PD IEC/TS 62224:2013

BSI Standards Publication

Multimedia home server systems — Conceptual model for digital rights management

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of IEC/TS 62224:2013. It supersedes DD IEC/TS 62224:2007 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/100, Audio, video and multimedia systems and equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2013

ISBN 978 0 580 79768 2

ICS 33.160.60; 35.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2013.

Amendments issued since publication

Amd. No.	Date	Text affected

IEC/TS 62224

Edition 2.0 2013-07

TECHNICAL SPECIFICATION

colour inside

Multimedia home server systems – Conceptual model for digital rights management

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE U

ICS 33.160.60; 35.100.01

ISBN 978-2-8322-0927-1

Warning! Make sure that you obtained this publication from an authorized distributor.

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

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 technical area 8: Multimedia home server systems of IEC technical committee 100: Audio, video and multimedia systems and equipment.

This second edition cancels and replaces the first edition published in 2007 and constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) the Diffie-Hellman method concerning Secure license transaction protocol (SLTP) model has been added,

b) the Protected Content Format (PCF) model which is dependent on each service has been deleted,

c) a description related to IEC 62227 has been added,

d) the classification of certification authority has been added.

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

Enquiry draft	Report on voting
100/2005/DTS	100/2060/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 stability 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 publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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, a 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 class home servers in private homes, also.

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. These matters have emerged as important social issues.

The targets of management by DRM technology are these digital licenses, such as copyrights. Essentially, these licenses should not only be protected but also promote re-creativity and should be broadly used as the property shared by the human race. Thus, the licenses with these characteristics should be managed and protected by a DRM system that follows open interoperable specifications shared throughout the world.

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 between the DRM module, the description of specifications for license information and encrypted contents format.

During the development of this model, much consideration was given to the usage of contents in consumer electronics equipment connected with home servers. In addition, particular attention was given to distribution, storage exchange and usage of content between distribution servers and the client destination system, allowing for conditions approved by the rights holder, but nevertheless without loss of convenience for the users. The standardization and its popularization based on this model will enable inter-connection between DRM modules allowing strong contents protection in various content network sharing systems or content distribution services over 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 the protocol specification to exchange license information between DRM modules. This Technical Specification also outlines which models should be defined as standard models as well as the standard meanings (mainly from the viewpoint of information security in the environment, including home server systems).

2 Normative references

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

IEC 62227:2008, *Multimedia home server systems – Digital rights permission code* Amendment 1:2012

ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory:Public-key and attribute certification framework*

ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

ITU-T Recommendation X.509:1997, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

RFC 3280 R. Housley (RSA Laboratories), W. Ford (VeriSign), W. Polk (NIST), D. Solo (Citicorp), *Request for Comments: 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Category: Standards Track* (April 2002), *http://rfc.slim.summitmedia.co.uk/rfc2380.html*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 9594-8:2008, as well as the following apply.

3.1
access condition
information that describes the content usage conditions

Note 1 to entry: 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 license for the content.

3.2
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

EXAMPLE A particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

[SOURCE: ISO/IEC 9594-8:2008, 3.4.10, modified, i.e. aligned to new requirements for terms and definitions.]

3.3
certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

Note 1 to entry: Optionally the certification authority may create the users' keys.

[SOURCE: ISO/IEC 9594-8:2008, 3.4.17, modified, i.e. aligned to new requirements for terms and definitions.]

3.4
certificate revocation list
certification authority revocation list
CARL
revocation list containing a list of public-key certificates issued to certification authorities that are no longer considered valid by the certificate issuer

[SOURCE: ISO/IEC 9594-8:2008, 3.4.18]

3.5
content identifier
identifier which is a unique value assigned to each content that is a unit of information provided by the content holder

3.6
content key
content encryption key unique to each content

Note 1 to entry: A content key is a key under the symmetric key cryptosystem.

3.7
data concatenation
concatenation of two bit-streams into a single bit-stream

Note 1 to entry: The first bit of the second original stream is next to the last bit of the first original stream.

3.8
decoder TREM
TREM in which encrypted content can be decrypted and played

3.9
destination TREM
TREM receiving a license

3.10
digital rights management
technology or functions to protect rights relating with digital content, for example, copyright, or system, or module that provide these functions

Note 1 to entry: Inside this system or module it manages content access conditions and behaves under these conditions.

3.11
encrypted content
encrypted content data with its related meta data, such as broadcasting content, download content, streaming content, and so on

3.12
entry TREM
TREM that has the function of generating a new license according to indication from outside and behaves as a source TREM

Note 1 to entry: An entry TREM is inside the license distribution server, and so on.

3.13
hash function
mathematical function which maps values from a large (possibly very large) domain into a smaller range

Note 1 to entry: A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.

