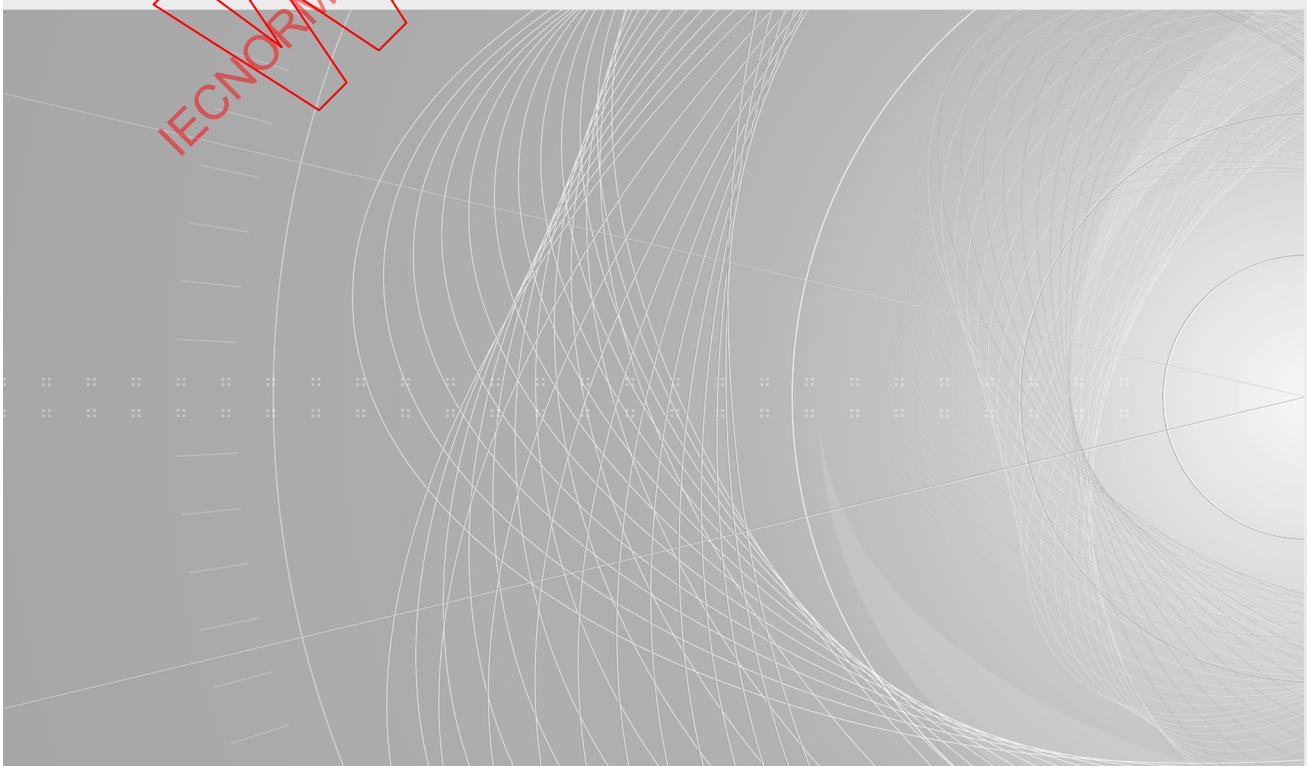
IEC/TS 62224

Edition 1.0 2007-11

TECHNICAL SPECIFICATION

Multimedia home server systems – Conceptual model for digital rights management



IEC/TS 62224:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TS 62224

Edition 1.0 2007-11

TECHNICAL SPECIFICATION

Multimedia home server systems – Conceptual model for digital rights management

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE V

ICS 33.160.60; 35.240.99

ISBN 2-8318-9361-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MULTIMEDIA HOME SERVER SYSTEMS – CONCEPTUAL MODEL FOR DIGITAL RIGHTS MANAGEMENT

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62224, which is a technical specification, has been prepared by IEC technical committee 100: Audio, video and multimedia systems and equipment.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
100/1064/DTS	100/1117A/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International Standard,
- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

A bilingual version of this document may be issued at a later date.

INTRODUCTION

Due to the recent trends in the rapid popularization of mobile phones and the Internet, as well as the realization of high-speed data transmission and large-volume data recording media, high-quality content distribution and ubiquitous information services are making progress and a new type of information distribution and network sharing service has gradually emerged into the market. It is capable of utilizing terabyte-sized home servers also in private homes.

Under these circumstances, in distribution of content over shared networks, it is crucial to establish digital rights management (DRM) technologies to protect the content from illegal copying and usage. A truly successful DRM system must be built on open worldwide specifications and provide maximum interoperability and user acceptance.

An open interoperable specification that follows this technical specification is able to construct highly expandable PKI-based DRM, targeting usage between systems, considering the expansion of recent content distribution services and clients (console type AV equipment, PC, mobile phone terminal, automotive telematics terminal, and so on). This technical specification gives protocol specifications for the exchange of license information among the DRM module, the description of specifications for license information and the encrypted content formats.

During the development of this model, the main consideration was the use of contents in consumer electronics equipment connected with a home server. Also considered were distribution, storage exchange and use of content between the distribution server and the destination client system, allowing for conditions approved by the rights holder, and without loss of convenience for the users. The standardization and its popularization based on this model will enable interconnection between DRM modules allowing strong content protection in various content distribution services over networks such as the Internet and mobile phone networks.

MULTIMEDIA HOME SERVER SYSTEMS – CONCEPTUAL MODEL FOR DIGITAL RIGHTS MANAGEMENT

1 Scope

This technical specification explains the conceptual model of a protocol specification to exchange licence information between DRM modules and outlines what should be defined as standards.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2005, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

ITU-T Recommendation X.509:2000, *Information technology – Open Systems Interconnection – The Directory: Authentication Framework*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions, in addition to some of those given in ITU-T Recommendation X.509, apply.

3.1.1
access condition
information that describes the content usage conditions

NOTE The access condition represents the conditional rules that restrict user ability to manipulate the content information and is a part of authorization information in the licence for the content.

3.1.2
access control list
list of conditions to access content for each principal such as content users, user groups and so on

3.1.3
asset identifier
information which identifies an asset which may include one or more contents

NOTE A licence should include an asset identifier. There are cases, for example, when an asset identifier is in accordance with a content identifier, which specify the group of content identifier or a part of the content identified by the content identifier.

3.1.4
certification authority
authority trusted by one or more users to create and assign public-key certificates

[ITU-T Recommendation X.509, 3.3.17]

3.1.5
certificate revocation list
signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes

[ITU-T Recommendation X.509, 3.3.12]

3.1.6
class certificate
certificate which declares the justifiability of TREM and its class public key with its related information

3.1.7
class private key
key kept privately inside a TREM being subject to the same TREM class

NOTE The TREM developer or manufacturer should keep and manage this key privately.

3.1.8
class public key
public key corresponding to the class private key

3.1.9
content credential
information to certify integrity of the content data and the generator of the content data

NOTE This information includes a digital signature of the content, i.e., the hash value of the content data encrypted with the generator's private key. In general, it is added at the end of the protected content format (PCF) data.

3.1.10
content identifier
identifier which is a unique value assigned to each content that is a unit of information provided by the content holder

3.1.11
content key
content encryption key unique to each content under the symmetric key cryptosystem

3.1.12
data concatenation
concatenation of two bit-streams into a single bit-stream

NOTE The first bit of the second original stream is next to the last bit of the first original stream.

