ECDH Shared Key $*KP_{d[I]}$ shall be shared between both UPTUs. At the end of this stage, two shared keys, Session Keys $K_{s[P]}$, and ECDH Shared Key $*KP_{d[I]}$ are not changed. And the shared Session Key $K_{s[I]n}$ is changed to $K_{s[I]n+1}$.

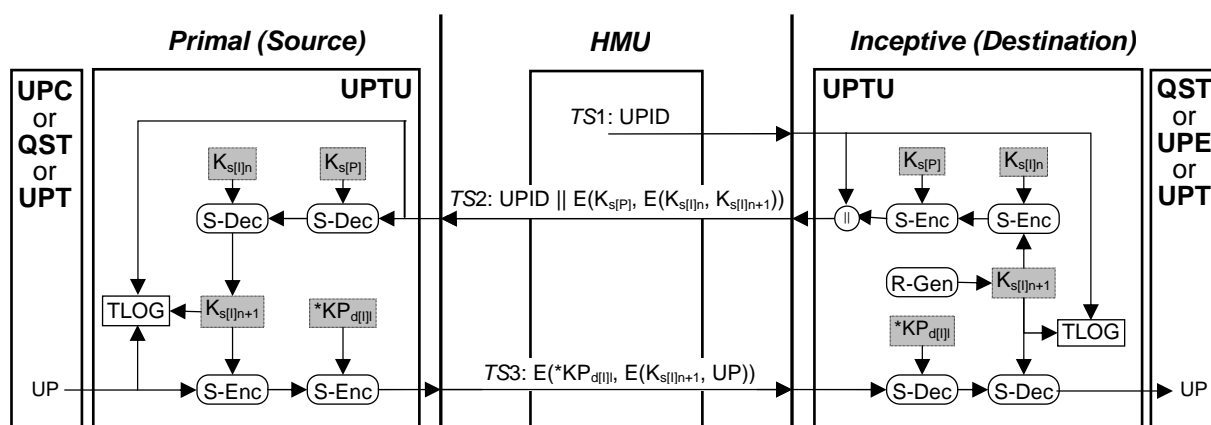


Figure 6.3 Basic steps of UT mode for transfer of a Usage Pass

[Transfer Stage]

- TS1 The HMU sends the UPID of the Usage Pass to be transferred to the Inceptive UPTU. When the Inceptive UPTU receives the UPID, the UPTU generates a new Session Key $K_{s[I]n+1}$. Then, the Inceptive UPTU starts to record Transaction Log.
- TS2 The Inceptive UPTU encrypts the Session Key $K_{s[I]n+1}$ with the Session Key $K_{s[I]n}$ and the Session Key $K_{s[P]}$ consecutively. The Inceptive UPTU sends the encrypted data with UPID to the Primal UPTU. After receiving them, the Primal UPTU decrypts the received data except UPID with the Session Key $K_{s[P]}$ and the Session Key $K_{s[I]n}$ that is generated previously consecutively. The Primal Device starts to record Transaction Log after the decryption.
- TS3 The Primal UPTU encrypts a Usage Pass with the Session Key $K_{s[I]n+1}$ and the ECDH Shared Key $*KP_{d[I]}$ consecutively. The Primal UPTU sends the encrypted Usage Pass to the Inceptive UPTU. After receiving it, the Inceptive UPTU decrypts it with the

Session Key $K_{s[i]n+1}$ and the ECDH Shared Key $*KP_{d[i]}$ consecutively.

6.1.2 Additional steps

Additional steps consist of four stages: (1) Reconnection Stage where a Primal UPTU and an Inceptive UPTU share new Session Keys and shared key with the Session Key $K_{s[i]TL}$ recorded in Transaction Log, (2) Recovery Stage where the Usage Pass is recovered to the pre-transferred one in the Primal Device (3) Two Usage Pass Inquiry Stages where HMU check a Usage Pass recorded in Primal Device and Inceptive Device.

6.1.2.1 Reconnection Stage

Additional steps for reconnection are shown in Figure 6.4. Before entering this stage, UPID, Device Public Key $KP_{d[i]TL}$ and Session Key $K_{s[i]TL}$ shall be recorded in Transaction Log of both UPTUs.

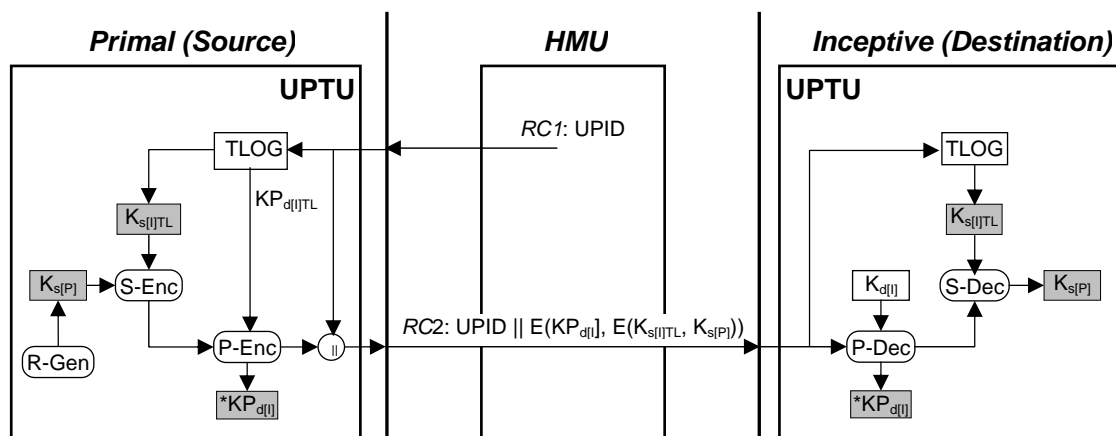


Figure 6.4 Additional steps of UT mode for reconnection

[Reconnection Stage]

RC1 The HMU sends the UPID recorded in the objective Transaction Log to the Primal UPTU. If the Primal UPTU cannot find the Transaction Log with the UPID, the UPTU shall quit the Reconnection Stage.

RC2 The Primal UPTU generates a new Session Key $K_{s[P]}$ and encrypts it with $K_{s[i]TL}$ and Device Public Key $KP_{d[i]TL}$ in the Transaction Log consecutively. The Primal UPTU sends the encrypted data with UPID to the Inceptive UPTU. After receiving it, the Inceptive UPTU decrypts the received data except UPID with the Session Key $K_{s[i]TL}$ and its own Device Private Key $K_{d[i]}$ consecutively. As a result, both UPTUs share $K_{s[P]}$, $K_{s[i]TL}$, and $*KP_{d[i]}$.

6.1.2.2 Recovery Stage

Additional steps to recover Usage Pass are shown in Figure 6.5. Before entering this stage, (1) UPID and Session Key $K_{s[i]TL}$ shall be recorded in Transaction Log of both UPTUs, (2) three keys; Session Keys $K_{s[P]}$, $K_{s[i]n}$ and ECDH Shared Key $*KP_{d[i]}$ shall be shared between both UPTUs. At the end of this stage, three shared keys are not changed.

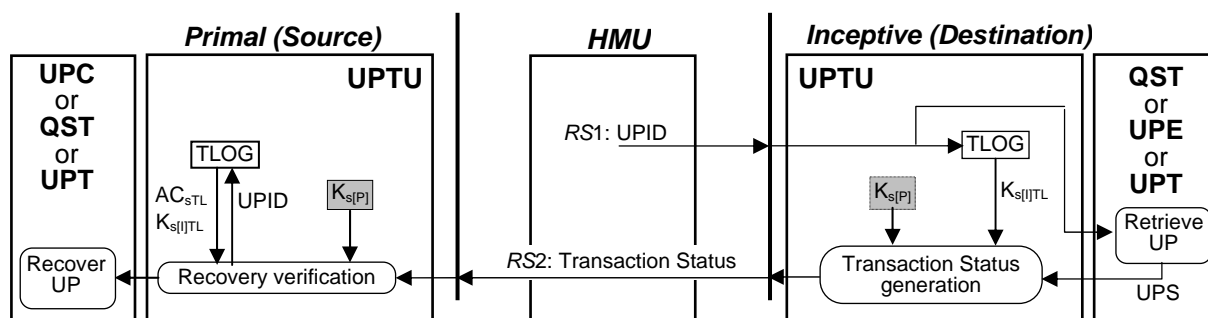


Figure 6.5 Additional steps of UT mode for recovery of a Usage Pass

[Recovery Stage]

- RS1** The HMU sends UPID of the Usage Pass to be recovered to the Inceptive UPTU. If the Inceptive UPTU cannot find the Transaction Log with the UPID, the UPTU shall quit the Recovery Stage. If the Inceptive UPTU find the Transaction Log, the UPTU generates Transaction Status using the Session Keys $K_{s[P]}$ and $K_{s[PTL]}$.
- RS2** The Inceptive UPTU sends Transaction Status to the Primal UPTU. After receiving it, the Primal UPTU verifies Transaction Status with the Session Key $K_{s[P]}$ and $K_{s[PTL]}$ of its Transaction Log. If the objective Usage Pass has already been moved or the Access Condition has already been changed, the Primal UPTU recovers the Usage Pass.

6.1.2.3 Usage Pass Inquiry Stage

Additional steps for inquiry of Usage Pass in a Primal Device and an Inceptive Device. Both Primal Device and Inceptive UPTU may send a Masked Usage Pass to the HMU. HMU inquires and confirms UPID and the Access Condition of the objective Usage Pass in this stage. Before entering this stage, the three keys, which are Session Keys $K_{s[P]}$, $K_{s[PTL]}$, and ECDH Shared Key $*KP_{d[PT]}$ shall be shared between both UPTUs. At the end of this stage, the three shared keys are not changed.

6.2 Bidirectional Transfer (BT) mode

The Usage Pass Transfer Protocol on BT mode includes the basic steps and the additional steps to resume interrupted Usage Pass Transfer. Both Primal Device and Inceptive Device may be Source Device and Destination Device. A Storage Device shall be the Inceptive Device. A Host Device shall be the Primal Device. A HMU in the Host Device shall manage the Usage Pass Transfer Protocol between a Primal UPTU and an Inceptive UPTU.

6.2.1 Basic steps

Basic steps consist of three stages: (1) Connection Stage where a Primal UPTU and an Inceptive UPTU share two Session Keys and two ECDH Shared Keys (2) two types of Transfer Stage where the Primal UPTU sends a Usage Pass to the Inceptive UPTU and its vice versa.

6.2.1.1 Connection Stage

Basic steps for connection are shown in Figure 6.6. As long as both Primal and Inceptive UPTU keep the latest Session Keys and ECDH Shared Keys, Connection Stage may be skipped.