[SOURCE: ISO/IEC 9594-8:2008, 3.4.35, modified, i.e. aligned to new requirements for terms and definitions]

3.14
license
information including one or more content keys and authorization information like access conditions, etc.

Note 1 to entry: If it is outside a TREM, it shall be a protected license, which is protected with session key generated in accordance with SLTP.

3.15
license identifier
identifier which is a unique value assigned to each license

3.16
license move
moving of a license from one TREM to another

Note 1 to entry: Once the license is moved, the license is deleted from the source TREM. A license move with the encrypted content copy equals a content move.

3.17
license relay module
LRM
system or module that relays a protected license between TREMs through an SLTP session

Note 1 to entry: LRM is an endpoint of an LRP connection and has the function of controlling internal bus and network in order to relay the protected license via the LRP connection.

3.18
license relay protocol
LRP
protocol between LRMs

Note 1 to entry: Over this protocol, secure license 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.

3.19
license server
server system that has a TREM and the LRM which mediates the transmission of a license issued by the TREM

3.20
license transaction
unit of processing to distribute, move or copy a license

Note 1 to entry: For each transaction, the different resources are assigned and managed.

3.21
license transfer
moving or copying a license from the TREM to the other TREM

3.22
mediator TREM
TREM that mediates license transfer as a main role

Note 1 to entry: It has both roles as destination and source TREMs.

3.23
protected license
license information protected to transfer between TREMs

Note 1 to entry: A protected license includes encrypted content keys and protected authorization information.

3.24
public key cryptosystem
cryptosystem in which encryption key and decryption key are different

Note 1 to entry: When concealing the data, the key used for encryption is publicly distributed. RSA and elliptic curve cryptosystem are well known as public key cryptosystems.

3.25
secure license transaction protocol
SLTP
protocol to transfer license information securely between TREMs

Note 1 to entry: This protocol consists of formats of the information exchanged between TREMs and a state transition specification of the TREM, which shall be implemented.

3.26
session private key
temporary private key which is used to share a session symmetric key between TREMs at each SLTP session

3.27
session public key
temporary public key which is used to share session symmetric key between TREMs at each SLTP session

3.28
session symmetric key
temporary symmetric key shared between TREMs at each SLTP session

3.29
SLTP session
secure session generated between TREMs according to the SLTP in order to transfer license

Note 1 to entry: Each SLTP session has a session symmetric key shared by both sides of the TREMs.

3.30
source TREM
role of a TREM as a TREM issuing a license

3.31
symmetric key cryptosystem
cryptosystem in which the same key is used to encrypt and decrypt the data

Note 1 to entry: Advanced Encryption Standard (AES) standardized by NIST in the U.S.A. is a well-known symmetric key cryptosystem.

3.32
tamper resistant module
TRM
module to protect from analysis or modification of information and its processing

Note 1 to entry: See [FIPS 140-2].

3.33
tamper resistant rights enforcement module
TREM
system or module which has functions of digital rights management

Note 1 to entry: TREM is structured as a tamper resistant module. TREM has functions to enforce rights, manage license and process the license transfer according to SLTP.

3.34
transaction identifier
identifier that is assigned to each license transaction

3.35
transaction log
log data representing the status of a license transfer transaction and the license issued in that transaction

Note 1 to entry: It is securely stored in the TREM.

3.36
TREM private key
TREM individual private key
key kept privately by each TREM individually

3.37
TREM public key
TREM individual public key
public key corresponding to a TREM (individual) private key

4 Abbreviations

AES	Advanced Encryption Standard
CA	Certification Authority
CCI	Copy Control Information
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

ID	IDentifier
LRM	License Relay Module
LRP	License Relay Protocol
PCF	Protected Content Format
SLTP	Secure License Transaction Protocol
T-DES	Triple DES
TID	Transaction IDentifier
TREM	Tamper-resistant Rights Enforcement Module
TRM	Tamper Resistant Module

5 Notation

5.1 Numerical values

In this Technical Specification, the following expressions of numerical values are used as shown in Table 1.

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

5.2 Notation list

This Technical Specification uses the following notations as shown in Table 2.

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	KR	A private key securely maintained by root CA
Root public key	KPR	The public key corresponding to KR
Private key of CA	KCi	A private key securely maintained by CA ”i” which is the issuer of the certificate of lower tier CA or the certificate of TREM public key (This does not include root private key.)
Public key of CA	KPCi	The public key corresponding to KCi (This does not include root public key.)
TREM private key for detecting SLTP message tampering	KTdk	A key that the TREM “k” keeps individually and secretly. This key is used to generate digital signature for detecting SLTP message tampering.
TREM public key for detecting SLTP message tampering	KPTdk	The public key corresponding to KTdk. This key is used to verify the digital signature that is generated by using KTdk.