3.1.13
decoder TREM
TREM in which encrypted content can be decrypted and played

3.1.14
destination TREM
TREM receiving a licence

3.1.15
digital rights management
technology or functions to protect rights relating with digital content, for example, copyright, or system or module which provides these functions

NOTE Inside this system or module it manages content access conditions and behaves under these conditions.

3.1.16
encrypted content
encrypted content data with its related meta data: broadcasting content, download content, streaming content, and so on

3.1.17
entry TREM
TREM that has the function of generating a new licence according to indication from outside and behaves as a source TREM, inside the licence distribution server and so on

3.1.18
hash function
(mathematical) function which maps values from a large (possibly very large) domain into a smaller range

[ITU-T Recommendation X.509, 3.3.32]

3.1.19
licence
information including one or more content keys and authorization information like access conditions, etc.

NOTE If it is outside a TREM, it should be a protected licence, which is protected with a session key generated in accordance with SLTP.

3.1.20
licence identifier
data as an output of the concatenated asset identifier (may be the content identifier) and the transaction identifier

3.1.21
licence move
moving of a licence from one TREM to the other

NOTE Once the licence is moved, the licence is deleted from the source TREM. A licence move with the encrypted content copy equals a content move.

3.1.22
licence relay module
LRM
system or module that relays a protected licence between TREMs through an SLTP session

NOTE LRM is an endpoint of an LRP connection and has the function of controlling internal bus and network in order to relay the protected licence via the LRP connection.

3.1.23
licence relay protocol
LRP
protocol between LRMs

NOTE Over this protocol, secure licence transaction protocol (SLTP) is realized for the Internet environment. For the SLTP, the LRP provides functions of transaction management, restart of disconnected SLTP session, protocol negotiation, and transfer of information relating with user authentication or accounting management.

3.1.24
licence server
server system that has a TREM and the LRM which mediates the transmission of a licence issued by the TREM

3.1.25
licence transaction
unit of processing to distribute, move or copy a licence

NOTE For each transaction, the different resources are assigned and managed.

3.1.26
mediator TREM
TREM that mediates licence transfer as a main role

NOTE A mediator TREM has both roles as destination and source TREMs.

3.1.27
principal
subject that accesses a specific content or asset, such as content operation equipment, a storage medium, a content user and a group or domain of them

3.1.28
protected content format (PCF)
data format in which the encrypted content is distributed

NOTE PCF can include multimedia contents and information representing their relationships. It can include a content credential.

3.1.29
protected licence
licence information protected to transfer between TREMs

NOTE A protected licence includes encrypted content keys and protected authorization information. The content keys are encrypted with the SLTP session key. The authorization information, including access conditions or its hash, is encrypted with the SLTP session key as a counter-measure to its modification. Because authorization information is often very short, hash is not only needed but also causes redundancy.

3.1.30
protection level
robustness to protect TREM and/or its content

NOTE Protection of TREM is realized as a tamper-resistant module.

3.1.31
public key cryptosystem
cryptosystem in which the encryption and the decryption keys are different

NOTE When concealing the data, the key used for encryption is publicly distributed. RSA and elliptic curve cryptosystem are well known as public key cryptosystems.

3.1.32
root private key
private key securely maintained by the certification authority

3.1.33
root public key
public key corresponding to the root private key

3.1.34
secure licence transaction protocol (SLTP)
protocol to transfer licence information securely between TREMs

NOTE This protocol consists of formats of the information exchanged between TREMs and a state transition specification of the TREM, which should be implemented.

3.1.35
session key
temporary key shared between TREMs at each SLTP session

NOTE A session key is a random number produced by one TREM and a key for the symmetric key cryptosystem.

3.1.36
SLTP session
secure session generated between TREMs according to the SLTP in order to transfer licence

NOTE Each SLTP session has a session key shared by both sides of the TREMs.

3.1.37
source TREM
TREM issuing a licence

3.1.38
symmetric key cryptosystem
cryptosystem in which the same key is used to encrypt and decrypt the data

NOTE The advanced encryption standard (AES) standardized by NIST in the U.S.A. is a well-known symmetric key cryptosystem.

3.1.39
tamper-resistant module
TRM
module to protect from analysis or modification of information and its processing

NOTE See FIPS 140-2.

3.1.40
tamper-resistant rights enforcement module
TREM
system or module which has functions of digital rights management

NOTE TREM is structured as a tamper-resistant module. TREM has functions to enforce rights, manage the licence and process the licence transfer according to SLTP.

3.1.41
transaction identifier
identifier that is assigned to each licence transaction

3.1.42
transaction log
log data representing the status of a licence transfer transaction and the licence issued in that transaction

NOTE A transaction log is securely stored in the TREM.

3.1.43
TREM class
set of TREM authorized in a security judgment

NOTE A TREM that belongs to a TREM class has a subset of the same class certificates set issued by that judgment.

3.1.44
TREM (individual) private key
key kept privately by each TREM individually

3.1.45
TREM (individual) public key
public key corresponding to a TREM (individual) private key

3.2 Abbreviated terms

ACL Access Control List
AES Advanced Encryption Standard
AID Asset Identifier
CA Certification Authority
CRL Certificate Revocation List
DES Data Encryption Standard
DRM Digital Rights Management
EC-DH Elliptic Curve Key Agreement Scheme, Diffie-Hellman
EC-DSA Elliptic Curve Verification Primitive, DSA version
GLF Generic Licence Format
ID Identifier
LRM Licence Relay Module
LRP Licence Relay Protocol
PCF Protected Content Format
SLTP Secure Licence Transaction Protocol
T-DES Triple DES
TID Transaction Identifier
TREM Tamper-resistant Rights Enforcement Module
TRM Tamper-resistant Module

4 Notation

4.1 Numerical values

In this model, the following expressions of numerical values are used.

Table 1 – Expression of numerical values

	Binary (BIN)	Decimal (DEC)	Hexadecimal (HEX)
Letters used for value	'0'~'1'	'0'~'9'	'0'~'9', 'A'~'F'
Appended letter	Nothing（or 'b'）	Nothing	'h'
Example	11001000 （or 11001000b）	200	C8h

4.2 Notations for keys

The following are the rules to represent keys in this model.

a) Keys that are used for cryptography shall be represented by a string starting with capital ‘K’.

b) Key expression with a capital ‘P’ in the second letter represents a public key of the public key cryptosystem. The public key shall have a corresponding private key which is represented by a key expression without a capital ‘P’ in the second letter.

c) A key expression with a small letter, ‘c’, ‘s’ or ‘x’ as the second letter represents the symmetric key (shared key) or private key corresponding to the public key. A symmetric key expression with small letter ‘s’ as the second letter represents a session key and ‘x’ represents a symmetric key for individual TREM.

d) Key expression with a small letter ‘t’ represents the embedded key in a TREM.

e) Key expression with a small letter ‘t’ and ‘c’ represents a symmetric key for a TREM class.

f) A numerical suffix letter or a letter ‘x’ or ‘j’ indicates a number or an identifier of each individual key or class key. The numerical suffix is a natural number and can be omitted.

4.3 Notation list

This model uses the following notations.