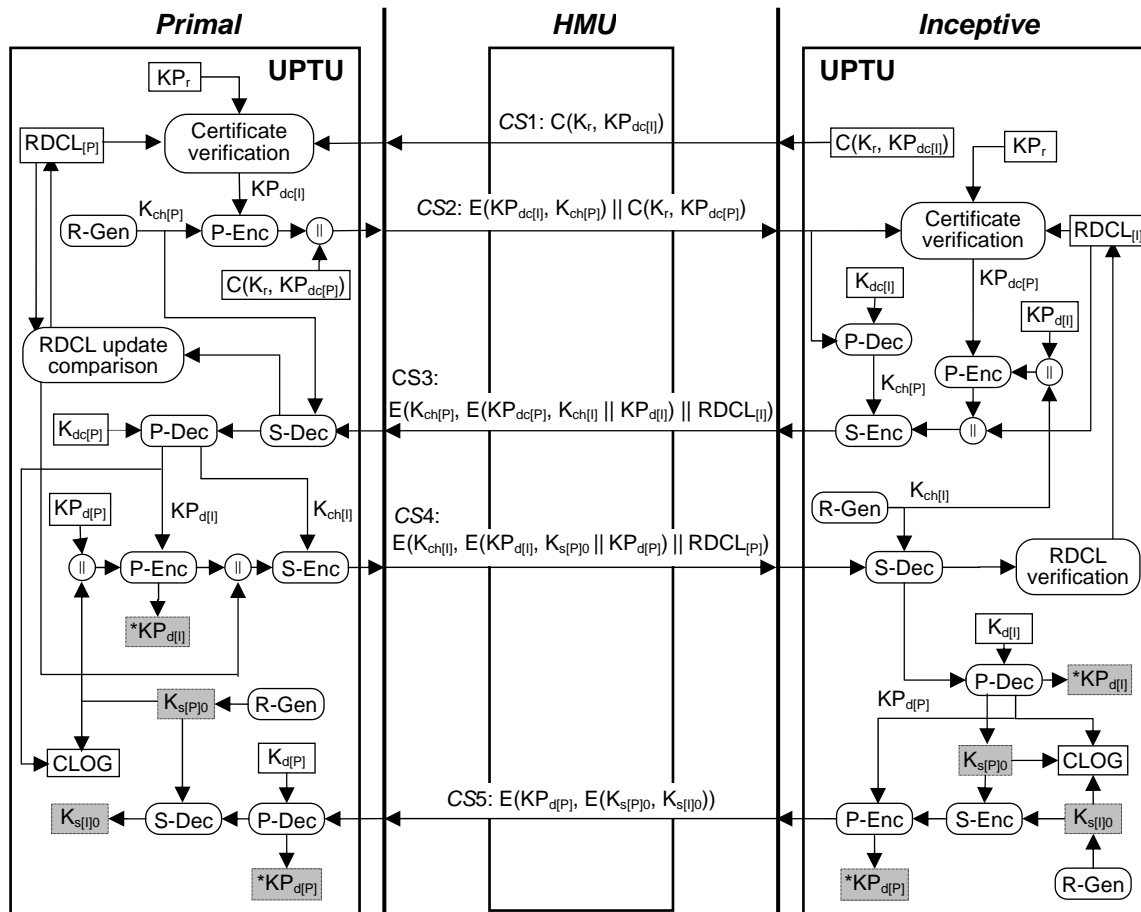


Figure 6.6 Basic steps of BT mode for connection

[Connection Stage]

- CS1 Same as CS1 of Connection Stage in UT mode.
- CS2 Same as CS2 of Connection Stage in UT mode.
- CS3 The Inceptive UPTU generates a Challenge Key $K_{ch[I]}$. And then, the Inceptive UPTU concatenates it with the Device Public Key $KP_{d[I]}$ and encrypts the data with Device Class Public Key $KP_{dc[P]}$. Moreover, the Inceptive UPTU concatenates the data with $RDCL_{[I]}$ recorded in the Inceptive Device and encrypts it with the Challenge Key $K_{ch[P]}$. After that, the Inceptive UPTU sends the encrypted data to the Primal UPTU. After receiving it, the Primal UPTU decrypts it with the Challenge Key $K_{ch[P]}$ and its own Device Class Private Key $K_{dc[P]}$ consecutively.
- CS4 First off, the Primal UPTU generates a Session Key $K_{s[P]0}$ and concatenates it with Device Public Key $KP_{d[P]}$. After that, the data is encrypted with the Device Public Key $KP_{d[I]}$. Here, if issue date of $RDCL_{[I]}$ recorded in the Inceptive Device is older than that

of $RDCL_{[P]}$, the Primal UPTU concatenates its own $RDCL_{[P]}$ with the encrypted data mentioned above. Meanwhile, if the date is newer than that of $RDCL_{[P]}$, the Primal UPTU shall replace the $RDCL_{[P]}$ with the received $RDCL_{[I]}$. Next, the Primal UPTU encrypts the data with the Challenge Key $K_{ch[I]}$ and sends the encrypted data to the Inceptive UPTU. After receiving it, the Inceptive UPTU decrypts it with the Challenge Key $K_{ch[I]}$ and the Device Private Key $K_{d[I]}$ consecutively. If a $RDCL_{[P]}$ is included in the received data, the Inceptive UPTU shall replace the $RDCL_{[I]}$ of its own with the $RDCL_{[P]}$ included in the received data.

CS5 The Inceptive UPTU generates a Session Key $K_{s[I]0}$, and encrypts it with the Session Key $K_{s[P]0}$ and the Device Public Key $KP_{d[P]}$. The Primal UPTU sends the encrypted data to the Inceptive UPTU. After receiving it, the Primal UPTU decrypts it with the Device Private Key $K_{d[P]}$ and the Session Key $K_{s[P]0}$ consecutively. As a result, both UPTUs share $K_{s[P]0}$, $K_{s[I]0}$, $*KP_{d[P]}$ and $*KP_{d[I]}$.

6.2.1.2 Primal to Inceptive Transfer Stage

Basic steps for transfer of a Usage Pass from the Primal Device to the Inceptive Device are shown in Figure 6.7. Before entering this stage, the four keys, two Session Keys $K_{s[P]m}$, $K_{s[I]n}$ and two ECDH Shared Keys $*KP_{d[P]}$, $*KP_{d[I]}$ shall be shared between both UPTUs. At the end of this stage, three shared keys, $K_{s[P]m}$, $*KP_{d[P]}$ and $*KP_{d[I]}$, are not changed. And shared key $K_{s[I]n}$ is changed to $K_{s[I]n+1}$.

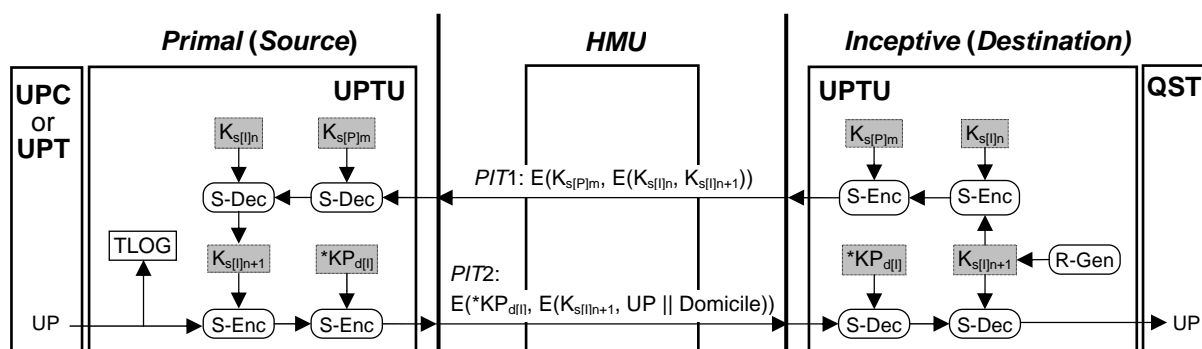


Figure 6.7 Basic steps of BT mode for transfer of a Usage Pass to an Inceptive Device

[Primal to Inceptive Transfer Stage]

PIT1 The Inceptive UPTU generates the Session Key $K_{s[I]n+1}$, and encrypts it with the Session Key $K_{s[I]n}$ and the Session Key $K_{s[P]m}$ consecutively. The Inceptive UPTU sends the encrypted data to the Primal UPTU. After receiving it, the Primal UPTU decrypts it with the Session Key $K_{s[P]m}$ and the Session Key $K_{s[I]n}$.

PIT2 The Primal UPTU concatenates a Usage Pass with Domicile to write it into the Inceptive QST. The Primal UPTU encrypts the concatenated data with the Session Key $K_{s[I]n+1}$ and the ECDH Shared Key $*KP_{d[I]}$ consecutively. The Primal UPTU sends the encrypted Usage Pass to the Inceptive UPTU and records a Transaction Log. After receiving it, the Inceptive UPTU decrypts it with the ECDH Shared Key $*KP_{d[I]}$

and the Session Key $K_{s[l]n+1}$ consecutively. The Usage Pass is written in the area of QST designated by Domicile.

6.2.1.3 Inceptive to Primal Transfer Stage

Basic steps for transfer of a Usage Pass from the Inceptive Device to the Primal Device are shown in Figure 6.8. Before entering this stage, the four keys, two Session Keys $K_{s[p]m}$, $K_{s[l]n}$, and two ECDH Shared Keys $*KP_{d[p]}$, $*KP_{d[l]}$ shall be shared between both UPTUs. At the end of this stage, three shared keys, $K_{s[l]n}$, $*KP_{d[p]}$ and $*KP_{d[l]}$, are not changed. And shared key $K_{s[p]m}$ is changed to $K_{s[p]m+1}$.

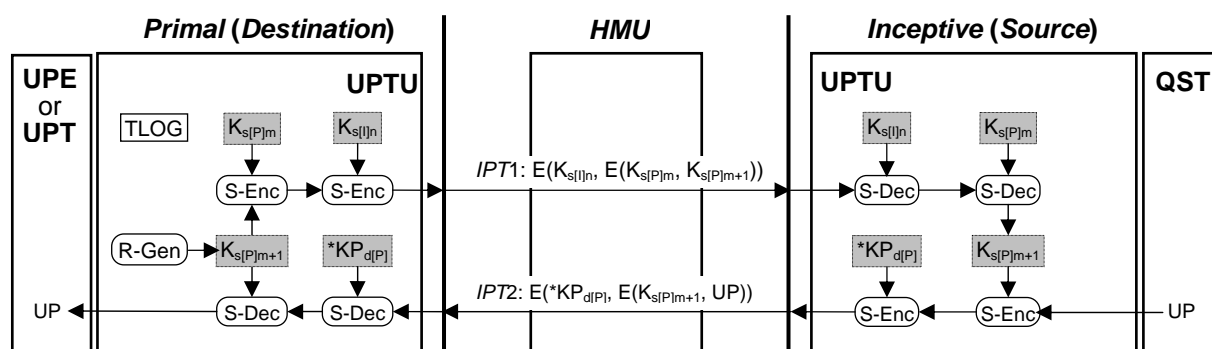


Figure 6.8 Basic steps of BT mode for transfer of a Usage Pass to a Primal Device

[Inceptive to Primal Transfer Stage]

- IPT1*** The Primal UPTU generates the Session Key $K_{s[p]m+1}$, and encrypts it with the Session Key $K_{s[p]m}$ and the Session Key $K_{s[l]n}$ consecutively. The Primal UPTU sends the encrypted data to the Inceptive UPTU and starts to record a Transaction Log. After receiving it, the Inceptive UPTU decrypts it with the Session Key $K_{s[l]n}$ and the Session Key $K_{s[p]m}$.
- IPT2*** The Inceptive UPTU encrypts a Usage Pass with the Session Key $K_{s[p]m+1}$ and the ECDH Shared Key $*KP_{d[p]}$ consecutively. The Inceptive UPTU sends the encrypted Usage Pass to the Primal UPTU. After receiving it, the Primal UPTU decrypts it with the ECDH Shared Key $*KP_{d[p]}$ and the Session Key $K_{s[p]m+1}$ consecutively, and completes to record the Transaction Log.

6.2.2 Additional steps

Additional steps consist of four stages: (1) Reconnection Stage where a Primal UPTU and an Inceptive UPTU share new Session Keys and ECDH Shared Keys with the Session Keys recorded in the Connection Log, (2) two types of Recovery Stage where the Usage Pass is recovered to the pre-transferred one in the Primal Device or Inceptive Device (3) Usage Pass Inquiry Stage where Primal Device check a Usage Pass recorded in Inceptive Device.

6.2.2.1 Reconnection Stage

Additional steps for reconnection are shown in Figure 6.9. Before entering this stage, Session Keys $K_{s[I]CL}$ and $K_{s[P]CL}$ shall be recorded in Connection Log of both UPTUs.