Name	Expression	Description
TREM private key for sharing session symmetric key with other TREM	KTsk	A key that the TREM “k” keeps individually and secretly. This key is used to share a session symmetric key with other TREM.
TREM public key for sharing session symmetric key with other TREM	KPTsk	The public key corresponding to KTsk. This key is used to share a session symmetric key with other TREM.
Relevant information	Ir	The information relating to root CA
	Ici	The information relating to CA “i” other than root CA
	Itxx	The information relating to the public key of TREM KPTxx
Certificate	C (KR, KPR || Ir)	A certificate of a root public key KPR KPR || Ir || E(KR, H(KPR || Ir))
	C (KR, KPCi || Ici)	A certificate of a public key KPCi issued by root CA whose private key is KR KPCi || Ici || E(KR, H(KPCi || Ici))
	C (KCi, KPCj || Icj)	A certificate of a public key KPCj issued by CA “i” whose private key is KCi KPCj || Icj || E(KCi, H(KPCj || Icj))
	C (KCj, KPTxx || Itxx)	A certificate of a public key KPTxx issued by CA “j” whose private key is KCj KPTxx || Itxx || E(KCj, H(KPTxx || Itxx))
Session private key	KTTkn	A temporary private key generated in TREM “k” per each SLTP session “n”. This is used to share session symmetric key between TREMs at SLTP session “n”.
Session public key	KPTTkn	A temporary public key corresponding to KTTkn. This is used to share session symmetric key between TREMs at SLTP session “n”.
Session symmetric key shared between TREMs	KSk1k2n	A temporary symmetric key which is shared between TREM “k1” and TREM “k2” at SLTP session “n” by using public key cryptosystem.
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

Diffie-Hellman method	DH(KPTTk1n, KTTk2n, epx)
	=
	DH(KPTTk2n,KTTk1n, exp)
		Session symmetric key which is shared between TREM “k1” and TREM “k2” at SLTP session “n” by using Diffie-Hellman method.
		epx: encryption parameter “x” of public key cryptosystem

6 Requirements

6.1 License service model

6.1.1 General

The following functional requirements for the license service model are considered as described in Figure 1:

a) content is encrypted and distributed in any way;

b) the license information includes content keys and access conditions (ACs);

c) once created by rights holder, encrypted content and protected license is decrypted only in TREM (tamper resistant rights enforcement module);

d) the license information is protected by cryptosystem outside TREMs and shall be moved among TREMs according to the AC of itself;

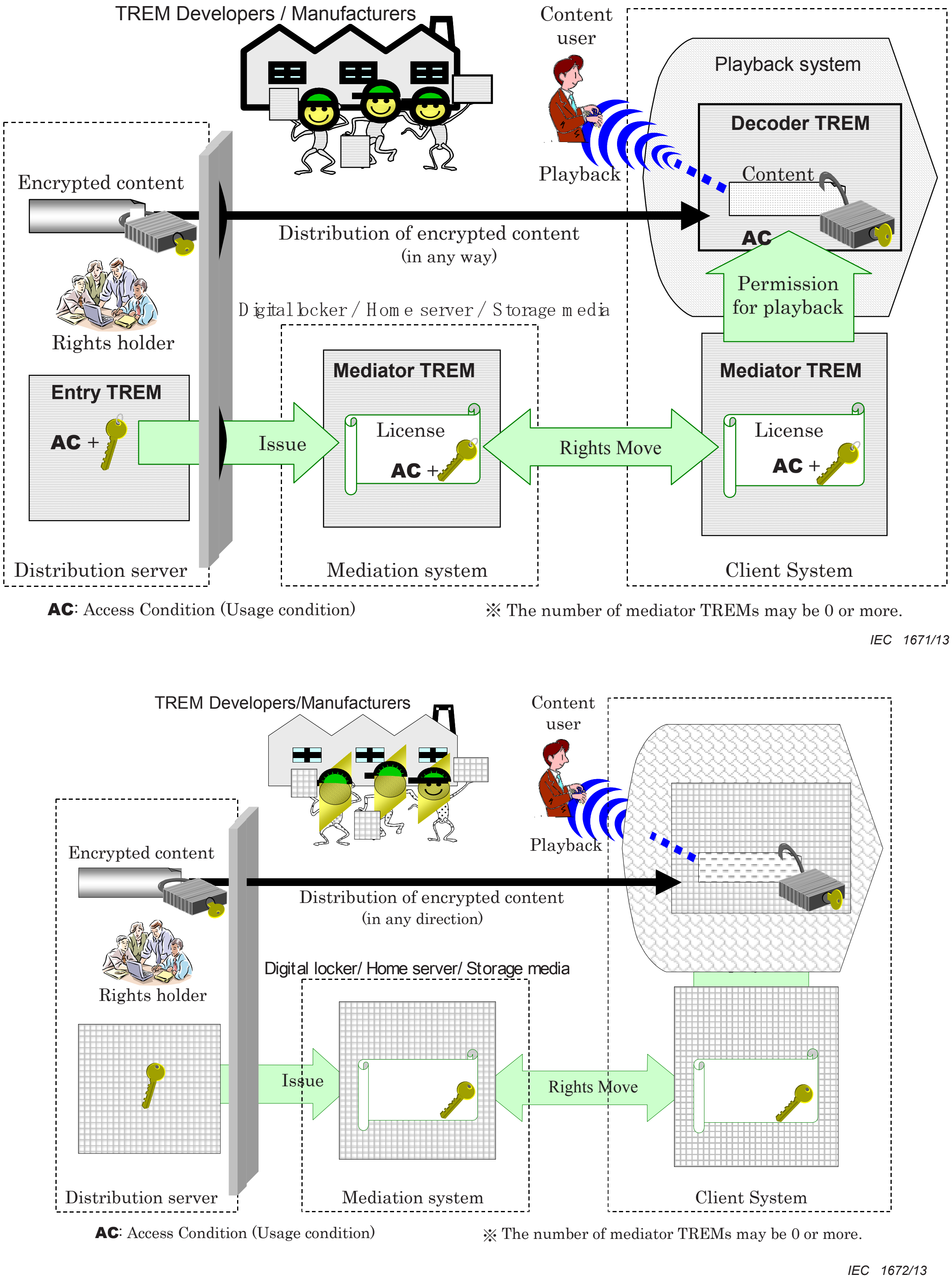
e) a role to issue the moved license is called source TREM and a role to receive the moved license is called destination TREM;