Table 2 – Notations used in this model

Name	Expression	Description
Encryption	E (K, D)	The result of encryption of information ‘D’ with a key ‘K’
Hash	H (D)	The result of hash of information ‘D’
Concatenation	A || B	The result of data concatenation of ‘A’ and ‘B’
Content key	Kc	A content encryption key associated with each content
Root private key	Ka	A private key securely maintained by CA
Root public key	KPa	The public key corresponding to Ka
Relevant information	Ixx	The information relating to xx
Certificate	C (Ka, KPxx || Ixx)	A certificate of a public key KPxx. KPxx || Ixx || E (Ka, H (KPxx || Ixx))
Class private key	Ktcx	A key that the same class TREM keeps inside them secretly
Class public key	KPtcx	The public key corresponding to Ktcx
TREM private key	Ktx	A key that the TREM keeps individually and secretly
TREM public key	KPtx	A public key corresponding to Ktx
Session key	Ksj (j=1, 2,...)	A temporary key of symmetric key cryptosystem shared between the communication entities per each communication session
CRL update time List	CRLUpdates	Date and time when CRL is renewed
Content ID	CID	The value of a unique identifier assigned to each content
Transaction ID	TID	The value of an identifier assigned for each transaction
Asset ID	AID	Identifier of asset that is authorized to access by a licence
Transaction log	TransactionLog	The log of the status of each transaction stored securely
Individual TREM symmetric key	Kx	A key of a symmetric key cryptosystem that each individual TREM uses inside its TRM

5 Requirements

5.1 Viewpoint of content user

5.1.1 Content usage environment

The aim of this conceptual model is that equipment operating digital contents is implemented conforming to the specifications compliant with this model, and then the rights to manipulate the contents can be exchanged freely among the equipment, storage media, and digital locker

services[1] without infringement of any rights. Implementation according to this model realizes the environment where the general consumer can purchase and enjoy high-quality contents (AV contents, programmes and multi-media contents) with any equipment, such as home server, TV, mobile phone, PC, PDA, IT microwave oven, automotive telematics terminal, etc. anywhere without infringement of any of the rights. Ubiquitous content usage environment like this is shown in Figure 1.

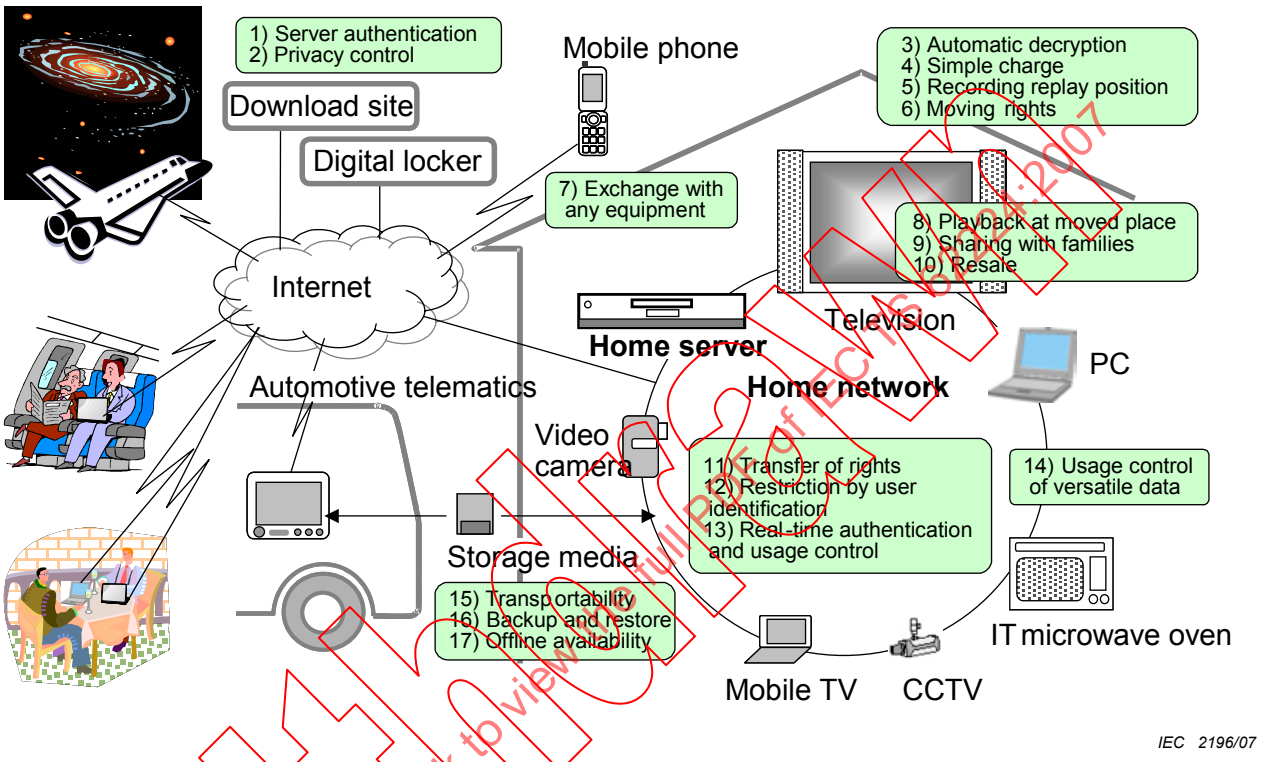


Figure 1 – Requirements in the target ubiquitous content usage environment

Requirements in the content usage environment from the viewpoint of a content user are as follows.

a) Server authentication: secure and reliable server authentication.

b) Privacy control: no-one can illegally access the privacy information of content users.

c) Automatic decryption: the network content is automatically decrypted and decoded without complex operations by the user.

d) Simple charge: the content can be played with simple charge.

e) Recording replay position: the user can restart the playing of content from the position last interrupted.

f) Moving rights: rights of purchased content can be moved within the conditions assigned by rights holder.

g) Exchange with any equipment: the user can exchange content between mobile and home equipments.

[1] Digital locker service: service to provide the user's virtual storage over the Internet. The user can store content, which the user already has or has purchased, to the virtual storage and read (download or receive as a streaming content) it from the virtual storage via the Internet.

h) Playback at moved place: after going to a second room, the user can watch the rest of the same content on a PC as the one which was being watched on the TV in the first room.

i) Sharing with families: the user can share a content purchased with other families without infringement of any rights.

j) Resale: the purchased content may be sold to another without infringement of any rights.

k) Transfer of rights: the user can transfer rights of purchased content to another.

l) Restriction by user identification: the player system can control the play of content according to the result of the user identification, for example, the age of the user.

m) Real-time authentication and usage control: the user system can process usage control in real time in receiving and playing of the content.

n) Usage control of versatile data: without infringement of any rights, the user can enjoy multimedia content including motion picture, music, superimposition, lyrics, image, programme, and others. The user equipment can also process non-multimedia data, for example, recipe data processed by an IT microwave oven.

o) Transportability: transportability of recording media. The user can carry a content stored in a recording media and watch the rest of the content without indicating the restart position.

p) Back-up and restore: in the case where the content package media is broken or lost, the user can revoke the rights to play the media and set the same (back-up) content to a new package media without renewal of the sales contractand.

q) Offline availability: The user can use purchased rights in an offline (non-network) environment.

5.1.2 Content distribution services

In this model, the following types of content distribution services that are required in the above environment are considered.

a) Network download service.

b) Streaming service.

c) Content exchange support service, which supports the copying or moving of protected contents among home or mobile equipments (such as P2P) and digital lockers without infringement of any rights.

d) KIOSK terminal, from which the user can purchase contents.

e) Superdistribution service, by which the user can purchase just the rights to play an encrypted content.