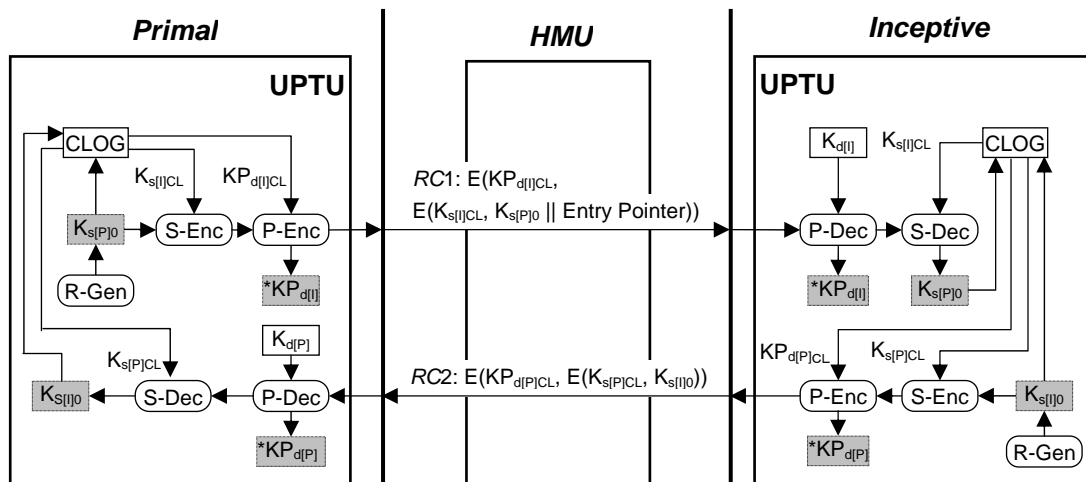


Figure 6.9 Additional steps of BT mode for reconnection

[Reconnection Stage]

- RC1** The Primal UPTU generates a Session Key $K_{s[P]0}$ and concatenates it with Entry Pointer to designate the entry of Connection Log in the Inceptive UPTU. The Inceptive UPTU encrypts the concatenated data with the Session Key $K_{s[I]CL}$ and the Device Public Key $KP_{d[I]CL}$ recorded in its own Connection Log consecutively. The Primal UPTU sends the encrypted data to the Inceptive UPTU. After receiving it, the Inceptive UPTU decrypts it with its own Device Private Key $K_{d[I]}$ and the Session Key $K_{s[I]CL}$ consecutively.
- RC2** The Inceptive UPTU generates a Session Key $K_{s[I]0}$, and encrypts it with the Session Key $K_{s[P]CL}$ and the Device Public Key $KP_{d[P]CL}$ recorded in the entry designated by Entry Pointer consecutively. The Inceptive UPTU sends the encrypted data to Primal UPTU. After receiving it, Primal UPTU decrypts it with the Device Private Key $K_{d[P]}$ and the Session Key $K_{s[P]CL}$ consecutively. As a result, both UPTUs share new Session Keys $K_{s[P]0}$, $K_{s[I]0}$ and new ECDH Shared Keys $*KP_{d[P]}$, $*KP_{d[I]}$.

6.2.2.2 Primal to Inceptive Recovery Stage

Additional steps for recovery of a Usage Pass in the Primal Device are shown in Figure 6.10. Before entering this stage, (1) Transaction Log of Primal UPTU shall be recorded, (2) the four keys, Session Keys $K_{s[P]m}$, $K_{s[I]n}$ and ECDH Shared Keys $*KP_{d[P]}$, $*KP_{d[I]}$, shall be shared between Primal UPTU and Inceptive UPTU. At the end of this stage, four shared keys are not changed.

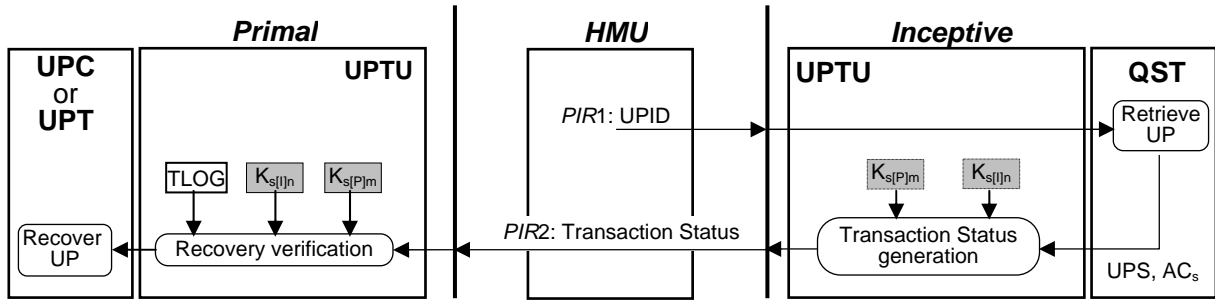


Figure 6.10 Additional steps of BT mode for recovery of Usage Pass in Primal Device

[Primal to Inceptive Recovery Stage]

- PIR1** The HMU sends UPID of the Usage Pass to be recovered to the Inceptive UPTU. The Inceptive UPTU receives the UPID and search the QST for the Usage Pass with the UPID and determine the Usage Pass Status. After that, UPID, Access Condition of the Usage Pass with the UPID, and the Usage Pass Status are concatenated. Hash value is calculated from the concatenated data, $K_{s[P]m}$, and $K_{s[I]n}$. The concatenated data and the hash value are concatenated and called Transaction Status.
- PIR2** The Inceptive UPTU sends the Transaction Status to the Primal UPTU. After receiving it, the Primal UPTU verifies the Transaction Status. If the objective Usage Pass has already been moved or the Access Condition has already been changed, the Primal UPTU recovers the Usage Pass.

6.2.2.3 Inceptive to Primal Recovery Stage

Additional steps for recovery of a Usage Pass in the Inceptive Device as Source are shown in Figure 6.11. Before entering this stage, (1) Transaction Log of Primal UPTU shall be recorded, (2) the four keys, Session Keys $K_{s[P]m}$, $K_{s[I]n}$ and ECDH Shared Keys $*KP_{d[P]}$, $*KP_{d[I]}$, shall be shared between Primal UPTU and Inceptive UPTU. At the end of this stage, three shared keys, $K_{s[P]m}$, $*KP_{d[P]}$ and $*KP_{d[I]}$, are not changed. And shared key $K_{s[I]n}$ is changed to $K_{s[I]n+1}$.

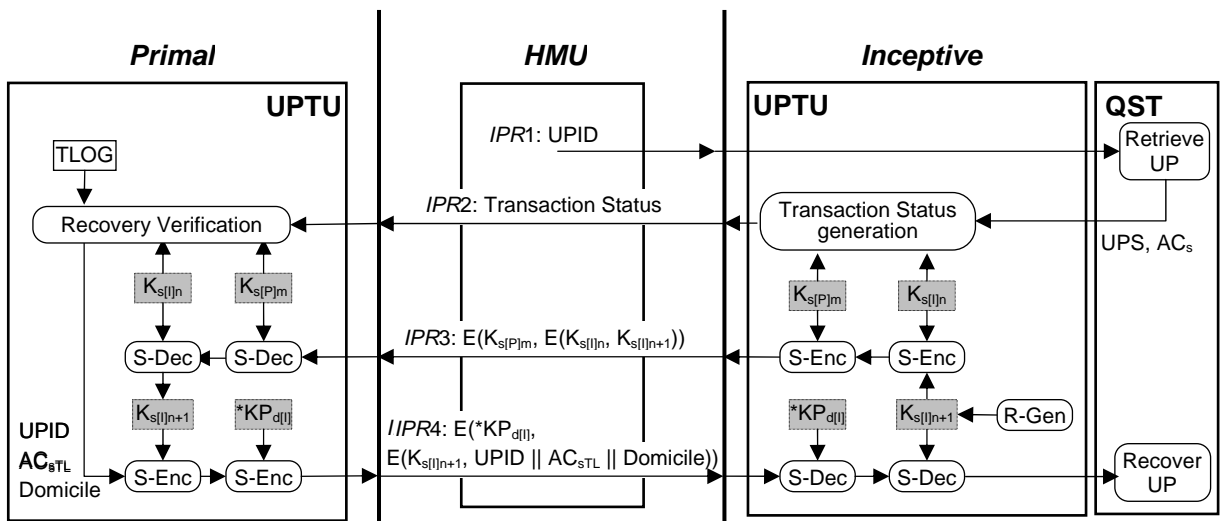


Figure 6.11 Additional steps of BT mode for recovery of Usage Pass in Inceptive Device

[Inceptive to Primal Recovery Stage]

- IPR1* Same as *PIR1* of Primal to Inceptive Recovery Stage in BT mode.
- IPR2* The Inceptive UPTU sends the Transaction Status to the Primal UPTU. After receiving it, the Primal UPTU verifies the Transaction Status. Unless the objective Usage Pass has already been moved or the Access Condition has already been changed, the Primal UPTU shall quit the Inceptive to Primal Recovery Stage.
- IPR3* Same as *PIT1* of Primal to Inceptive Transfer Stage in BT mode.
- IPR4* The Primal UPTU concatenates the UPID with the Access Condition of the Usage Pass with the UPID and Domicile in Transaction Log. The Primal UPTU encrypts the concatenated data with the Session Key $K_{s[[]]n+1}$ and the ECDH Shared Key $*KP_{d[[]]}$ consecutively. The Primal UPTU sends the encrypted data to the Inceptive UPTU. After receiving it, the Inceptive UPTU decrypts it with the ECDH Shared Key $*KP_{d[[]]}$ and the Session Key $K_{s[[]]n+1}$ consecutively. The Inceptive UPTU restores the Access Condition according to the received one at the area of QST designated by Domicile.

6.2.2.4 Usage Pass Inquiry Stage

Additional steps for inquiry of Usage Pass in an Inceptive Device are shown in Figure 6.12. The Inceptive UPTU may send a Masked Usage Pass to the Primal UPTU. The Primal UPTU inquires and confirms UPID and the Access Condition of the Usage Pass to be transferred from the Inceptive UPTU, and records it to Transaction Log. Before entering this stage, the four keys, Session Keys $K_{s[P]m}$, $K_{s[[]]n}$ and ECDH Shared Keys $*KP_{d[P]}$, $*KP_{d[[]]}$, shall be shared between both UPTUs. At the end of this stage, four shared keys are not changed.



Figure 6.12 Basic steps of BT mode for inquiry of a Usage Pass in Inceptive Device

[Usage Pass Inquiry Stage]

- UPI* The Inceptive UPTU calculates keyed hash from a Masked Usage Pass. It is called Masked Usage Pass. The Session Key $K_{s[[]]n}$ and $K_{s[P]m}$ are used as the keyed hash calculation. The Inceptive UPTU sends the Masked Usage Pass with the keyed hash to the Primal UPTU. The Primal UPTU verifies the masked Usage Pass and records it to Transaction Log. This step is optional.

Note that Inceptive UPTU may send a masked Usage Pass without keyed hash to HMU.

7 Usage Pass

This chapter describes the structure of Usage Pass. It is shown in Table 7.1. The structure shall comply with the ASN.1 DER which is specified in X680 and X690.

Table 7.1 Structure of Usage Pass

BP	Length	Field	Value
0	1	tag	Usage Pass tag (6Ah)
1	3	size	82014Eh
4	1	structure_ identifier	tag StructureIdentifier tag (40h)
5	1		size 0Eh
6	14		data Usage Pass Format.
20	1	up_ identifier	tag UPassIdentifier tag (41h)
21	1		size 20h
22	32		data Usage Pass Identifier
54	1	ac_ storage	tag Acs tag (42h)
55	1		size 10h
56	16		data Access Condition for Storage Module (AC _s)
72	1	cipher_ info	tag CipherInformation tag (43h)
73	1		size 41h
74	65		data Cipher Information of Content (CIC)
139	1	ac_ export	tag Ace tag (44h)
140	2		size 8180h
142	128		data Access Condition for Export Module (AC _e)
270	1	cont_ identifier	tag ContentIdentifier tag (45h)
271	1		size 20h
272	32		data Content Identifier
304	1	copyright_ info	tag CopyrightInformation tag (46h)
305	1		size 20h
306	32		data Copyright Information

7.1 Usage Pass Format

The structure of Usage Pass Format is shown in Table 7.2. The size is 14-byte.

Table 7.2 Usage Pass Format

BP \ bit	7	6	5	4	3	2	1	0
0	(MSB)							
...	Name							
4								
5	Reserved			(MSB)		Version		(LSB)
6	(MSB)							
...	Type Map							
13								

7.1.1 Name

Name shall be set to “SAFIA” whose character codes are specified ISO/IEC646.

7.1.2 Version

Version shall be set to 1h.

7.1.3 Type Map

Type Map shall be set a bitmap to indicate the Usage Pass Type (PT) where the Usage Pass belongs.

Table 7.3 Type Map of Usage Pass Format

BP \ bit	7	6	5	4	3	2	1	0
0	PT7	PT6	PT5	PT4	PT3	PT2	PT1	PT0
1	PT15	PT14	PT13	PT12	PT11	PT10	PT9	PT8
...	...							
7	PT63	PT62	PT61	PT60	PT59	PT58	PT57	PT56

When PT_x (x = 0, ..., 63) is set to 1b, the Usage Pass belongs to Usage Pass Type x. When PT_x is set to 0b, it does not belong to Usage Pass Type x. Behavior based on Usage Pass Type is defined in the following. Information on the supported Usage Pass Type is included in Device Class Certificate of each Device.