f) the TREM processes user request according to the AC in the license;

g) an entry TREM (see 3.12) in such as content management/distribution server can receive plain content data and plain license information, and can create the encrypted content and the protected license information and behave as a source TREM;

h) a mediator TREM (see 3.22) in a content/license mediation system behaves as both source and destination TREMs; and

i) a decoder TREM (see 3.8) in such as a playback system can receive the license from the other TREM and decrypt encrypted contents according to the AC included in the license.



AC: Access Condition (Usage condition) ※ The number of mediator TREMs may be 0 or more.

AC: Access Condition (Usage condition) ※ The number of mediator TREMs may be 0 or more.

Figure 1 – License service model to consider the threats

6.1.2 Threats and countermeasures

6.1.2.1 General

Table 3 shows threats in the license service environment described in 6.1 and countermeasures against each threat.

Table 3 – Threats and countermeasures in the license service model

Subject	Attack (threat)		Countermeasures	
TREM user and network user	Analysis of TREM		a) Manufacturing TREM as TRM.	
	Camouflage	Camouflage of the destination TREM	b) Encryption with session key shared after mutual authentication by the certificates of both destination and source TREMs.	
		Replay (camouflage of the source TREM)		
		Camouflage of disconnection of license transaction session	c) Comparison between logs in each TREMs.	
	Leakage of private key for the CA or the TREM		d) Issue of CRL	Key renewal.
TREM manufacturer	Illegal manufacturing			Termination of the broken or illegal TREM.
	Leakage of key information			

6.1.2.2 Manufacturing TREM as TRM

TREM shall be TRM (tamper resistant module) in order to prevent the content user from analyzing the TREM and stealing the secret keys from it.

6.1.2.3 Encryption with session key

In the license distribution service, impersonation of the TREM such as replay attack by camouflage of the license 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 charged license shall be encrypted with the session key shared after the mutual authentication of the source and destination TREMs using TREM public keys for detecting SLTP message tampering.

6.1.2.4 Comparison between logs

It is necessary that the license transaction logs are securely stored in the TREM. When the session to transfer/move a license is disconnected and the recovery of the session to send the license 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 license was already received by the destination or not. Otherwise, anyone may camouflage the unauthorized copy of license with the session recovery.

There are many possibilites of unexpected disconnections that may occur during the process of purchasing licenses through communication networks. This may especially happen in wireless mobile networks. If there is no countermeasure for this type of threat, a distributor could only repeatedly send licenses to a deceitful TREM camouflaged with the legally disconnected TREM. Because not only a disconnection may have occurred, but also because there is no evidence that the license was received, the source TREM shall certainly deliver the license to the destination in exchange for accounting or decrease of the rights.

6.1.2.5 Issue of CRL

CRL (certificate revocation list defined in ITU Recommendation X.509 and ISO/IEC 9594-8) can be used in order to terminate the use of illegal or broken keys and TREMs. On description of CRL, see RFC 3280.