In this model, the following functional requirements for these services are considered.

a) Ubiquitous service: the user can purchase any content and play it wherever and whenever.

b) Mediation function: any type of digital content can be downloaded and forwarded with its rights into any type of content operation system (like a digital content player device) through any type of mediation server system such as contents management system, contents distribution system, digital locker server, home server and so on.

c) Automatic session recovery: the content distribution service system can automatically reconnect just after disconnection in downloading content. After reconnection, only the rest of the content data not yet downloaded should be downloaded.

5.1.3 Integrity of content

The superdistribution service, considered in this conceptual model, encourages the exchange of encrypted content among users unknown to each other. With superdistribution, it is necessary for the user who has received encrypted content from an unreliable site to be able

to confirm the integrity of the encrypted content, because anyone may modify the original content data at one of the unreliable sites where the content distribution was mediated.

5.2 Viewpoint of rights holder

In this model, it is considered that multimedia contents (for example, movies, games, documents, programmes, etc.) are distributed, stored and used according to the conditions designated by the rights holders. It must also be considered that the rights are protected without spoiling the usability.

5.2.1 Overview of requirements for content protection

The following are the requirements for content protection in the content distribution and usage environment described in 6.1.

a) Right to read: the content holder can grant the right to read and play, display or print the content.

b) Right to edit: the content holder can grant the right to edit and store the content.

c) Right to copy or move: the content holder can grant the right to copy or change the rights. After the rights are changed , the rights in the source shall be deleted.

d) Editing of rights: the content holder can edit the rights within the limited rights granted.

e) Permission for each principal: the content holder can grant the rights for each principal such as a content operation equipment, a storage medium, a content user and a group or domain of them.

f) Permission with a time limit: the content holder can grant the rights with a time limit.

g) Rights countability: the content holder can restrict the number of rights and the number of equipments or media through which the rights are changed or copied, for example, in order to limit the number of users who use a content simultaneously.

h) Rights exchange among servers: the rights may be exchanged among content management server, content distribution server, digital locker server, home server and so on.

i) Ubiquitous access control: The rights granted by content holders shall be enforced to the principal (via equipment or media) whenever and wherever in this universe.

5.2.2 Licence service model

In this conceptual model, the licence service model that satisfies the requirements described in 6.1 and 6.2.1 is considered in order to consider the threats of content distribution services in the next paragraph. The following functional requirements for the licence service model are described in Figure 2.

a) Content is encrypted and distributed in any way.

b) The licence information includes content keys and access conditions (ACs).

c) Once created by rights holder, the encrypted content and protected licence are decrypted only in TREM (tamper-resistant rights enforcement module).

d) The licence information is protected by cryptosystem outside TREMs and shall be moved among TREMs according to the AC itself.

e) A role to issue the changed licence is called source TREM and a role to receive the changed licence is called destination TREM.

f) The TREM processes user a request according to the AC in the licence.

g) Entry TREM (defined in of 3.1.17) in such a content management/distribution server can receive plain content data and plain licence information and can create the encrypted content and the protected licence information and behave as a source TREM.

h) Mediator TREM (defined in of 3.1.26) in a content/licence mediation system behave as both source and destination TREMs.

i) Decoder TREM (defined in of 3.1.13) in such a playback system can receive the licence from the other TREM and decrypt encrypted contents according to the AC included in the licence.

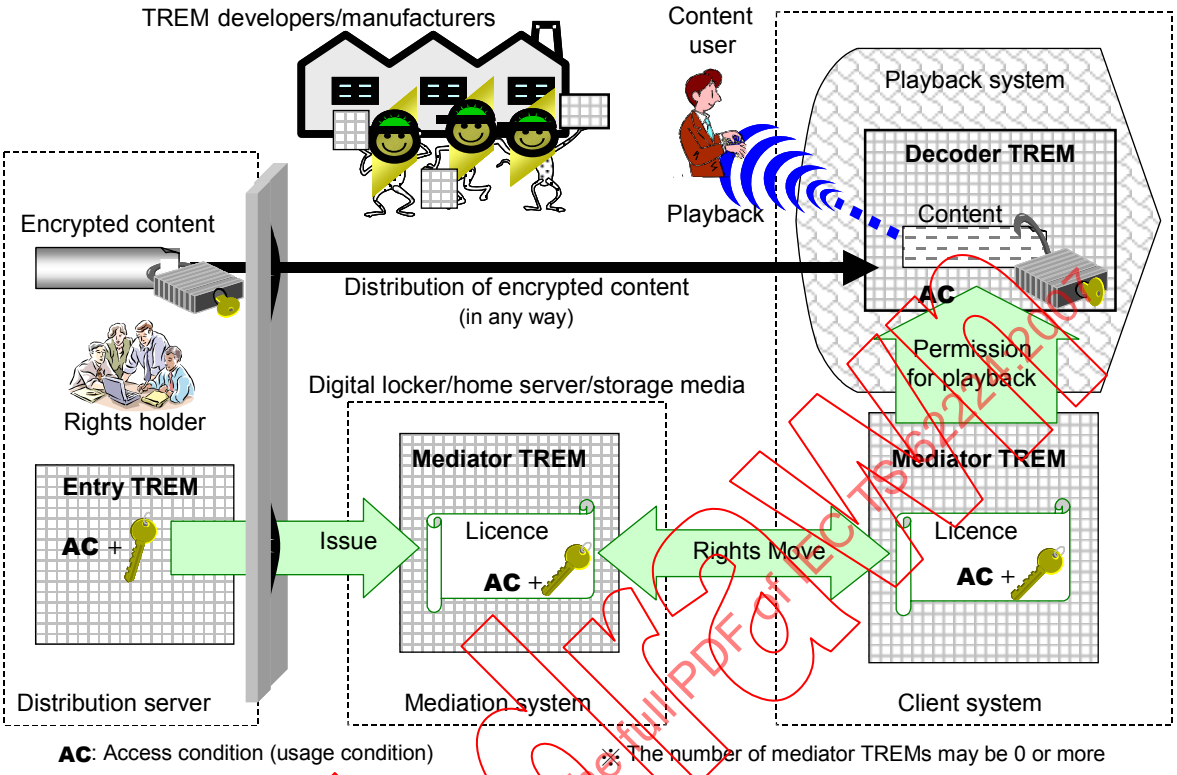


Figure 2 – Licence service model to consider the threats

5.2.3 Threats and counter-measures

Table 3 shows threats in the licence service environment described in 6.2.2 and counter-measures against each threat.

Table 3 – Threats and counter-measures in the licence service model

Subject	Attack (threat)		Counter-measures	
TREM user	Analysis of TREM		1) Manufacturing TREM as TRM	
	Camou-flage	Camouflage of the destination TREM	2) Encryption with session key shared after mutual authentication by the certificate of the destination TREM	
		Replay (camouflage of the source TREM)		
TREM user and network user	Leakage of TREM class private keys or temporary private keys		3) Encryption with individual key for each destination TREM instance	
	Camouflage of disconnection of the licence transaction session		4) Comparison between logs in each TREMs	
	Leakage of private key for the CA or the TREM class		5) Issue of CRL	Key renewal
TREM manufacturer	Illegal manufacturing			Termination of the broken or illegal TREM
	Leakage of key information			
PC user	Analysis of software TREM		6) Content protection level control	

5.2.3.1 Manufacturing TREM as TRM

TREM must be TRM in order to prevent the content user from analysing the TREM and stealing the secret keys from it.

5.2.3.2 Encryption with session key

In the licence distribution service, impersonation of the TREM such as replay attack by camouflage of the licence sender TREM causes unauthorized unlimited copies of the content. So, in order to prevent anyone from developing the module impersonating the source (sender) or destination (receiver) TREM, the changed licence must be encrypted with the session key shared after the mutual authentication of the source and destination TREMs using the certificate for the class public key of the destination TREM.