[Storage Module]

Before a Usage Pass is output from a Storage Module, the Storage Module shall compare Usage Pass Type of the Usage Pass with Acceptable Usage Pass Type of Destination Device. The Storage Module shall not transfer the Usage Pass to Destination Device if the Usage Pass Type is not supported by the Destination Device.

[Transmit Module]

Before a Usage Pass is output from a Transmit Module, the Transmit Module shall compare Usage Pass Type of the Usage Pass with Acceptable Usage Pass Type of Destination Device. The Transmit Module shall not transfer the Usage Pass to Destination Device if the Usage Pass Type is not supported by the Destination Device as long as the special exceptions are not determined.

7.2 Usage Pass Identifier

Usage Pass Identifier is assigned uniquely to each Usage Pass in the SAFIA Security Domain. The size of Usage Pass Identifier is 32-byte.

Table 7.4 Usage Pass Identifier

BP \ bit	7	6	5	4	3	2	1	0
0	Reserved				(MSB)	Version		(LSB)
1	Reserved		(MSB)	Type			(LSB)	
2	(MSB) Reserved (LSB)							
3								
4								
5								
5	(MSB) Adapter Number (LSB)							
6								
7								
8	(MSB) Number (LSB)							
...								
...								
31								

7.2.1 Version

Version is described in SAFIA Specification for each application.

7.2.2 Type

Type is described in SAFIA Specification for each application.

7.2.3 Adapter Number

Adapter number is uniquely assigned to each adapter. 00h shall be set to most significant byte. Binary Coded Decimal of Licensee ID shall be set to the following 2-byte.

7.2.4 Number

Number shall be uniquely assigned to each Usage Pass.

7.3 Access Condition for Storage Module (AC_s)

AC_s is the information to control the output of Usage Pass in a Storage Device. The AC_s is comprised of Control Count and Move Control for Storage Module. The size of AC_s is 16-byte.

Table 7.5 Access Condition for Storage Module

BP \ bit	7	6	5	4	3	2	1	0
0	Control Count							
1	Move Control for Storage Module		Not used					
2	Not used							
...								
15								

7.3.1 Control Count

Structure of Control Count is shown in Table 7.6.

Table 7.6 Control Count

bit BP	7	6	5	4	3	2	1	0
0	(MSB) FM (LSB)		Not used		(MSB)	COUNT		(LSB)

COUNT indicates different rules according to the value of FM as shown in Table 7.7.

Table 7.7 Function of COUNT

Value of FM	Description
00b	Generation Count
01b	Copy Count
10b	Play Count
11b	Not used

Output of a Usage Pass of which FM is “Not used (11b)” from a Storage Module shall be prohibited.

7.3.1.1 Generation Count

Generation Count is the permitted order of generation of Usage Pass Copy.

Table 7.8 Generation Count

Value of COUNT	Description
0h	No more copy
1h	One generation
2h	Two generations
3h, ..., Eh	Not used
Fh	Not asserted

[Import Module]

Creation of a Usage Pass of which FM is “Generation Count (00b)” and COUNT is “One generation (1h)”, “Two generations (2h)” and “Not asserted (Fh)” is allowed. When a content with the Usage Information including copy restriction in terms of the order of generation is imported, UPC shall convert the Usage Information (especially as copy control information) into Generation Count. When the created Usage Pass is output from the Import Module, the Usage Pass in the UPC shall be invalidated.

[Storage Module]

Output of a recorded Usage Pass of which FM is “Generation Count (00b)” from a Storage Module and recording a received similar Usage Pass to the QST follow the below description.

- No more copy

Output of this Usage Pass through Usage Pass Copy and Usage Pass Play are allowed. A Usage Pass duplicated from the one recorded in the QST is transferred to the Destination Device.

This value shall not be changed in the QST.

Output of this Usage Pass through Usage Pass Move is allowed. A new Usage Pass of which this value is “One generation (1h)” is created in the QSTC. In the details, The Usage Pass is duplicated from the one recorded in the QST. And this value of the duplicated Usage Pass is changed to “One generation (1h)”. Then, the Usage Pass in the QST shall be invalidated. After that, the created Usage Pass is transferred to the Destination Device.

When a Storage Module receives this Usage Pass, the Storage Module shall not record it to the QST.

- One generation

Output of this Usage Pass through Usage Pass Copy and Usage Pass Play are allowed. A Usage Pass duplicated from the one recorded in the QST is transferred to the Destination Device. This value shall not be changed in the QST.

Output of this Usage Pass through Usage Pass Move is allowed. A new Usage Pass of which this value is “Two generations (2h)” is created in the QSTC. In the details, the Usage Pass is duplicated from the one recorded in the QST. And this value of the duplicated Usage Pass is changed to “Two generations (2h)”. Then, the Usage Pass in the QST shall be invalidated. After that, the created Usage Pass is transferred to the Destination Device.

When a Storage Module receives this Usage Pass, the Storage Module shall record it to the QST as “No more copy (0h)”.

- Two generations

A Usage Pass of which this value is “Two generations (2h)” shall not exist in the Storage Module. If such a Usage Pass exists, Output of this Usage Pass through Usage Pass Copy, Usage Pass Move, and Usage Pass Play shall be prohibited.

When a Storage Module receives this Usage Pass, the Storage Module shall record it to the QST as “One generation (1h)”.

- Not asserted

Output of this Usage Pass through Usage Pass Copy, Usage Pass Move and Usage Pass Play are allowed. A Usage Pass duplicated from the one recorded in the QST is transferred to the Destination Device. This value of the recorded Usage Pass shall not be changed. In case of Usage Pass Move, the recorded Usage Pass shall not be invalidated.

When a Storage Module receives this Usage Pass, the Storage Module shall record it to the QST as it is.

[Export Module]

UPE shall convert the value of Generation Count into the Usage Information (especially as copy control information) to comply with the other Security Domain. Then, the content is exported with the Usage Information. After that, the received Usage Pass in the UPE shall be invalidated. If the value can not be converted, export shall be prohibited.

[Transmit Module]

Transmitting of the received Usage Pass of which FM is “Generation Count (00b)” from a Source Storage Device to the Destination Storage Device follows the below description.

- No more copy
Transmitting shall be prohibited.
- One generation, Two generation and Not asserted
UPT shall transmit the received Usage Pass to the Destination Device as it is. When the Usage Pass is output from the Transmit Module, the Usage Pass in the UPT shall be invalidated.

Table 7.9 Control rule of Generation Count for functional modules

Module			Generation Count (FM = 00b) of imported /recorded / received Usage Pass				
Name	Role	Action	No more copy	One generation	Two generation	Not asserted	Not used
Import	Source	-	Prohibited	Allowed ^{*1} FM=00b One generation	Allowed ^{*1} FM = 00b Two generation	Allowed ^{*1} FM = 00b Not asserted	Prohibited
Storage	Destination	-	Prohibited	Allowed ^{*2} FM = 00b No more copy	Allowed ^{*2} FM= 00b One generation	Allowed ^{*2} FM = 00b Not asserted	Prohibited
	Source	UP Copy	Allowed ^{*3} FM = 00b No more copy	Allowed ^{*3} FM = 00b One generation	Prohibited	Allowed ^{*3} FM = 00b Not asserted	Prohibited
		UP Move	Allowed ^{*4} FM = 00b One generation	Allowed ^{*4} FM=00b Two generation	Prohibited	Allowed ^{*7} FM = 00b Not asserted	Prohibited
		UP Play	Allowed ^{*3} FM = 00b No more copy	Allowed ^{*3} FM = 00b One generation	Prohibited	Allowed ^{*3} FM = 00b Not asserted	Prohibited
Export	Destination	-	Allowed ^{*5} FM = 00b No more copy	Allowed ^{*5} FM = 00b One generation	Allowed ^{*5} FM = 00b Two generation	Allowed ^{*5} FM = 00b Not asserted	Prohibited
Transmit	Destination / Source	-	Prohibited	Allowed ^{*6} FM = 00b One generation	Allowed ^{*6} FM = 00b Two generation	Allowed ^{*6} FM = 00b Not asserted	Prohibited

- *1: Converting the Usage Information (especially as copy control information) conforming to other Security Domain into Generation Count in the SAFIA Security Domain.
- *2: Record of the received Usage Pass.
- *3: Transfer of the recorded Usage Pass.
- *4: Transfer of the recorded Usage Pass. The Usage Pass in the Storage Device shall be invalidated.
- *5: Converting Generation Count into the Usage Information conforming to other Security Domain.
- *6: Transfer of the received Usage Pass from a Storage Device to another.
- *7: Transfer of the recorded Usage Pass. The Usage Pass in the Storage Device shall not be invalidated.

7.3.1.2 Copy Count

Copy Count is the permitted times of Usage Pass Copy.

Table 7.10 Copy Count

Value of COUNT	Description
0h	No more copy
1h, ..., Eh	Permitted times
Fh	Not asserted

[Import Module]

Creation of a Usage Pass of which FM is “Copy Count (01b)” and COUNT is “Permitted times (1h, ...,Eh)” and “Not asserted (Fh)” is allowed. When a content with the Usage Information including copy restriction in terms of the number of times is imported, UPC of Import Module shall convert the Usage Information into Copy Count. When the created Usage Pass is output from the Import Module, the Usage Pass in the UPC shall be invalidated.

[Storage Module]

Output of a recorded Usage Pass of which FM is “Copy Count (01b)” from a Storage Module and recording a received similar Usage Pass to the QST follow the below description.

- No more copy

Output of this Usage Pass through Usage Pass Copy shall be prohibited.

Output of this Usage Pass through Usage Pass Move is allowed. A new Usage Pass of which FM is set to “Generation Count (00b)” and COUNT is set to “One generation (1h)” is created in the QSTC. In the details, The Usage Pass is duplicated from the recorded Usage Pass in the QST. And FM and COUNT of the duplicated Usage Pass are changed to each of “Generation Count (00b)” and “One generation (1h)”. Then, the recorded Usage Pass shall be invalidated. After that, the created Usage Pass is transferred to the Destination Device.

Output of this Usage Pass through Usage Pass Play is allowed. A Usage Pass duplicated from the recorded Usage Pass is transferred to the Destination Device. This value of the recorded Usage Pass shall not be changed.

When a Storage Module receives this Usage Pass, the Storage Module shall not record it to the QST.

- Permitted times

Output of this Usage Pass through Usage Pass Copy is allowed. A new Usage Pass of which FM is set to “Generation Count (00b)” and COUNT is set to “One generation (1h)” is created in the QSTC. In details, the Usage Pass is duplicated from the one recorded in the QST. And FM and COUNT of the duplicated Usage Pass are changed to each of “Generation Count (00b)” and “One generation (1h)”. Then, this value of the recoded Usage Pass in the QST shall be decremented by one. After that, the created Usage Pass is transferred to the Destination Device.

Output of this Usage Pass through Usage Pass Move is allowed. COUNT of the output Usage Pass created in QSTC is set to a value less than or equal to the COUNT of the recorded Usage Pass in the QST. Values or status of the output Usage Pass other than COUNT are duplicated from the recorded Usage Pass. After that, the created Usage Pass is transferred to the Destination

Device. In the case that the COUNT of the output Usage Pass is equal to the COUNT of the recorded Usage Pass, the recorded Usage Pass in the QST shall be invalidated. In the other case, COUNT of the recorded Usage Pass shall be updated as follows: (Updated COUNT) = (Recorded COUNT) – ((Output COUNT) + 1).

Transfer of this Usage Pass through Usage Pass Play is allowed. A new Usage Pass of which this value is set to “No more copy (0h)” is created in the QSTC. In the details, the Usage Pass is duplicated from the one recorded in the QST. And this value of the duplicated Usage Pass is changed to “No more copy (0h)”. Then, the created Usage Pass is transferred to the Destination Device. This value of the recorded Usage Pass shall not be changed.

When a Storage Module receives this Usage Pass, the Storage Module shall record it to the QST as it is.

- Not asserted

Output of this Usage Pass through Usage Pass Copy, Usage Pass Move and Usage Pass Play are allowed. A Usage Pass duplicated from the one recorded in the QST is transferred to the Destination Device. This value shall not be changed in the QST. In case of Usage Pass Move, the recorded Usage Pass shall not be invalidated.

When a Storage Module receives this Usage Pass, the Storage Module shall record it to the QST as it is.

[Export Module]

UPE shall convert the value of Copy Count of the received Usage Pass into the Usage Information (especially as copy control information) to comply with the other Security Domain. Then, the content is exported with the Usage Information. After that, the Usage Pass in the UPE shall be invalidated. If the value can not be converted, export is prohibited.