6.1.3 Evaluation criteria

In order to realize a secure content protection environment, it is necessary that the security evaluation criteria for TREM are specified. The security criteria for content protection should be compliant with ISO/IEC 15408-1 and include the following:

- the security functions for content protection described in 6.1.2;
- indications, if the necessary algorithms for cryptosystem, hash function and function to generate random numbers are properly implemented;
- indications with respect to the robustness of TRM for TREM, for example, the security level of TRM compliant with FIPS 140-2; and
- a description of the process to design, develop and manufacture the TREM.

7 Design considerations

7.1 General

In this clause the following conceptual models satisfying the requirements described in Clause 6 are specified:

a) security model;
b) interconnection model; and
c) license information model.

7.2 Security model

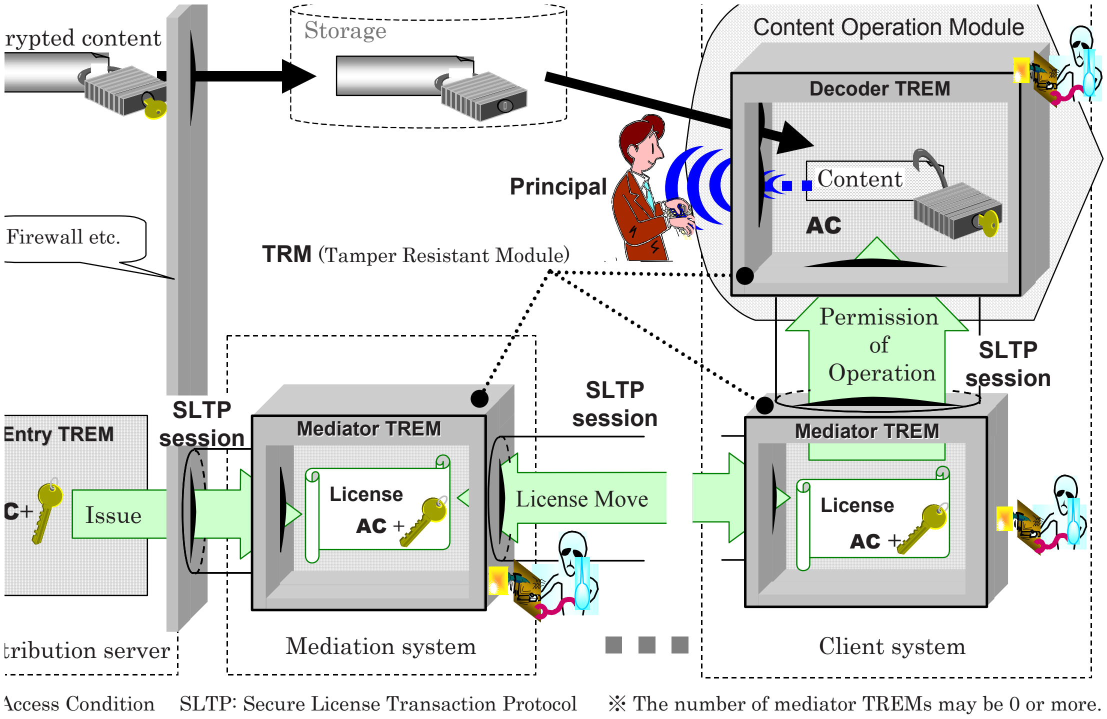
7.2.1 General

In this subclause, a security model satisfying the requirements described in 6.1.2 is specified.

7.2.2 Overview of security model

In the security model (see Figure 2) of this conceptual model, content to be protected is encrypted and distributed in any way. Also, in this model, the content encryption key and the rights information including access conditions (AC) for the content are protected using TRM and cryptosystem and have the following lifecycle as a license:

a) the license is created in an entry TREM;
b) the license is at first issued as a protected license from the entry TREM;
c) the license is transferred to a decoder TREM through more than 0 mediator TREMs; and
d) the license is used to decryption of the content according to the AC in the decoder TREM.



IEC 1673/13

Figure 2 – Security model of content protection

7.2.3 TREM functions

The TREM shall have the following functions:

a) tamper resistant function preventing leakage of license information as a TRM;

b) function to create and maintain the SLTP session;

c) function to move license between TREMs always using the SLTP session;

d) in case of mediator TREM, function to decrypt the license and transfer it to other TREM according to the protected mediator access conditions (AC); and

e) in case of decoder TREM, function to decrypt the license and decrypt the content with the decrypted key according to the protected decoder access condition.

7.2.4 Secure license 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 license transaction protocol between TREMs. Standardization and implementation of SLTP are needed also as countermeasures especially those described in 6.1.2.3 and 6.1.2.4.

SLTP is a protocol to transfer license information securely between TREMs. This protocol shall consist of formats of the information exchanged between TREMs and a specification of state transition inside the TREM.