5.2.3.3 Encryption with individual key

The changed licence should be encrypted with also key for each individual destination TREM instance, in order to prevent anyone from breaking the TREM class public key. Otherwise, once the TREM class public key is broken by anyone to analyse an instance of the TREM class, all the other instances of the same class are also broken.

5.2.3.4 Comparison between logs

It is necessary that the licence transaction logs are securely stored in the TREM. When the session to transfer/change licence is disconnected and the recovery of the session to send the licence is needed once more, the log of the destination TREM should be securely transferred to the source TREM in order to compare the logs of source and destination to confirm if the licence was already received by the destination or not. Otherwise, anyone may camouflage the unauthorized copy of the licence with the session recovery.

The probabilities of disconnection unexpected by the user are many during purchasing of licence through communication networks, especially wireless mobile networks. If there is no counter-measure for this type of threat, a distributor could only repeatedly send licences to a deceitful TREM camouflaged with the legally disconnected TREM. Because not only the disconnection may really have occurred but also there is no evidence that the licence arrived, the source TREM must certainly deliver the licence to the destination in exchange for accounting or decrease of the rights.

5.2.3.5 Issue of CRL

CRL can be used in order to terminate the use of illegal or broken keys and TREMs. For the description of CRL, see RFC 3280.

5.2.3.6 Protection level control

The robustness of software TRM is remarkably low if compared with that of a dedicated hardware TRM. In the environment where TREM as hardware TRM and TREM as software TRM coexist, the fact that the software TRM was broken influences the whole of the environment without protection level control.

Protection level control is in accordance with the following rules described in Figure 3.

a) The higher the value of the TRM level, the more robust the system is against attacks (threats).

b) The licence can be changed to the TRM with the same or higher level as the permitted level of the licence.

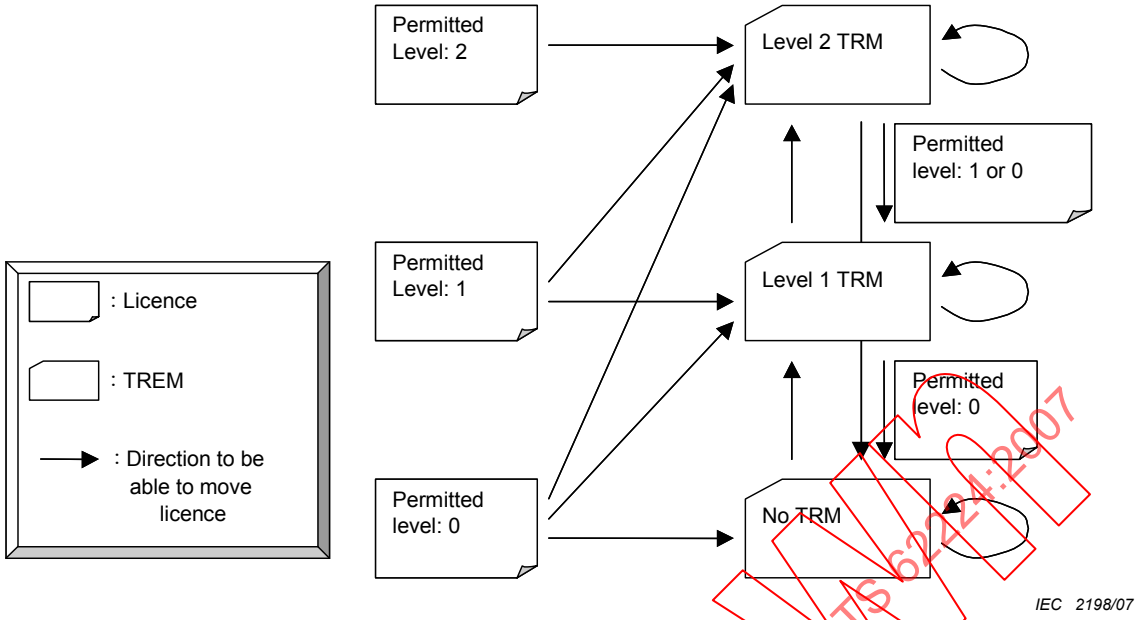


Figure 3 – Example of protection level control

5.2.4 Evaluation criteria

In order to realize a secure content protection environment, it is necessary that the security evaluation criteria for TREM are specified for each TRM protection level described in 6.2.3.6 and all of the TREMs are judged to conform to the criteria or not. The security criteria for content protection should be compliant with ISO/IEC 15408 and include the following.

- Security functions for content protection described in 6.2.3.
- If the necessary algorithms for cryptosystem, hash function and function to generate random numbers are properly implemented.
- Robustness of TRM for TREM, for example, the security level of TRM compliant with FIPS 140-2.
- Process to design, develop and manufacture the TREM.

6 Design considerations

In this clause, the following conceptual models satisfying the requirements described in Clause 5 are specified.

a) Security model.

b) Interconnection model.

c) Licence information model.

d) Protected content format model.

6.1 Security model

In this subclause, the security model satisfying the requirements described in 6.2.3 is specified.

6.1.1 Overview of security model

In the security model (Figure 4) of this conceptual model, contents to be protected are encrypted and distributed in any way. Also, in this model, the content encryption key and the

licence information including access conditions (AC) for the content are protected using TRM and cryptosystem and have the following lifecycle as a licence.

a) The licence is created in an entry TREM.
b) The licence is at first issued as a protected licence from the entry TREM.
c) The licence is transferred to a decoder TREM through more than 0 mediator TREM.
d) The licence is used to decrypt the content according to the AC in the decoder TREM.

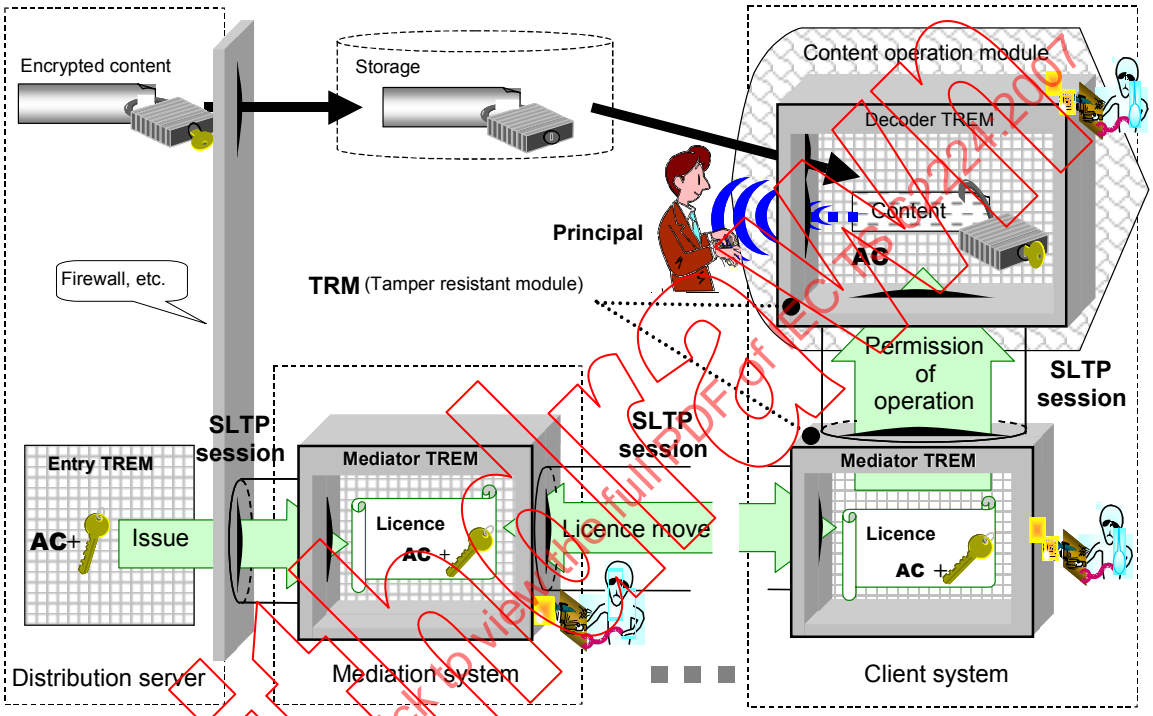


Figure 4 – Security model of content protection

The TREM shall have the following functions.