[Transmit Module]

Transmitting of the received Usage Pass of which FM is “Copy Count” from the Source Storage Device to the Destination Storage Device follows the below description.

- No more copy

Transmitting shall be prohibited.

- Permitted times and Not asserted

UPT shall transmit the received Usage Pass to the Destination Storage Device as it is. When the Usage Pass is output from the Transmit Module, the Usage Pass in the UPT shall be invalidated.

Table 7.11 Control rule of Copy Count for functional modules

Module			Copy Count (FM = 01b) of imported / recorded / received Usage Pass					Not asserted
Name	Role	Action	No more copy	Permitted times			Eh	
				1h	2h	...		
Import	Source	-	Prohibited	Allowed ^{*1} FM = 01b Permitted times = 1h	Allowed ^{*1} FM = 01b Permitted times = 2h	...	Allowed ^{*1} FM = 01b Permitted times = Eh	Allowed ^{*1} FM = 01b Not asserted
Storage	Destination	-	Prohibited	Allowed ^{*2} FM = 01b Permitted times = 1h	Allowed ^{*2} FM = 01b Permitted times = 2h	...	Allowed ^{*2} FM = 01b Permitted times = Eh	Allowed ^{*2} FM = 01b Not asserted
	Source	UP Copy	Prohibited	Allowed ^{*4} FM = 00b One generation	←	...	←	Allowed ^{*3} FM = 01b Not asserted
		UP Move	Allowed ^{*5} FM = 00b One generation	Allowed ^{*9} FM = 01b Permitted times = 1h	Allowed ^{*9} FM = 01b Permitted times = 1h, 2h	...	Allowed ^{*9} FM = 01b Permitted times = 1h, ..., Eh	Allowed ^{*8} FM = 01b Not asserted
		UP Play	Allowed ^{*3} FM = 01b No more copy	←	←	...	←	Allowed ^{*3} FM = 01b Not asserted
Export	Destination	-	Allowed ^{*6} FM = 01b No more copy	Allowed ^{*6} FM = 01b Permitted times = 1h	Allowed ^{*6} FM = 01b Permitted times = 2h	...	Allowed ^{*6} FM = 01b Permitted times = Eh	Allowed ^{*6} FM = 01b Not asserted
Transmit	Destination / Source	-	Prohibited	Allowed ^{*7} FM = 01b Permitted times = 1h	Allowed ^{*7} FM = 01b Permitted times = 2h	...	Allowed ^{*7} FM = 01b Permitted times = Eh	Allowed ^{*7} FM = 01b Not asserted

- *1: Converting the Usage Information conforming to other Security Domain into Copy Count in the SAFIA Security Domain.
- *2: Record of the received Usage Pass.
- *3: Output of the recorded Usage Pass.
- *4: Output of the recorded Usage Pass. Copy Count of the Usage Pass in the Storage Device shall be decremented by one.
- *5: Output of the recorded Usage Pass. The Usage Pass in the Storage Device shall be invalidated.
- *6: Converting Copy Count into the Usage Information conforming to other Security Domain.
- *7: Transfer of the received Usage Pass from a Storage Device to another.
- *8: Output of the recorded Usage Pass. The Usage Pass in the Storage Device shall not be invalidated.
- *9: Output of the recorded Usage Pass. The Usage Pass in the Storage Device shall be invalidated in case that Copy Count of the recorded Usage Pass is same as the Copy Count of the output Usage Pass.

7.3.1.3 Play Count

Play Count is the permitted times of playback.

Table 7.12 Play Count

Value of COUNT	Description
0h	No more playback
1h	One time playback
2h, ..., Eh	Permitted times
Fh	Not asserted

[Import Module]

Creation of a Usage Pass of which FM is “Play Count (10b)” and COUNT is “One time playback (1h)”, “Permitted times (2h, ..., Eh)” and “Not asserted (Fh)” is allowed. When a content with the Usage Information including playback restriction in terms of the number of times is imported, UPC of Import Module shall convert the Usage Information into Play Count. When the created Usage Pass is output from the Import Module, the Usage Pass in the UPC shall be invalidated.

[Storage Module]

Output of a Usage Pass of which FM is “Play Count (10b)” from a Storage Device and recording a similar Usage Pass to the QST follow the below description.

- No more playback

Output of this Usage Pass through Usage Pass Copy, Usage Pass Move and Usage Pass Play shall be prohibited.

When a Storage Module receives this Usage Pass, the Storage Module shall not record it to the QST.

- One time playback

Output of this Usage Pass through Usage Pass Copy and Usage Pass Move shall be prohibited.

Output of this Usage Pass through Usage Pass Play is allowed. A new Usage Pass of which FM is set to “Generation Count (00b)” and COUNT is set to “No more copy (0h)” is created in the QSTC. In the details, The Usage Pass is duplicated from the one recorded in the QST. And FM and COUNT of the duplicated Usage Pass are changed to each of “Generation Count (00b)” and “No more copy (0h)”. Then, this value of Usage Pass remaining in the QST shall be set to “No more playback”. After that, the created Usage Pass is transferred to the Destination Device.

When a Storage Module receives this Usage Pass, the Storage Device shall record it to the QST as it is.

- Permitted times

Output of this Usage Pass through Usage Pass Copy shall be prohibited.

Output of this Usage Pass through Usage Pass Move is allowed. A new Usage Pass of which this value is decremented by one is created in the QSTC. In the details, the Usage Pass is duplicated from the one recorded in the QST. And this value of the duplicated Usage Pass is decremented one. Then, the Usage Pass remaining in the QST shall be invalidated. After that, the created Usage Pass in the QSTC is transferred to the Destination Device.

Output of this Usage Pass through Usage Pass Play is allowed. A new Usage Pass of which FM is set to “Generation Count (00b)” and COUNT is set to “No more copy (0h)” is created in the QSTC. In the details, The Usage Pass is duplicated from the one recorded in the QST. And FM and COUNT of the duplicated Usage Pass are changed to each of “Generation Count (00b)” and “No more copy (0h)”. Then, this value of the Usage Pass remaining in the QST shall be decremented by one. After that, the created Usage Pass is transferred to the Destination Device.

When a Storage Module receives a Usage Pass of which this value is “Permitted times (1h, ..., Eh)”, the Storage Module shall record it to the QST as it is.

- Not asserted

Output of this Usage Pass through Usage Pass Copy, Usage Pass Move and Usage Pass Play are allowed. A Usage Pass duplicated from the one recorded in the QST is transferred to the Destination Device. This value shall not be changed in the QST. In case of Usage Pass Move, the Usage Pass shall not be invalidated in the QST.

When a Storage Module receives this Usage Pass, the Storage Module shall record it to the QST as it is.

[Export Module]

Exporting of content with a Usage Pass of which FM is “Play Count (10b)” follows the below description.

- No more copy and Permitted times = Eh

Exporting shall be prohibited.

- Permitted times = 2h, ..., Dh and Not asserted

UPE shall convert the value of Play Count into the Usage Information to comply with the other Security Domain. Then, the content is exported with the Usage Information. After that, the Usage Pass in the UPE shall be invalidated. If the value can not be converted, export is prohibited.

[Transmit Module]

Transmitting of the received Usage Pass of which FM is “Play Count (10b)” from the Source Storage Device to the Destination Storage Device follows the below description.

- No more playback and Permitted times = Eh

Transmitting shall be prohibited.

- One time playback, Permitted times = 2h, ..., Dh and Not asserted

UPT shall transmit the received Usage Pass to the Destination Storage Device as it is. When the Usage Pass is output from the Transmit Module, the Usage Pass in the UPT shall be invalidated.

Table 7.13 Control rule of Play Count for functional modules

Module			Play Count (FM = 10b) of imported / recorded / received Usage Pass							
Name	Role	Action	No more playback	One time playback	Permitted times					Not asserted
					2h	3h	...	Dh	Eh	
Import	Source	-	Prohibited	Allowed ^{*1} FM = 10b One time playback	Allowed ^{*1} FM = 10b Permitted times = 2h	Allowed ^{*1} FM = 10b Permitted times = 3h	...	Allowed ^{*1} FM = 10b Permitted times = Dh	Allowed ^{*1} FM = 10b Permitted times = Eh	Allowed ^{*1} FM = 10b Not asserted
Storage	Destination	-	Prohibited	Allowed ^{*2} FM = 10b One time playback	Allowed ^{*2} FM = 10b Permitted times = 2h	Allowed ^{*2} FM = 10b Permitted times = 3h	...	Allowed ^{*2} FM = 10b Permitted times = Dh	Allowed ^{*2} FM = 10b Permitted times = Eh	Allowed ^{*2} FM = 10b Not asserted
	Source	UP Copy	Prohibited	←	←	←	...	←	←	Allowed ^{*3} FM = 10b Not asserted
		UP Move	Prohibited	Prohibited	Allowed ^{*4} FM = 10b One time play	Allowed ^{*4} FM = 10b Permitted times = 2h	...	Allowed ^{*4} FM = 10b Permitted times = Ch	Allowed ^{*4} FM = 10b Permitted times = Dh	Allowed ^{*8} FM = 10b Not asserted
		UP Play	Prohibited	Allowed ^{*5} FM = 00h No more copy	←	←	...	←	←	Allowed ^{*3} FM = 10b Not asserted
Export	Destination	-	Prohibited	Allowed ^{*6} FM = 10b One time playback	Allowed ^{*6} FM = 10b Permitted times = 2h	Allowed ^{*6} FM = 10b Permitted times = 3h	...	Allowed ^{*6} FM = 10b Permitted times = Dh	Prohibited	Allowed ^{*6} FM = 10b Not asserted
Transmit	Destination / Source	-	Prohibited	Allowed ^{*7} FM = 10b One time playback	Allowed ^{*7} FM = 10b Permitted times = 2h	Allowed ^{*7} FM = 10b Permitted times = 3h	...	Allowed ^{*7} FM = 10b Permitted times = Dh	Prohibited	Allowed ^{*7} FM = 10b Not asserted

*1: Converting the Usage Information (especially as copy control information) conforming to other Security Domain into Play Count in the SAFIA Security Domain.

*2: Record of the received Usage Pass.

*3: Output of the recorded Usage Pass.

*4: Output of the recorded Usage Pass. The Usage Pass in the Storage Device shall be invalidated.

*5: Output of the recorded Usage Pass. Play Count of the Usage Pass remaining in the Storage Device shall be decremented by one.

*6: Converting Play Count into the Usage Information conforming to other Security Domain.

*7: Transfer of the received Usage Pass from a Storage Device to another.

*8: Output of the recorded Usage Pass. The Usage Pass in the Storage Device shall not be invalidated.

7.3.2 Move Control for Storage Module

Structure of Move Control for Storage Module is shown in Table 7.14.

Table 7.14 Move Control of Storage Module

BP \ bit	7	6
0	MU	MB

7.3.2.1 MU

This bit indicates the permission of the output of Usage Pass through Usage Pass Move in UT mode from a Storage Module.

Table 7.15 MU

Value	Description
0	Usage Pass Move in UT mode is permitted in accordance with Control Count specific rules
1	Usage Pass Move in UT mode is prohibited

7.3.2.2 MB

This bit indicates the permission of the output of Usage Pass through Usage Pass Move in BT mode from a Storage Module.

Table 7.16 MB

Value	Description
0	Usage Pass Move in BT mode is permitted in accordance with Control Count specific rules
1	Usage Pass Move in BT mode is prohibited

7.4 Cipher Information of Content

Cipher Information of Content (CIC) is the information to decrypt a SAFIA Content. Content Key K_c shall be included in it. The size of CIC is 65-byte.

Table 7.17 Cipher Information of Content

BP \ bit	7	6	5	4	3	2	1	0
0	(MSB) Cipher Scheme							(LSB)
1	Content Key							
...								
16								
17	(MSB) Type Specific Cipher Info							(LSB)
...								
64								

7.4.1 Cipher Scheme

Cipher Scheme shall be effective length of the immediate following bytes.

7.4.2 Content Key

Content Key K_c is described in section 5.5.

7.4.3 Type Specific Cipher Info

Type Specific Cipher Info is determined according to Usage Pass Type shown by Usage Pass Format in section 7.1.3. If SAFIA Content is encrypted in CBC mode, initialization vector or seed of initialization vector is included in it.

7.5 Access Condition for Export Device (AC_e)

AC_e is the information to control playback of content in a Content Decryptor. The structure is determined according to Usage Pass Type shown by Usage Pass Format in section 7.1.3. The size of AC_e is 128-byte.