In the basic normal sequence of the SLTP model, the following messages are exchanged in accordance with the following steps (see Figure 3) to generate the SLTP session as the countermeasures described in 6.1.2.3 and secret data is transferred through the SLTP session securely.

a) Generating SLTP session

- Preparing for detecting SLTP message tampering:

The certificate of TREM public key for detecting SLTP message tampering is sent from a message sender TREM to a message receiver TREM and checked at the receiver TREM.

For example, C(KR,KPCi || Ici),C(KCi,KPCj || Icj) and C(KCj,KPTdk || Itdk) are sent from sender TREM to the receiver TREM, where C(KR,KPCi|| Ici) and C(KCi,KPCj || Icj) are certificates constructing PkiPath and C(KCj,KPTdk || Itdk) is the certificate of sender TREM (TREM "k" is the sender TREM).

Then the environment for detecting message tampering by using digital signature has been generated between sender TREM and receiver TREM.

- Sharing a session symmetric key:

  The destination and the source TREMs share a session symmetric key. There are several methods to share and the following are principal examples of these methods:

  1) By using a TREM private key and public key for sharing a temporary key

     First, source TREM receives the certificates C(KR,KPCi || Ici),C(KCi,KPCj || Icj) and C(KCj,KPTsk1 || Itsk1) of the destination TREM "k1" and checks those certificates. Then, the source TREM "k2" creates a session symmetric key KSk1k2n and encrypts it with KPTsk1. Finally, the source TREM sends the encrypted session symmetric key to the destination TREM.

  2) By using a session private key and a session public key

     The destination TREM "k1" creates a session public key "KPTTk1n" and a session private key "KTTk1n" and, similarly, the source TREM "k2" creates a session public key "KPTTk2n" and a session private key "KTTk2n". Then, both of those TREMs derive a common session symmetric key "KSk1k2n" by exchanging each other's session public keys by using the Diffie-Hellman method.

Source TREM "k2": DH(KPTTk1n, KTTk2n , epx)

↓

KSk1k2n

↑

Destination TREM "k1": DH(KPTTk2n, KTTk1n , epx)

b) Transferring secret data through an SLTP session

- Secret data is encrypted with shared session symmetric key:

  Secret data is encrypted with a shared session symmetric key in the sender TREM and the encrypted secret data is sent from the sender TREM to receiver TREM

  E(KSk1k2n, SD)

  SD: Secret data.

- Message data is checked by using digital signature:

  Message data are appended digital signatures of the sender TREM, and the receiver TREM checks it

  MD || E(KTdk1, H(MD))

  KTdk1: TREM private key for detecting SLTP message tampering of

  TREM "k1"

  MD: Message data.

c) Closing SLTP session

Generated SLTP session is closed explicitly or implicitly (for example: closed by “time out” or new request from same TREM).