a) Tamper-resistant function preventing leakage of licence information as a TRM.
b) Function to create and maintain the SLTP session.
c) Function to move licence between TREMs always using the SLTP session.
d) In the case of mediator TREM, function to decrypt the licence and transfer it to other TREM according to the protected mediator access conditions (ACm).
e) In the case of decoder TREM, function to decrypt the licence and decrypt the content with the decrypted key according to the protected decoder access condition.

6.1.2 Secure licence transaction protocol (SLTP) model

In this subclause, the SLTP model to satisfy all of the requirements described in Clause 6 is explained as an example of the most simple secure licence transaction protocol between TREMs. Standardization and implementation of SLTP are needed also as counter-measures, as described in 6.2.3.2 and 6.2.3.4.

SLTP is a protocol to move licence information securely between TREMs. This protocol must consist of formats of the information exchanged between TREMs and a specification of state transition inside the TREM.

6.1.2.1 Generation of SLTP session

In the basic normal sequence of the SLTP model, the following messages are exchanged in accordance with the following steps (Figure 5) to generate the SLTP session as the counter-measures described in 6.2.3.2 and send the licence information securely.

a) Destination certificate: Class public key certificate (defined in ITU-T Recommendation X.509) is sent from licence destination TREM to licence source TREM and checked at the source.

b) Source key: First step of the TREM authentication. The source TREM generates a random number as the first session key, encrypts it with the class public key of the destination and transmits that result to the destination. The destination decrypts it with the class private key to share the first session key with the source.

c) SLTP session key: The second step of TREM authentication. The destination generates another random number as the second session key, encrypts it with the first session key and transmits that result to the source. The source decrypts it with the first session key and shares the second session key with the destination as the SLTP session key.

d) Licence: The source encrypts the licence and CRL list with the SLTP session key and transmits it to the destination. The destination decrypts it with the SLTP session key to obtain the licence.

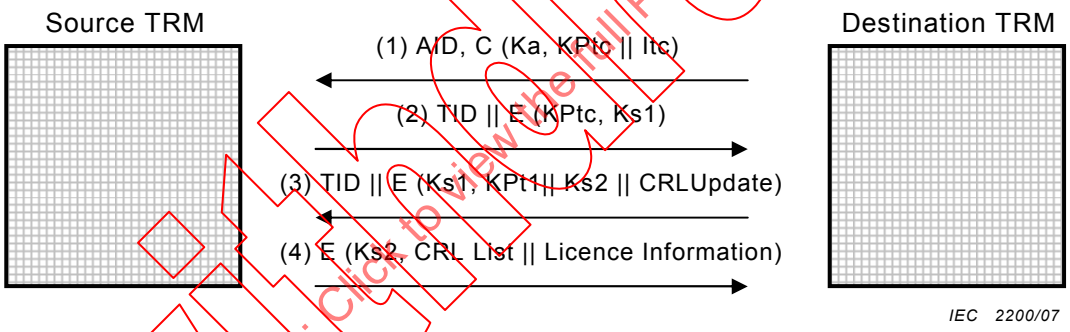


Figure 5 – Basic procedure of SLTP model

In order to use a random number as a session key, the random number shall be generated securely enough. The secure random numbers shall be different in each generation and values that are difficult to be estimated within the period meaningful for the attackers.

If the received information cannot be interpreted properly in the TREM, the TREM rejects it immediately, in order to prevent any type of attacks using the fragile of the module.

6.1.2.2 Recovery of SLTP session

The counter-measure described in 6.2.3.4 should be supported for secure recovery of SLTP session.

6.1.3 Certification authority

In order to let a TREM class participate in the content distribution service environment, the manufacturer (developer or builder) of the TREM class is required to create a pair of class public keys and class private keys and apply for the class public key with the information relating to the CA .

If the CA has authorized that the application information is proper and the TREM conforming to the security criteria is properly manufactured (or structured), the CA creates the certificate for the TREM class public key and its related information according to RFC 3280. A digital signature with the private key of the CA is added to the certificate, and then the certificate is issued to the manufacturer.

The TREM manufacturer embeds the certificate and the corresponding class private key into the TREM, and then the TREM becomes able to receive the licence moved from the other class of TREM already authorized by the same CA (see Figure 6).

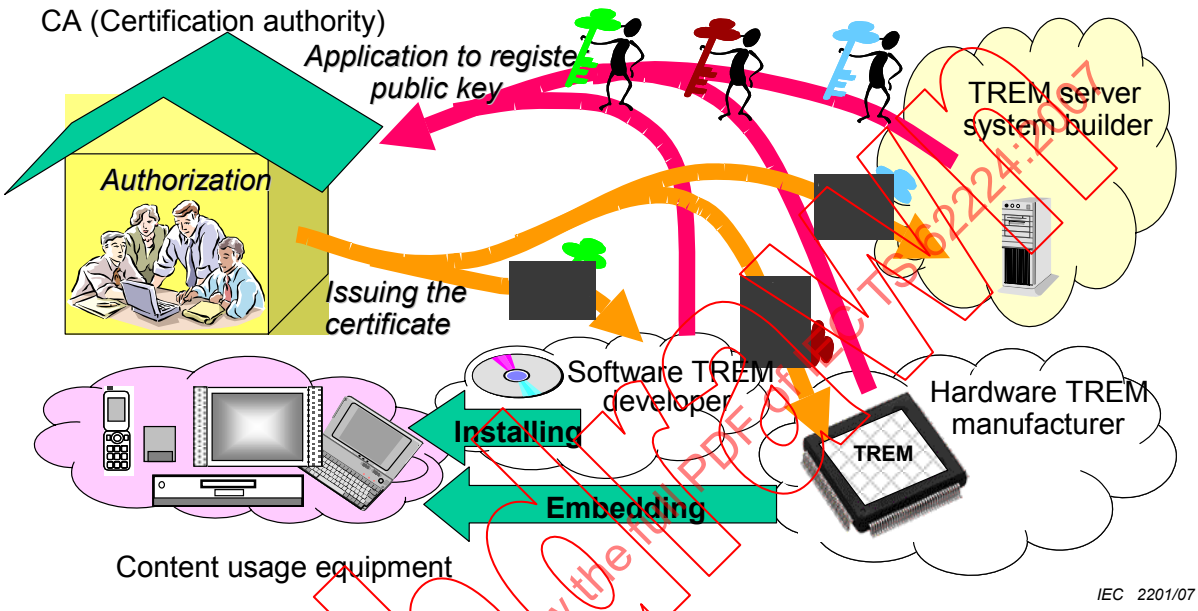


Figure 6 – Overview of issuing TREM class certificates

6.1.4 Key revocation and termination of TREM

Key revocation and termination of TREM by CRL shall be supported in this security model because of the requirements described in 6.2.3.5.