7.6 Content Identifier

Content Identifier is uniquely assigned to every content in the SAFIA Security Domain. The size of Content Identifier is 32-byte.

Table 7.18 Content Identifier

BP \ bit	7	6	5	4	3	2	1	0
0	Reserved				(MSB)	Version		(LSB)
1	Reserved		(MSB)	Type				(LSB)
2	(MSB)							
3	Reserved							
4	(LSB)							
5	(MSB)							
6	Adapter Number							
7	(LSB)							
8	(MSB)							
...	Number							
31	(LSB)							

7.6.1 Version

Version is described in SAFIA Specification for each application.

7.6.2 Type

Type is described in SAFIA Specification for each application.

7.6.3 Adapter Number

Adapter Number is uniquely assigned to each adapter. 00h shall be set to most significant byte. Binary Coded Decimal of Licensee ID shall be set to the following 2-byte.

7.6.4 Number

Number shall be uniquely assigned to each SAFIA Content.

7.7 Copyright Information

Copyright Information is text described with character codes specified in ISO/IEC646. A copyright holder may fill out this information.

8 Device Class Certificate and Revoked Device Class List

A Device Class Certificate and a Revoked Device Class List (RDCL) are given to all Devices when it is manufactured. They are provided by SAFIA License Group. Every Device shall keep the Device Class Certificate and the RDCL in UPTU. Format of Device Class Certificate and RDCL shall comply with X509 and RFC3280.

8.1 Device Class Certificate

Device Class Certificate is the certificate corresponding to a Device Class Public Key and indicating the information of acceptable Usage Pass.

8.2 Format of Device Class Certificate

Device Class Certificate used in this document has three fields of a certificate as specified in X509. They are tbsCertificate, signatureAlgorithm and signatureValue. Three optional fields of tbsCertificate, namely issuerUniqueId, subjectUniqueId and extensions, shall be omitted.

An example of Device Class Certificate is shown in Table 8.1. The length of signatureValue field is variable.

Table 8.1 Device Class Certificate

BP	Length	Field		Value		
0	1	tag		Sequence tag (30h)		
1	3	size		Pk_L + Sv_L + 218; length of the following field (Example – 820180h, when Pk_L = 93 and Sv_L = 73)		
4	1	data	tag	Sequence tag (30h)		
5	3		size	length of data field of tbsCertificate, (Example- 820125h, when Pk_L = 93)		
8	5		tbsCertificate	data	version	see section 8.2.1
13	12				serialNumber	see section 8.2.2
25	14				signature	see section 8.2.3
39	38				issuer	see section 8.2.4
77	36				validity	see section 8.2.5
113	95				subject	see section 8.2.6
208	Pk_L				subjectPublicKeyInfo	see section 8.2.7 Pk_L is the length of this field.
Pk_L + 208	14		signatureAlgorithm		same value of signature of tbsCertificate, see section 8.2.8	
Pk_L + 222	Sv_L (<= 75)	signatureValue		a signature value for tbsCertificate, see section 8.2.9		

8.2.1 version

This field shall be set to v3 (the value is equal to 2).

Table 8.2 version

BP	Length	Field	Value
0	1	tag	[0] (A0h)
1	1	size	03h
2	1	data	tag Integer tag (02h)
3	1		size 01h
4	1		data v3 (02h)

8.2.2 serialNumber

This field shall be set to a serial number. The value shall be from 0100 00000000 00000000h to 7FFF FFFFFFFF FFFFFFFFh. Its length is fixed 10-byte.

Table 8.3 serialNumber

BP	Length	Field	Value
0	1	tag	Integer tag (02h)
1	1	size	0Ah
2	10	data	serial number of this certificate

8.2.3 signature

The ECDSA with SHA-256 algorithm shall be used in this document. This field shall comply with RFC3279 and ID/ECDSA-00. And it is shown in Table 8.4.

Object Identifier of algorithm: iso(1). member-body(2). us(840). ansi-X962(10045). signatures(4). ecdsa-with-SHA2(3). ecdsa-with-SHA256(2)

Parameters of algorithm: NULL

Table 8.4 signature

BP	Length	Field	Value		
0	1	tag	Sequence tag (30h)		
1	1	size	0Ch		
2	1	data	algorithm	tag	Object identifier type tag (06h)
3	1			size	08h
4	8			data	OID:1.2.840.10045.4.3.2 (2A8648CE 3D040302h)
12	1	parameters		tag	Null type tag (05h)
13	1			size	00h

8.2.4 issuer

This field shall be set to only two attribute types shown in the following.

C = “[2-byte character string which stands for a Country Name]”,

O = “[12-byte character string which stands for an Organization Name]”,

These character strings shall consist of ‘0’, ..., ‘9’, ‘A’, ..., ‘Z’, ‘a’, ..., ‘z’, ‘-’, ‘ (space)’ which are specified in ISO/IEC646.

Table 8.5 Issuer

BP	Length	Field			Value			
0	1	tag			Sequence tag (30h)			
1	1	size			24h			
2	1	data	C	tag	Set tag (31h)			
3	1			size	0Bh			
4	1			data	tag	Sequence tag (30h)		
5	1					size	09h	
6	1			data	id	tag	Object identifier tag (06h)	
7	1					size	03h	
8	3					data	OID2.5.4.6 (550406h)	
11	1			data	text	tag	PrintableString tag (13h)	
12	1					size	02h	
13	2					data	described as Country Name	
15	1			data	O	tag	Set tag (31h)	
16	1					size	15h	
17	1					data	tag	Sequence tag (30h)
18	1							size
19	1	data	id			tag	Object identifier tag (06h)	
20	1					size	03h	
21	3					data	OID2.5.4.10 (55040Ah)	
24	1	data	text			tag	PrintableString tag (13h)	
25	1					size	0Ch	
26	12					data	described as Organization Name	

8.2.4.1 Country Name

Country name is information to indicate the nationality of the certification authority. A two-letter ISO3166 country code shall be used.

8.2.4.2 Organization Name

Organization name is information to indicate the certification authority.

8.2.5 validity

The description format of notBefore and notAfter of this field shall be GeneralizedTime, which is specified in X680. The value of notBefore shall be described as date and time of Greenwich Mean Time. When setting the value to this field, second unit shall not be omitted and less than second unit shall be omitted. The value of notAfter shall be fixed to 9999-12-31 23:59:59 in Greenwich Mean Time, namely "99991231235959Z".

Table 8.6 validity

BP	Length	Field		Value	
0	1	tag		Sequence tag (30h)	
1	1	size		22h	
2	1	data	notBefore	tag	GeneralizedTime tag (18h)
3	1			size	0Fh
4	15		data	the issue date of this certificate	
19	1		notAfter	tag	GeneralizedTime tag (18h)
20	1	size		0Fh	
21	15	data		393939 39313233 31323335 3935395Ah	

8.2.6 subject

This field shall be set to only four attribute types shown in the following.

C = “[2-byte character string which stands for a Country Name]”,

O = “[12-byte character string which stands for an Organization Name]”,

CN = “[16-byte character string which stands for a Device Name]”,

DNQ = “[3-byte character string which stands for Device Type Name]” || “[16-byte character string of Acceptable Usage Pass Type Map expressed with hexadecimal value]”

These character strings shall consist of ‘0’, ..., ‘9’, ‘A’, ..., ‘Z’, ‘a’, ..., ‘z’, ‘-’, ‘ ’ (space) which are specified in ISO/IEC646.

Table 8.7 subject

BP	Length	Field	Value		
0	1	tag	Sequence tag (30h)		
1	1	size	5Dh		
2	1	C	tag		
3	1		size		
4	1		data	tag	
5	1			size	
6	1		data	id	tag
7	1				size
8	3			data	
11	1		text	tag	
12	1			size	
13	2			data	
15	1		O	tag	
16	1			size	
17	1			data	tag
18	1	size			
19	1	data		id	tag
20	1				size
21	3			data	
24	1	text		tag	
25	1			size	
26	12			data	
38	1	CN		Tag	
39	1			size	
40	1			data	tag
41	1		size		
42	1		data	id	tag
43	1				size
44	3			data	
47	1		text	tag	
48	1			size	
49	16			data	
65	1		DNQ	Tag	
66	1			Size	
67	1			data	tag
68	1	size			
69	1	data		id	tag
70	1				size
71	3			data	
74	1	text		tag	
75	1			size	
76	19			data	

8.2.6.1 Country Name

Country Name is information to indicate the nationality of the organization which produces the Device. A two-letter ISO3166 country code shall be used.

8.2.6.2 Organization Name

Organization Name is information to indicate the organization which produces the Device.

8.2.6.3 Device Name

Device Name is information to indicate the Device, for example, model name, model number and so forth.

8.2.6.4 Device Type Name

Device Type Name is the information that indicates the functional type of Device,

8.2.6.5 Acceptable Usage Pass Type Map

Acceptable Usage Pass Type Map shown in Table 8.8 is a bitmap to indicate Usage Pass Type which a Device supports.

Table 8.8 Acceptable Usage Pass Type Map

BP \ bit	7	6	5	4	3	2	1	0
0	AT7	AT6	AT5	AT4	AT3	AT2	AT1	AT0
1	AT15	AT14	AT13	AT12	AT11	AT10	AT9	AT8
...								
7	AT63	AT62	AT61	AT60	AT59	AT58	AT57	AT56

When ATx (x = 0, ..., 63) is set to 1b, a Device supports a Usage Pass of Usage Pass Type x. When ATx is set to 0b, The Device does not support a Usage Pass of Usage Pass Type x. Behavior based on Usage Pass Type is described in Section 7.1.3 of this document.

- Example1 - a Host Device which supports the Usage Pass of Usage Pass Type 1.
 Device Type Name = "RP1"

Acceptable Usage Pass Type Map = 0200000000000000h

DNQ = "RP1020000000000000" (character codes are specified in ISO/IEC646)
 = 525031 30323030 30303030 30303030 30303030h

- Example 2 - a Storage Device which supports the Usage Pass of Usage Pass Types 0, ...,47
 Device Type Name = "DRV"

Acceptable Usage Pass Type Map = FFFFFFFF0000h

DNQ = "DRVFFFFFFFF0000" (character codes are specified in ISO/IEC646)
 = 445256 46464646 46464646 46464646 30303030h

8.2.7 subjectPublicKeyInfo

This field shall be set to Device Class Public Key. The detail of this field is not described in this document.

8.2.8 signatureAlgorithm

This field shall be set to same value of signature of tbsCertification.

8.2.9 signatureValue

This field shall be set to value of signature for tbsCertification through ECDSA. This field shall comply with RFC3279. And it is shown in Table 8.9.

Table 8.9 signatureValue

BP	Length	Field	Value		
0	1	tag	Bit string tag (03h)		
1	1	size	$Sv_L - 2 = T_L + S_L + 7$; length of the following data field ($\leq 49h$)		
2	1	data	00h		
3	1		tag	Sequence tag (30h)	
4	1		size	length of total of t and s ($\leq 46h$)	
5	1		t	tag	Integer tag (02h)
6	1			size	T_L ; length of data field of t ($\leq 21h$)
7	T_L			data	signature t
$T_L + 7$	1		s	tag	Integer tag (02h)
$T_L + 8$	1			size	S_L ; length of data field of s ($\leq 21h$)
$T_L + 9$	S_L			data	signature s

8.3 Revoked Device Class List

RDCL is a serial number list of the revoked Device Class Certificate.

8.3.1 Length of Revoked Device Class List

It is the variable length of RDCL. Its maximum length is 8192-byte in SAFIA Security Domain. Every UPTU shall have storage to record RDCL.

8.4 Format of Revoked Device Class List

RDCL used in this document has three fields of a certificate revocation list as specified in X509. They are tbsCertList, signatureAlgorithm and signatureValue. Two optional fields of tbsCertList, namely nextUpdate and nextcrlExtensions shall be omitted.

An example of RDCL is shown in Table 8.10. The values of RL_S , Tc_S , Rc_L and Sv_L are variable.