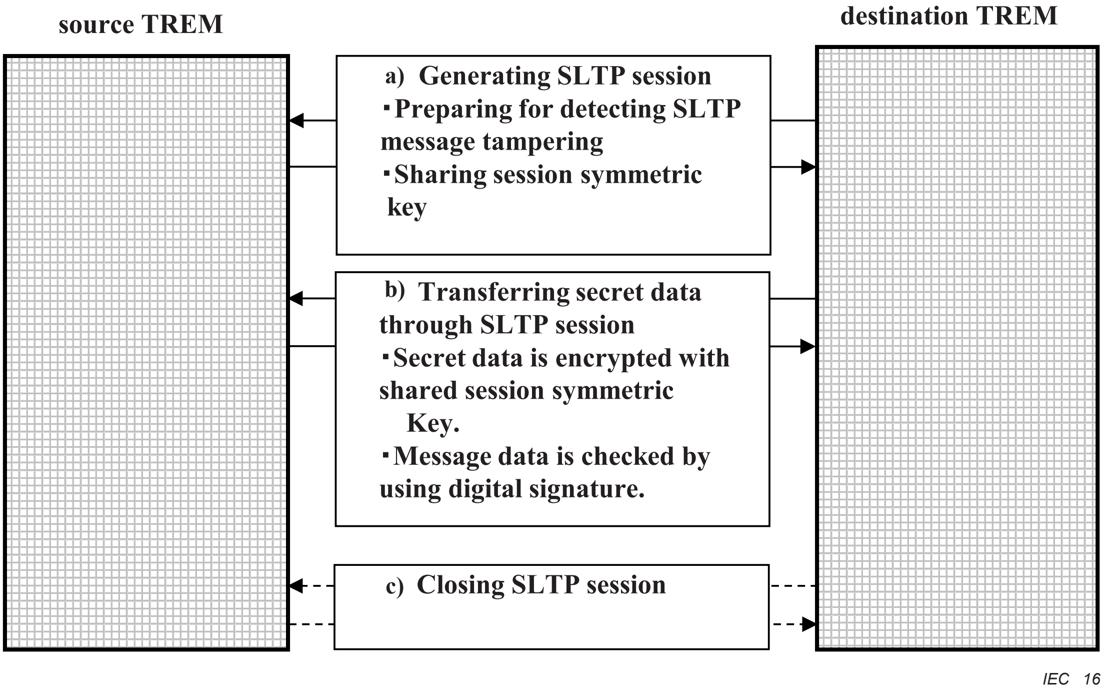

source TREM
destination TREM
a) Generating SLTP session
・Preparing for detecting SLTP message tampering
・Sharing session symmetric key
b) Transferring secret data through SLTP session
・Secret data is encrypted with shared session symmetric Key.
・Message data is checked by using digital signature.
c) Closing SLTP session
IEC 1674/13

Figure 3 – 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 their generation and values and shall be difficult to be figured out within the period significant for the attackers.

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

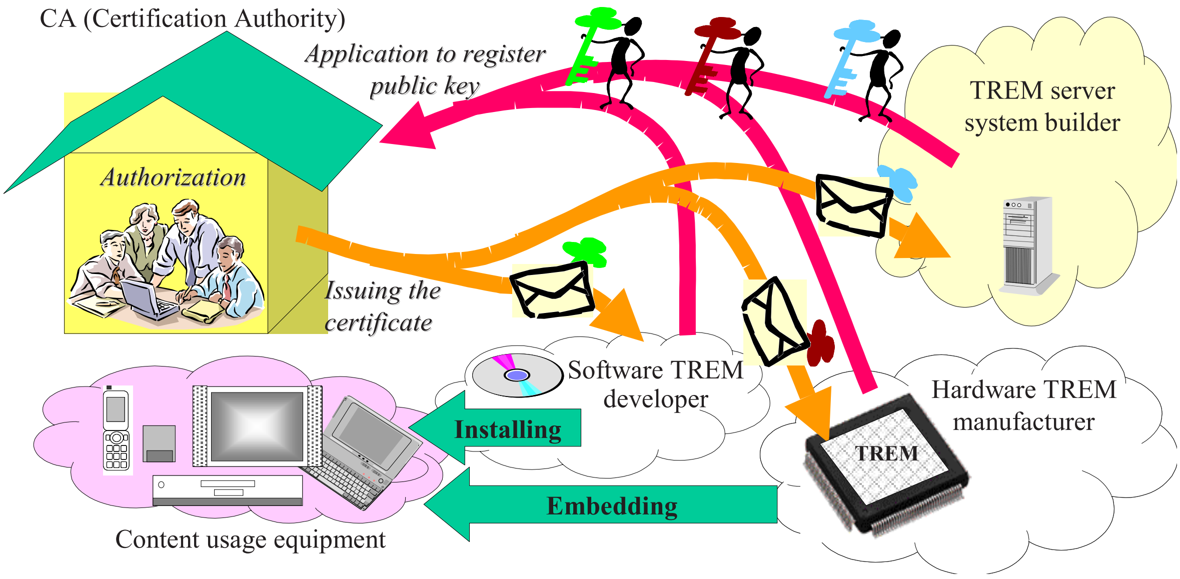
Countermeasures described in 6.1.2.4 should be taken for secure recovery of the SLTP session.

7.2.5 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 to apply them to the class public key with the relating information to the CA (certification authority).

If the CA has confirmed that the application information is correct and the TREM conforming to the security criteria is properly manufactured (or structured), the CA creates a certificate for the TREM class public key and its relating information in accordance with [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 is able to receive the license moved from another class of the TREM that is already authorized by the same CA (see Figure 4).


CA (Certification Authority)
Application to register public key
Authorization
Issuing the certificate
TREM server system builder
Software TREM developer
Hardware TREM manufacturer
TREM
Installing
Embedding
Content usage equipment

IEC 1675/13

Figure 4 – Overview of issuing TREM class certificates

7.2.6 Key revocation and termination of the TREM

The key revocation and termination of the TREM by CRL (certificate revocation list, defined in ITU Recommendation X.509 and ISO/IEC 7498-1) shall be supported in this security model because of the requirements described in 6.1.2.5.

The CRL is a list of identifiers of revoked certificates with a digital signature from the CA. The CRL is used as follows:

a) after it has been issued from the CA, the CRL is embedded into the TREMs, especially entry TREMs;

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

7.3 Interconnection model

7.3.1 Generic interconnection model

In this interconnection model (see Figure 5), the license relay module (LRM) relays the license protected by the SLTP session between TREMs. The LRM is a system or module that controls the internal bus and network in order to relay a protected license between TREMs through an SLTP session. However, the protected license can neither be decrypted nor be interpreted by the LRM.