CRL is a list of identifier of revoked certificate with digital signature by the CA. The CRL is used as follows.

a) After issued from the CA, CRL is embedded into the TREMs, especially entry TREMs.

b) If the destination TREM sends the revoked certificate to the source TREM (i.e., identifier of the certificate for destination TREM is found in the CRL), the licence move is rejected.

c) If the certificate is not revoked, the CRL is transferred to the destination TREM with the licence.

d) If all the certificates belonging to destination TREM are revoked, the licence issued after the revocation shall neither be distributed nor moved to the TREM. This means the termination of TREM.

6.2 Interconnection model

6.2.1 Generic interconnection model

In this interconnection model (Figure 7), LRM relays the licence protected by SLTP session between TREMs. LRM is a system or module that has the function of controlling internal bus

and network in order to relay a protected licence between TREMs through the SLTP session; but the protected licence can neither be decrypted nor be interpreted in LRM.

The source and destination LRMs are in front of each TREM in each licence exchange system and relay the protected licence using inter LRM protocol called LRP. For the SLTP, the LRP provides functions of transaction management, restart of disconnected SLTP session, protocol negotiation, and transfer of information related to user authentication or accounting management.

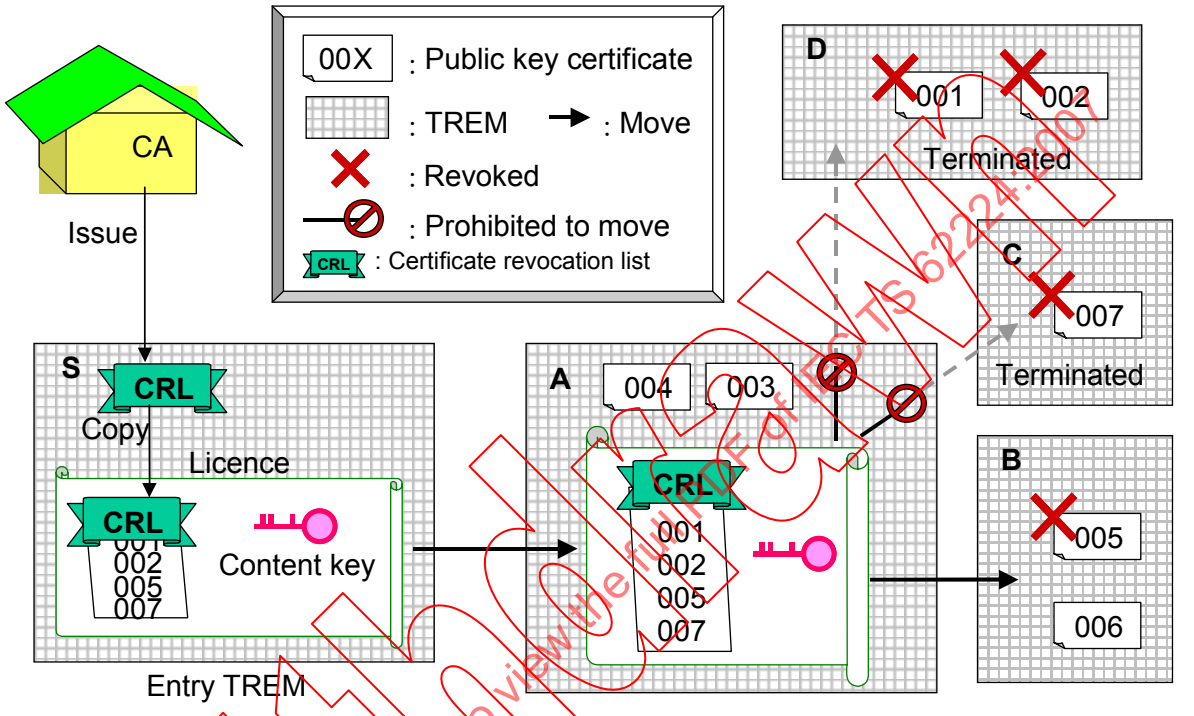


Figure 7 – Revocation of certificates and termination of TREMs

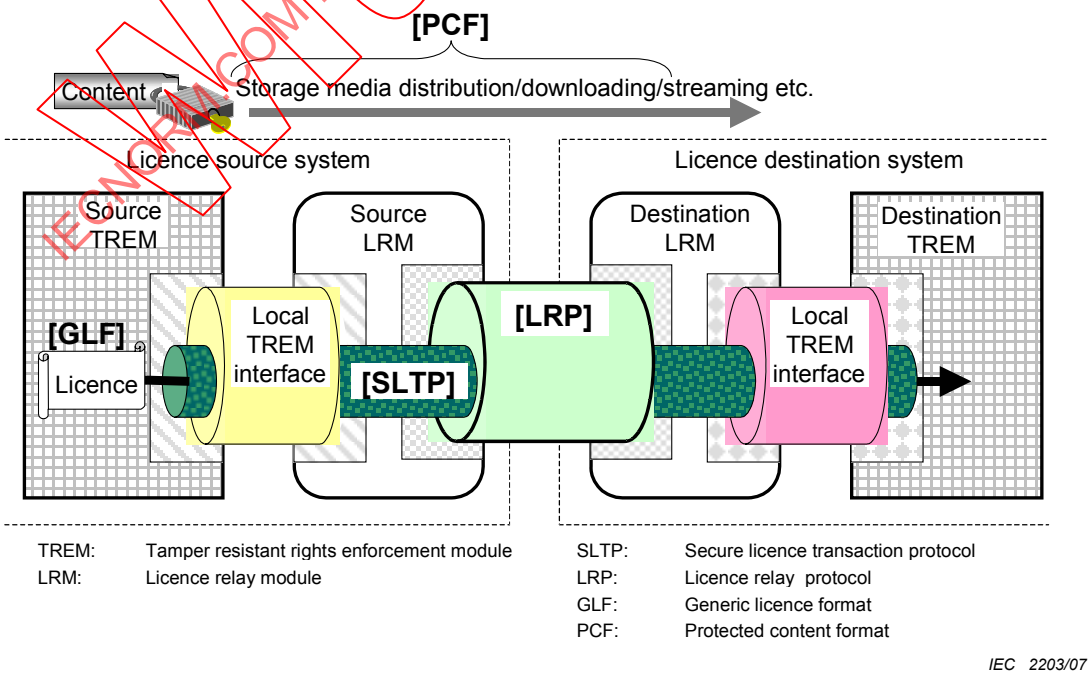


Figure 8 – Generic interconnection model for content protection

The reason why LRM and LRP are divided from TREM and SLTP is as follows.

a) The lower layer protocols (for example, local bus interface) of each local TREM class are different and various. So, if a licence is needed to be exchanged between the different classes of TREMs, it is necessary to convert each local lower layer protocol by LRM (of course, using LRP in case of exchange over the Internet).

b) Most TREMs for business are needed to be manufactured as cheap and robust TRMs. So, they can not have many functions supported in LRM.

c) If divided, the manufacturer can apply to CA for TREM alone. So, even if only the functions of LRM are extended or changed, the manufacturer does not need to apply once more.

The SLTP does not depend on the type of licence description format transferred by it. It is possible to utilize various rights expression like XrML, CCI (copy control information) and others. Whereas, in this model, generic licence format (GLF) is considered to be standardized to cover various types of services and equipment such as digital locker server, home server, set top box AV terminal, PC and mobile phone.