Table 8.10 RDCL

BP	Length	Field		Value		
0	1	tag		Sequence tag (30h)		
1	RI_S	size		Tc_S+ Rc_L + Sv_L + 89; length of the following data field, (Example - 81CCh, when Tc_S = 1, Rc_L = 41 and Sv_L = 73), The length of this field is a variable value; RI_S.		
RI_S + 1	1	data	tbsCertList	tag	Sequence tag (30h)	
RI_S + 2	Tc_S			size	Rc_L + 74 ; length of data field of tbsCertList (Example - 73h, when Rc_L = 41), The length of this field is a variable value; Tc_S.	
RI_S + Ts_S + 2	5			data	version	see section 8.4.1
RI_S + Ts_S + 7	14				signature	see section 8.4.2
RI_S + Ts_S + 21	38				issuer	see section 8.4.3
RI_S + Ts_S + 59	17				thisUpdate	see section 8.4.4
RI_S + Ts_S + 76	Rc_L				revokedCertificates	see section 8.4.5
RI_S + Ts_S + Rc_L + 76	14			signatureAlgorithm		same value of signature of tbsCertList, see section 8.4.6
RI_S + Ts_S + Rc_L + 90	Sv_L	signatureValue		a signature value for tbsCertList, see section 8.4.7		

8.4.1 version

This field shall be set to v3 (the value is equal to 2). See section 8.2.1.

8.4.2 signature

See section 8.2.3.

8.4.3 issuer

See section 8.2.4.

8.4.4 thisUpdate

The description format of this field shall be GeneralizedTime. The value shall be described as date and time of Greenwich Mean Time. When setting the value to this field, second unit shall not be omitted and less than second unit shall be omitted.

Table 8.11 thisUpdate

BP	Length	Field	Value
0	1	tag	GeneralizedTime tag (18h)
1	1	size	0Fh
2	15	data	the issue date of this RDCL

8.4.5 revokedCertificates

The structure of revokedCertificates is shown Table 8.12.

Table 8.12 revokedCertificates

BP	Length	Field	Value
0	1	tag	Sequence tag (30h)
1	L	size	length of data field (= 13 × N)
L + 1	13	data	revokedCertSerial
...			...
L + 13 × N – 12	13		revokedCertSerial

L: natural number, N: Zero or natural number

In the case where there are two or more revoked certificates, every revokedCertSerial is described sequentially. In the case where there is no revoked certificate, the data field of revokedCertificates is removed.

A revokedCertSerial describes the single serial number or the contiguous plural serial numbers of revoked Device Class Certificate. The structure of revokedCertSerial is shown in Table 8.13. In the case of plural numbers, two revokedCertSerial(s) are used.

Table 8.13 revokedCertSerial

BP	Length	Field	Value
0	1	tag	Integer tag (02h)
1	1	size	0Bh
2	1	data	flag
3	10		serial number

flag = 1: individual serial number

flag = 2: start number of contiguous serial numbers

flag = 3: end number of contiguous serial numbers

The serial number(s) of revokedCertSerial shall be listed in ascending order. Device Class

Certificate of which serial number is listed in revokedCertificates shall be revoked. The start number (flag = 2) shall be paired with the end number (flag = 3). And these numbers shall be described continuously. Device Class Certificate of which serial number is between the start number and the end number shall be revoked.

- Example 1. – No revoked Device Class Certificate.

revokedCertificates =

30 00 : revokedCertificates

- Example 2. – Serial numbers of revoked Device Class Certificates are 0100 00000000 00000001h and 0100 00000000 10000001h to 0100 00000000 FFFFFFFFh.

revokedCertificates =

30 27 : revokedCertificates

02 0B : revokedCertSerial

01 : flag = 1

01 00 00 00 00 00 00 00 00 01 : serial number = 0100 00000000 00000001h

02 0B : revokedCertSerial

02 : flag = 2

01 00 00 00 00 00 10 00 00 01 : start number = 0100 00000000 10000001h

02 0B : revokedCertSerial

03 : flag = 3

01 00 00 00 00 00 FF FF FF FF : end number = 0100 00000000 FFFFFFFFh

8.4.6 signatureAlgorithm

This field shall be set to same value of signature of tbsCertList. See section 8.4.2.

8.4.7 signatureValue

This field shall be set to a value of signature for tbsCertList through ECDSA. See section 8.2.9.

9 Log management

This chapter describes log management. Transaction Log and Connection Log recording is managed by UPTU. Transaction Log is needed to recover Usage Pass when the Usage Pass Transfer does not complete successfully. Connection Log is needed for reconnection of Usage Pass Transfer Protocol. Connection Log is for only BT mode. All entries of Transaction Log for both mode and Connection Log for BT mode shall be invalidated, when RDCL is updated.

9.1 Unidirectional Transfer (UT) mode

In UT mode, only Transaction Log is used.

9.1.1 Transaction Log

If Reconnection Stage and Recovery Stage are supported, both the Primal UPTU and the Inceptive UPTU shall record every Transaction Log corresponding to every Usage Pass Transfer. A Usage Pass Identifier is recorded in each Transaction Log. If a UPTU has plural entries of Transaction Logs of which Usage Pass Identifier are same, only the latest entry of Transaction Log shall be used in Reconnection and Recovery Stage. All entries of Transaction Log in the UPTU shall be invalidated when RDCL is updated in Connection Stage of either UT mode or BT mode.

Information recorded in Transaction Log is shown in Table 9.1. Attribute of a part of Transaction Log is external and the rest is internal. External log is allowed to be output to the outside of the Device and internal log is prohibited to be output to the outside of the Device.

Table 9.1 Information of Transaction Log for UT mode

Information	Attribute	Role
Usage Pass Identifier	External	Primal Inceptive
Type Map	Internal	Primal
Inceptive Device Public Key	Internal	Primal
Inceptive Session Key	Internal	Primal Inceptive
Session Status	External	Primal Inceptive
Original Access Condition	Internal	Primal
Usage Pass Location (Optional)	External	Primal Inceptive

9.1.1.1 Usage Pass Identifier

Usage Pass Identifier is the identifier assigned to each Usage Pass. The identifier is recorded when a Session Key is generated or received at Transfer Stage. Transaction Log is looked up with this identifier.

9.1.1.2 Type Map

Type Map is Acceptable Usage Pass Type Map described in a Device Class Certificate of the Inceptive Device. The data is recorded at the same time when Usage Pass Identifier is recorded.

9.1.1.3 Inceptive Device Public Key

Inceptive Device Public Key is a Device Public Key of the Inceptive Device. The key is recorded at the same time when Usage Pass Identifier is recorded.

9.1.1.4 Inceptive Session Key

Inceptive Session Key is a Session Key generated in the Inceptive UPTU. The key is recorded at the same time when Usage Pass Identifier is recorded.

9.1.1.5 Session Status

Session Status is status information that shows the progress of Usage Pass Transfer. Session Status is 1-byte data shown in Table 9.2.

Table 9.2 Session Status

Status	Abb.	Value	Role	Timing of state transition
Receive Prepared	RP	02h	Inceptive	When a generated Session Key is sent to the Primal UPTU
Receive Completed	RC	03h	Inceptive	When the Usage Pass is received from the Primal UPTU
Send Prepared	SP	04h	Primal	When the Session Key is received from the Inceptive UPTU
Send Completed	SC	05h	Primal	When the Usage Pass is sent to the Inceptive UPTU
UnSpecified	US	00h	Primal/ Inceptive	State other than the above

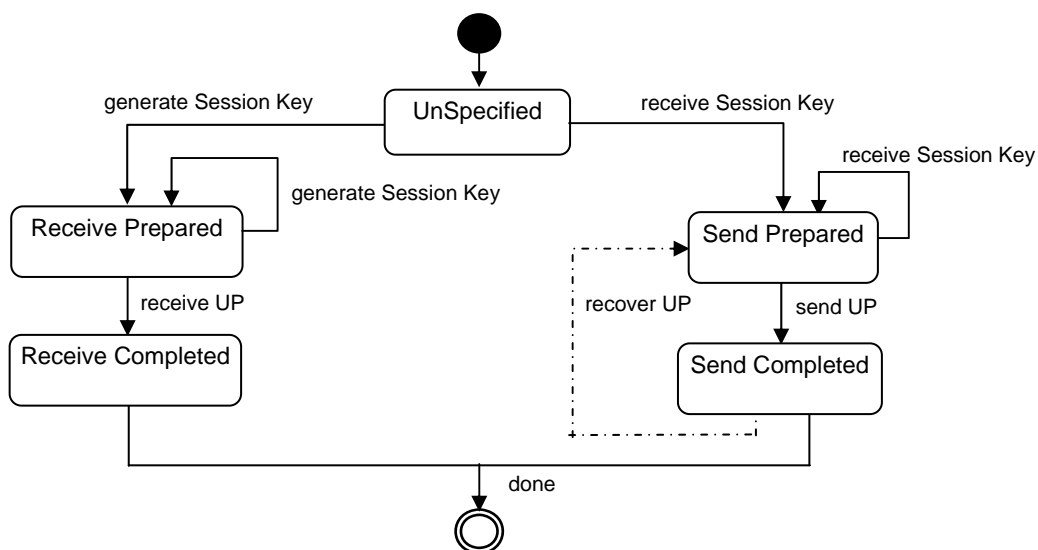


Figure 9.1 State transition diagram of Session Status

9.1.1.6 Original Access Condition

Original Access Condition is AC_s included in the objective Usage Pass that is pre-transferred. The data is recorded at the same time when Usage Pass Identifier is recorded.

9.1.1.7 Usage Pass Location

As for Primal Device, location where Usage Pass is recorded is recorded. As for Inceptive Device, location of Usage Pass to be recorded is recorded. Recording of this data is optional. However, Storage Device shall record it.

9.1.2 Transaction Status

An Inceptive UPTU sends Transaction Status to a Primal UPTU to inform the state of the objective Usage Pass recorded or kept in the Inceptive Device. When the Primal UPTU judges whether the Usage Pass Recovery is allowed, the UPTU uses the Transaction Status. The structure of Transaction Status is as the followings.

Transaction Status ::= UPID || SS || UPS || TstatusHashValue

TstatusHashValue ::= H(tbsTransactionStatus)

tbsTransactionStatus ::= K_{s[P]} || K_{s[I]} || UPID || SS || UPS

UPID : the Usage Pass Identifier of the objective Usage Pass.

Session Status (SS) : Session Status recorded in Transaction Log of the Inceptive UPTU.

Usage Pass Status (UPS) : A status information shown in Table 9.3 of objective Usage Pass recorded in the Inceptive Device.

K_{s[P]}: A Primal Device Session Key that is generated most recently.

K_{s[I]} : An Inceptive Device Session Key recorded in Transaction Log of the Inceptive UPTU.

Table 9.3 Usage Pass Status of Transaction Status

Status	Abb.	Value	Device	Description of the status
Not Exist	NE	FFh	Storage Device	Usage Pass does not exist in QST
			Host Device	Usage Pass is not consumed or not received; if the Usage Pass is kept in the Host Device, this Usage Pass shall be deleted before sending of Transaction Status
Invalid	IVD	01h	Storage Device	Recoverable Usage Pass exists in QST (already moved)
			Host Device	Usage Pass has already been exported or consumed
Valid	VD	00h	Storage Device	Usage Pass exists in QST
			Host Device	Not used

9.1.3 Recovery condition

If the following conditions are satisfied, the Primal UPTU may recover an objective Usage Pass.

- Transaction Log is recorded in Primal UPTU and its Usage Pass Identifier is the same as that in Transaction Status.
- TstatusHashValue of Transaction Status is verified.

- Rule shown in Table 9.4 is satisfied.

Table 9.4 Rule for Usage Pass Recovery of UT mode

Transaction Status		Session Status			
		RP	RC	SP SC US	
		Usage Pass Status			
Transaction Log		NE VD IVD	NE	VD IVD	NE VD IVD
Session Status	SP	Prohibited	Prohibited	Prohibited	Prohibited
	SC	Allowed	Allowed	Prohibited	Prohibited
	RP RC US	Prohibited	Prohibited	Prohibited	Prohibited

- Allowed

When a Primal Device is a Storage Device, the Device may overwrite AC_s in its QST with AC_s recorded in Transaction Log and validates it. Session Status in the Transaction Log in the Primal UPTU shall be set to “Send Prepared” just before the recovery. When a Primal Device is a Host Device, the Device may prepare to re-transfer the objective Usage Pass to the Inceptive Device.

- Prohibited

The objective Usage Pass shall not be recovered.

9.2 Bidirectional Transfer (BT) mode

In BT mode, Transaction Log and Connection Log are used.