SLTP, LRP and GLF do not depend on the distribution method and type of the encrypted content. They are also applicable to various services such as exchanging among recording media, download and the streaming services, and it is possible to utilize various types of protected contents form depending on respective distribution services. Whereas, in this model, the protected content format (PCF) is supposed as the encrypted content format model used to exchange the content between recording media and download the content.

6.2.2 Licence relay protocol (LRP) model

LRP has not only the function of relaying the message of SLTP but also the following functions.

a) Management and recovery of licence transaction.

b) Protocol negotiation between TREMs.

c) Cooperation on user authentication and accounting.

6.2.2.1 Management and recovery of licence transaction

The LRM binds plural transaction IDs to each licence move transaction according to SLTP and manages them. When recovery of a licence transaction is required, the LRM automatically starts the recovery session for the transaction using the recovery function of SLTP. After completion of the transaction, garbage collection of the transaction resources is executed.

6.2.2.2 Protocol negotiation

The LRP supports the following negotiation functions for SLTP.

a) Version negotiation: function to negotiate versions of SLTP, LRP and the licence format used in the SLTP session.

b) Cryptosystem negotiation: function to negotiate algorithms for the public key cryptosystem and the symmetric cryptosystem used in the SLTP session.

c) Hash algorithm negotiation: function to negotiate algorithms for the hash function used in the SLTP session.

d) Character code set negotiation: function to negotiate character code set used in the SLTP session.

e) Rights script negotiation: function to negotiate rights description language or form transferred via the SLTP session.

6.2.2.3 Cooperation on user authentication and accounting

The licence destination LRM can send user authentication information to the licence source LRM as a LRP message parameter added to the destination certification message of SLTP. The licence source LRM can execute the process to cooperate with the user management function or the accounting function using the user authentication information.

6.2.3 Implementation model of inter-connection

The licence transfer system based upon LRP containing SLTP can be realized on various communication protocols through their corresponding interfaces implemented by the licence requesting agent and the licence issuing agent (Figure 9).

The licence requesting agent and the licence issuing agent get and put LRP message (which contain SLTP message) with destination LRM and source LRM respectively, and those agents exchange the LRP message between each other following the procedures defined by LRP.

One agent can exchange LRP messages with other agents through various interfaces (for example, local function/object interface, remote function/object interface, internet interface, etc.), because the LRP message is independent of any communication protocols.

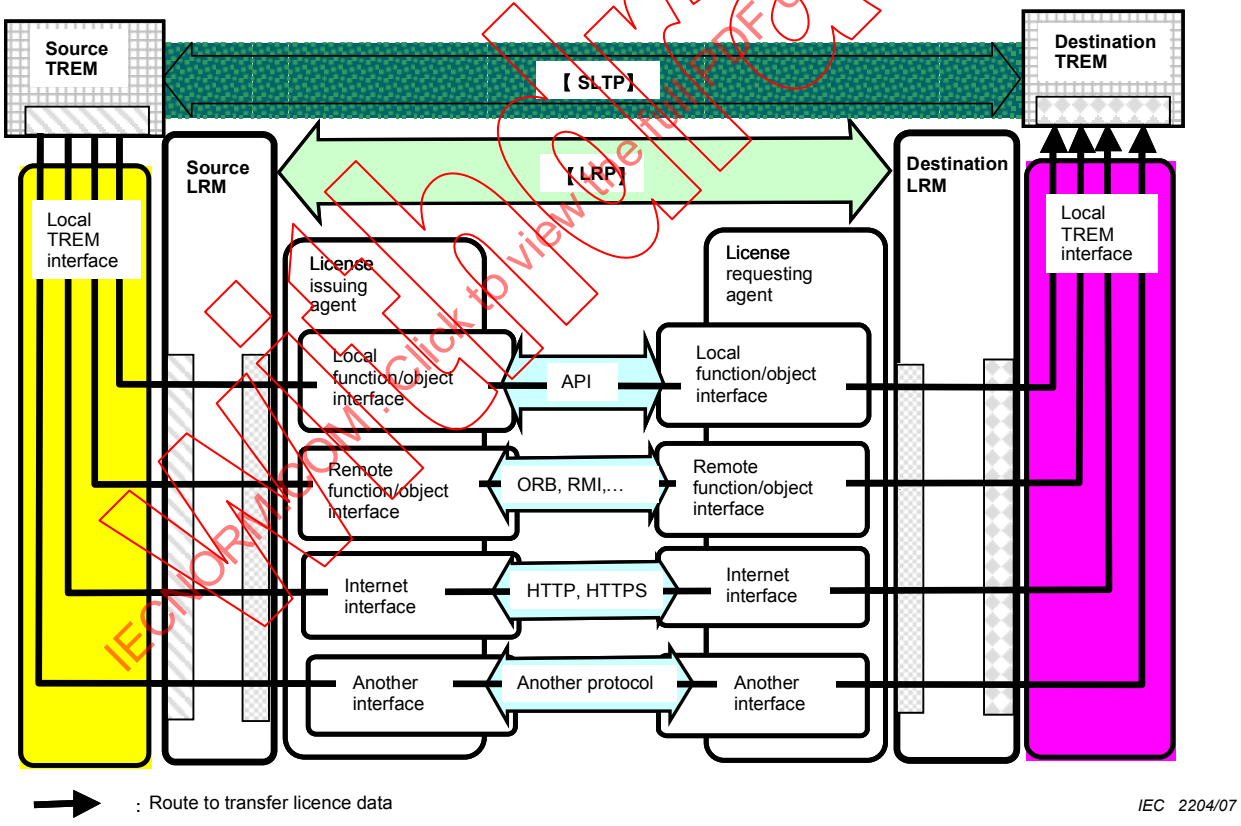


Figure 9 – Implementation model of inter-connection

In this implementation model, the licence requesting agent and the licence issuing agent implement the following functions:

- the interfaces of communication protocols to transfer the LRP message;

- the procedure to exchange LRP messages defined by LRP.

LRM implements the interfaces for the LRP message, so LRM translates the LRP message to input parameters of local TREM interface and translates output data of local TREM interface to LRP message.

6.3 Licence information model

6.3.1 Access conditions

Two types of access condition information described in Table 4 are considered in this licence information model. Both types are transferred as parameters of licence information.

Table 4 – Types of access condition

Type of access condition	Meaning	Examples
Mediator access conditions	Access conditions enforced by mediator TREM	Number to be able to play, number to be able to move and content protection level (security level)
Decoder access conditions	Access conditions enforced by decoder TREM	Size to be able to play, time limit to play, flag to prohibit editing and flag to prohibit changing speed to play

ACL is also considered in order to enforce the different content usage rule for each principal (user, user group and so on) in digital locker service and others.

6.3.2 Generic licence format (GLF) model

In this conceptual model, the generic licence format (GLF) is considered as the licence format that can be used in any content use case described in Clause 6. GLF has fields for any type of rights description and can be used in common with digital locker, home server, TV, PC, mobile phone, and so on.

In GLF model, ACL, ACL entry list, is used. ACL entry represents usage conditions for specific operation and specific principal (user, group and others). Usage conditions consist of decoder access condition (ACd) and media access condition (ACm) defined in 7.3.1. An example of the GLF structure is shown in Figure 10.

In this model, the licence has fields for content keys for each content element. The content key shall be encrypted and transferred between TREM using SLTP. ACL together with content key, Asset ID and Transaction ID shall be transferred in protected form using SLTP.