9.2.1 Connection Log

If Reconnection Stage is supported, both the Primal UPTU and the Inceptive UPTU shall record Connection Log at Connection and Reconnection Stage. Connection Log in the Primal Device shall consist of one entry for each HIFU, if it is recorded. Meanwhile, Connection Log in the Inceptive Device may consist of plural entries with the proviso that Recovery-Allowed Primal Device Indicator is functional. However, existence of plural entries of Connection Log for a Primal Device in an Inceptive Device shall not be allowed.

Every Connection Log for any HIFU in the Primal UPTU and all entries of Connection Log in the Inceptive UPTU shall be invalidated when RDCL is updated in Connection Stage of either UT mode or BT mode.

Information recorded in Connection Log is shown in Table 9.5.

Table 9.5 Information recorded in Connection Log

Information	Attribute	Role
Self Session Key	Internal	Primal Inceptive
Partner Session Key	Internal	Primal Inceptive
Partner Device Public Key	Internal	Primal Inceptive
Type Map	Internal	Primal Inceptive
Partner Message Version	Internal	Primal Inceptive
Primal Device Specifier	External	Inceptive

9.2.1.1 Type Map

Type Map is Acceptable Usage Pass Type Map described in a Device Class Certificate of the partner Device. The data is overwritten at the same time when Partner Device Public Key is overwritten.

9.2.1.2 Partner Device Public Key

Partner Device Public Key is a Device Public Key kept in a partner UPTU. If UPTU is Source, the key shall be overwritten whenever a Session Key is received from Destination UPTU at Connection Stage. If UPTU is Destination, the key shall be overwritten whenever a Session Key is generated by oneself at Connection Stage.

9.2.1.3 Self Session Key

Self Session Key is a Session Key generated by oneself at Connection or Reconnection Stage. If UPTU is Source, the key shall be overwritten whenever a Session Key is received from Destination UPTU at Connection Stage or Reconnection Stage. If UPTU is Destination, the key shall be overwritten whenever a Session Key is generated by oneself at Connection Stage or Reconnection Stage.

9.2.1.4 Partner Session Key

Partner Session Key is a Session Key generated in a partner UPTU at Connection or Reconnection Stage. The key shall be overwritten at the same time when Self Session Key is overwritten.

9.2.1.5 Partner Message Version

Partner Message Version is Message Version supported by a partner UPTU. It is exchange at Connection Stage.

9.2.1.6 Primal Device Specifier

Primal Device Specifier is a Serial Number assigned to the Device Class Certificate embedded in the partner Primal UPTU.

9.2.2 Transaction Log

If Recovery Stage is supported, the Primal UPTU shall record every Transaction Log corresponding to every Usage Pass Transfer. Transaction Log shall consist of one or more entries which belong to each HIFU, if it is recorded. All entries of Transaction Log which belongs to a HIFU shall be invalidated when (1) RDCL is updated in Connection Stage of either UT mode or BT mode, (2) Connection Stage is completed, namely Connection Log for the HIFU is overwritten, or (3) Recovery Permission Indicator sent from the Inceptive Device in Reconnection Stage shows that the Primal UPTU is not allowed to execute Recovery Stage on the Usage Passes which were transferred before the Reconnection Stage.

A Usage Pass Identifier is recorded in each entry of Transaction Log. If a UPTU has plural entries of Transaction Log of which Usage Pass Identifier are same, only the latest Transaction Log shall be used in Recovery Stage. Information recorded in Transaction Log is shown in Table 9.6.

Table 9.6 Information of Transaction Log for BT mode

Information	Attribute	Role
Usage Pass Identifier	External	Source Destination
Transfer Type	External	Source Destination
Original Access Condition	Internal	Destination
Original Usage Pass	Internal	Source
Usage Pass Location	External	Source Destination

9.2.2.1 Usage Pass Identifier

Usage Pass Identifier is the identifier assigned to each Usage Pass. The identifier is recorded when a Session Key is generated or received. Transaction Log is looked up with this identifier.

9.2.2.2 Transfer Type

Transfer Type is information that shows the behavior of Primal Device. Transfer Type is shown in Table 9.7.

Table 9.7 Transfer Type

Type	Abb.	Description of the type
Source for Importing	SI	Primal Device as Source for importing
Source for Transmitting	ST	Primal Device as Source for transmitting
Destination of Copy	DC	Primal Device as Destination for Usage Pass Copy
Destination of Move	DM	Primal Device as Destination for Usage Pass Move
Destination of Play	DP	Primal Device as Destination for Usage Pass Play

9.2.2.3 Original Access Condition

Original Access Condition is AC_s included in the objective Usage Pass that is pre-transferred. If the Primal Device is Destination, the data is recorded at the same time when Usage Pass Identifier is recorded.

9.2.2.4 Original Usage Pass

Original Usage Pass is the objective Usage Pass that is pre-transferred. If the Primal Device is Source, the data is recorded at the same time when Usage Pass identifier is recorded. This data may be kept in UPC and UPT as invalidity.

9.2.2.5 Usage Pass Location

When Primal Device is Source, location of Usage Pass to be recorded in Inceptive Device is recorded. When Primal Device is Destination, location where Usage Pass is recorded in Inceptive Device is recorded.

9.2.3 Recovery-Allowed Primal Device Indicator

As for Inceptive Device, plural entries recording of Connection Log is allowed. On the other hand, the Primal Device which is allowed to execute Recovery Stage for an Inceptive Device shall be limited to a Primal Device which was completed Transfer Stage from/to the Inceptive Device most

recently in terms of security. Therefore, if recording of plural entries of Connection Log is supported on an Inceptive Device, Recovery-Allowed Primal Device Indicator shall be recorded in the UPTU of the Inceptive Device.

Into the Indicator, information to specify the Primal Device, which is allowed to execute Recovery Stage for the Inceptive Device, is included. Number of the entry of Connection Log for the Primal Device is a typical example.

In order to accomplish the limitation described above, the Indicator shall be record or updated when Transfer Stage for the Inceptive Device is completed.

9.2.4 Recovery Permission Indicator

The Inceptive Device shall notify whether the connected Primal Device is allowed to execute Recovery Stage with the recorded Transaction Log or not as Recovery Permission Indicator in the Reconnection Stage. Recovery Permission Indicator may be set to indicate that Recovery Stage execution with the recorded Transaction Log is allowed if Recovery-Allowed Primal Device Indicator designate the entry of Connection Log which is used for the Reconnection Stage, For all the other cases, Recovery Permission Indicator shall be set to indicate that Recovery Stage execution with the recorded Transaction Log is not allowed

Primal Device shall invalidate all the recorded entries of Transaction Log for the objective entry of Connection Log if the received Recovery Permission Indicator indicates that the Primal Device shall not retain the Transaction Log.

9.2.5 Transaction Status

An Inceptive UPTU sends Transaction Status to a Primal UPTU to inform the state of the objective Usage Pass recorded in the Inceptive QST. When the Primal UPTU judges whether the Usage Pass Recovery is allowed, the UPTU uses the Transaction Status.

The structure of Transaction Status is as the followings.

Transaction Status ::= UPID || AC_s || UPS || UPL || UPstatusHashValue

UPstatusHashValue ::= H(tbsUsagePassStatus)

tbsUsagePassStatus ::= K_{s[P]} || K_{s[I]} || UPID || AC_s || UPS || UPL

UPID : the Usage Pass Identifier of the objective Usage Pass.

AC_s : Access Condition for Storage Module recorded in the Inceptive QST.

Usage Pass Status (UPS) : A status information shown in Table 9.3 of objective Usage Pass recorded in the Inceptive Device.

Usage Pass Location (UPL) : Location where the objective Usage Pass is recorded.

K_{s[P]} : A Primal Device Session Key that is generated most recently.

K_{s[I]} : An Inceptive Device Session Key that is generated most recently.

9.2.6 Recovery condition

If the following conditions are satisfied, the Primal Device may recover an objective Usage Pass with the used of Original Usage Pass or Original Access Condition in Transaction Log.

- Transaction Log is recorded in Primal UPTU and its Usage Pass Identifier is the same as that in Transaction Status.
- Usage Pass Location of Transaction Log and Transaction Status are same value.
- UPstatusHashValue in Transaction Status is verified.
- Rule shown in Table 9.8 is satisfied.

Table 9.8 Rule for Usage Pass Recovery of BT mode

Transaction Log		Transaction Status		Usage Pass Status (UPS)		
		NE	IVD	VD		
Transfer Type	Source	SI ST	Allowed Recover UP	Prohibited	Prohibited	
	Destination	DM	Prohibited	Allowed Recover AC _s	Prohibited	
		DC DP	Prohibited	Prohibited	Allowed Recover AC _s	

- Recover UP

A Primal Device is Source. The objective Usage Pass is not recorded in Inceptive QST. The Primal Device may prepare to re-transfer the objective Usage Pass to the Inceptive Device with the recorded Original Usage Pass in Transaction Log.

- Recover AC_s

A Primal Device is Destination. The objective Usage Pass is not received or received but not consumed. The Primal Device may transfer the AC_s recorded in Transaction Log as Original Access Condition to the Inceptive Device. If the Inceptive Device receives the AC_s, the Device shall overwrite AC_s in its QST with the received AC_s and shall validate it.

- Prohibited

The objective Usage Pass shall not be recovered.

Annex A ECDH Algorithm

A.1 Encryption

The following information is used for encryption.

- Data: *TEXT*
- Common base point : $G(G_x, G_y)$
- Order of elliptic curve : r
- Public key : $KP(KP_x, KP_y) = K \times G$

The procedures of the key calculation of ECDH and the encryption using the key are as follows;

- (1) generate random / pseudorandom number q ($0 < q < r$),
 - (2) calculate $q \times G = Q(Q_x, Q_y)$,
 - (3) calculate $q \times KP = W(W_x, W_y)$,
 - (4) calculate ECDH Shared Key $*KP$ using W_x ,
 - (5) encrypt *TEXT* with $*KP$: $E(*KP, TEXT)$,
 - (6) concatenate $Q_x, Q_y, E(*KP, TEXT)$,
- as the result, encrypted data $Q_x || Q_y || E(*KP, TEXT)$ is given.

A.2 Decryption

The following information is used for decryption.

- Encrypted data: $Q_x || Q_y || E(*KP, TEXT)$
- Common base point : $G(G_x, G_y)$
- Order of elliptic curve : r
- Private key: K , in the case of public key $KP(KP_x, KP_y) = K \times G$

The procedures of the key calculation of ECDH and the decryption using the key are as follows;

- (1) calculate $K \times Q(Q_x, Q_y) = W(W_x, W_y)$,
 - (2) calculate ECDH Shared Key $*KP$ using W_x ,
 - (3) decrypt $E(*KP, TEXT)$ with $*KP$,
- as the result, ECDH Shared Key $*KP$ is shared and *TEXT* is given.

Annex B ECDSA Algorithm

B.1 Digital signature creation

The following information is used for generating signature.

- Data: *TEXT*
- Common base point : $G = (G_x, G_y)$
- Order of elliptic curve : r
- Private key using for signature : K_r

The procedure of generating signature is as shown below;

- (1) calculate hash value; $H(TEXT)$ by using hash function SHA-256,
 - (2) generate random / pseudorandom number k ($0 < k < r$),
 - (3) calculate $k \times G = (K_x, K_y)$,
 - (4) calculate signature $t = K_x \text{ mod } r$,
 - (5) calculate signature $s = k^{-1} \{H(TEXT) + K_r t\} \text{ mod } r$,
 - (6) concatenate *TEXT* and signature t and s ,
- as the result, data with the signature, $TEXT || t || s$ is given.

B.2 Digital signature verification

The following information is used for verifying signature.

- Data with the signature : $TEXT || t || s$,
- Common base point : $G = (G_x, G_y)$
- Order of elliptic curve : r
- Public key corresponding to private key used for the signature $KP_r = K_r \times G = (KP_{rx}, KP_{ry})$

The procedure of verifying signature is as shown below:

- (1) calculate hash value, $H(TEXT)$ by using hash function SHA-256;
- (2) calculate $W = s^{-1} \text{ mod } r$,
- (3) calculate $U1 = H(TEXT) \times W \text{ mod } r$,
- (4) calculate $U2 = t \times W \text{ mod } r$,
- (5) calculate $U1 \times G + U2 \times KP_r = U1 \times (G_x, G_y) + U2 \times (KP_{rx}, KP_{ry}) = (U_x, U_y)$,
- (6) calculate $v = U_x \text{ mod } r$,

If $v = t$, the *TEXT* is correct.