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

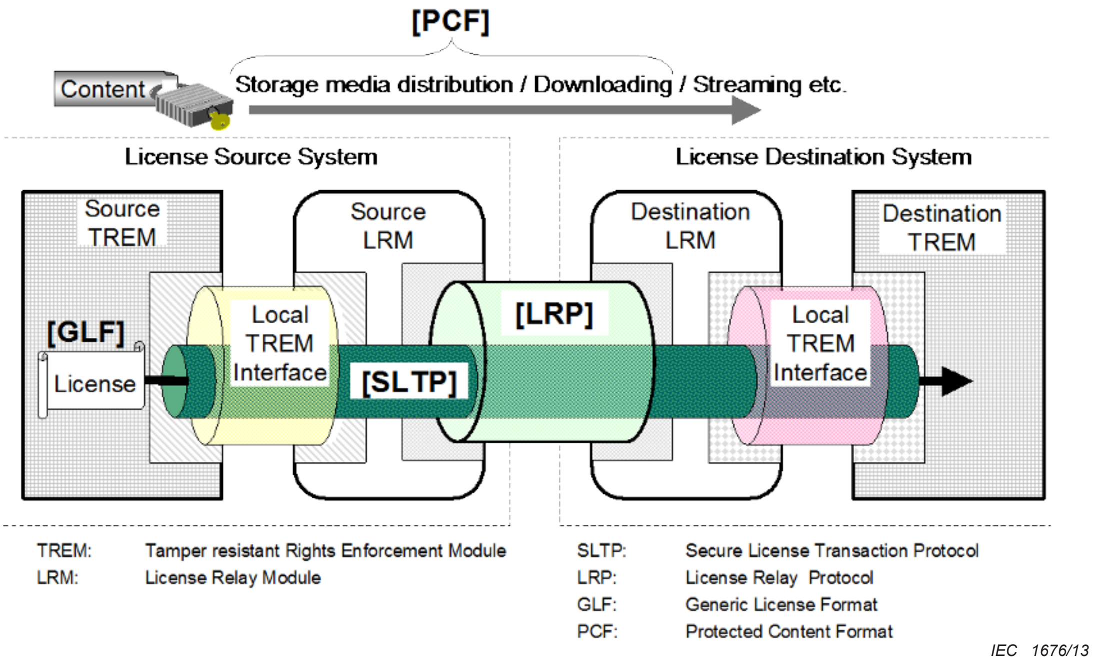

[PCF]
Content
Storage media distribution / Downloading / Streaming etc.
License Source System
License Destination System
Source TREM
Source LRM
Destination LRM
Destination TREM
[GLF]
License
Local TREM Interface
[SLTP]
[LRP]
Local TREM Interface
TREM: Tamper resistant Rights Enforcement Module
LRM: License Relay Module
SLTP: Secure License Transaction Protocol
LRP: License Relay Protocol
GLF: Generic License Format
PCF: Protected Content Format
IEC 1676/13

Figure 5 – Generic interconnection model for content protection

The following reasons explain why LRM and LRP are separated from TREM and SLTP:

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

b) most TREMs for businesses need to be manufactured as cheaply and robustly as TRMs. So, they cannot have many functions supported in LRM; and

c) if divided, the manufacturer can carry out only an issue application of a TREM to a CA. So, even if only the functions of the LRM are extended or changed, the manufacturer does not need to apply it again.

The SLTP does not depend on the type of license description format transferred by it. It is possible to utilize various rights expressions like XrML, CCI (copy control information) and others.

SLTP, LRP do not depend on the distribution method and type of the encrypted content. They are also applicable to various services such as exchanges among recording media, and download and the streaming services. It is also possible to utilize various types of protected content from dependent respective distribution services.

7.3.2 License relay protocol (LRP) model

7.3.2.1 General

A LRP has not only the function of relaying the message of SLTP, but also the following functions:

a) management and recovery of license transaction;

b) protocol negotiation between TREMs; and

c) cooperation on user authentication and accounting.

7.3.2.2 Management and recovery of license transaction

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

7.3.2.3 Protocol negotiation

The LRP supports the following negotiation functions for SLTP

a) version negotiation: function to negotiate versions of SLTP, LRP and the license 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 the character code set used in the SLTP session; and

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

7.3.2.4 Cooperation on user authentication and accounting

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

7.3.3 Implementation model of inter-connection

The license transfer system based upon LRP containing SLTP can be realized on various communication protocols through their corresponding interfaces implemented by the license requesting agent and license issuing agent (see Figure 6).

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

One agent can exchange a LRP message with another agent through various interfaces (e.g. the local function/object interface, remote function/object interface, internet interface, etc.), because the LRP message is independent of any communication protocols.

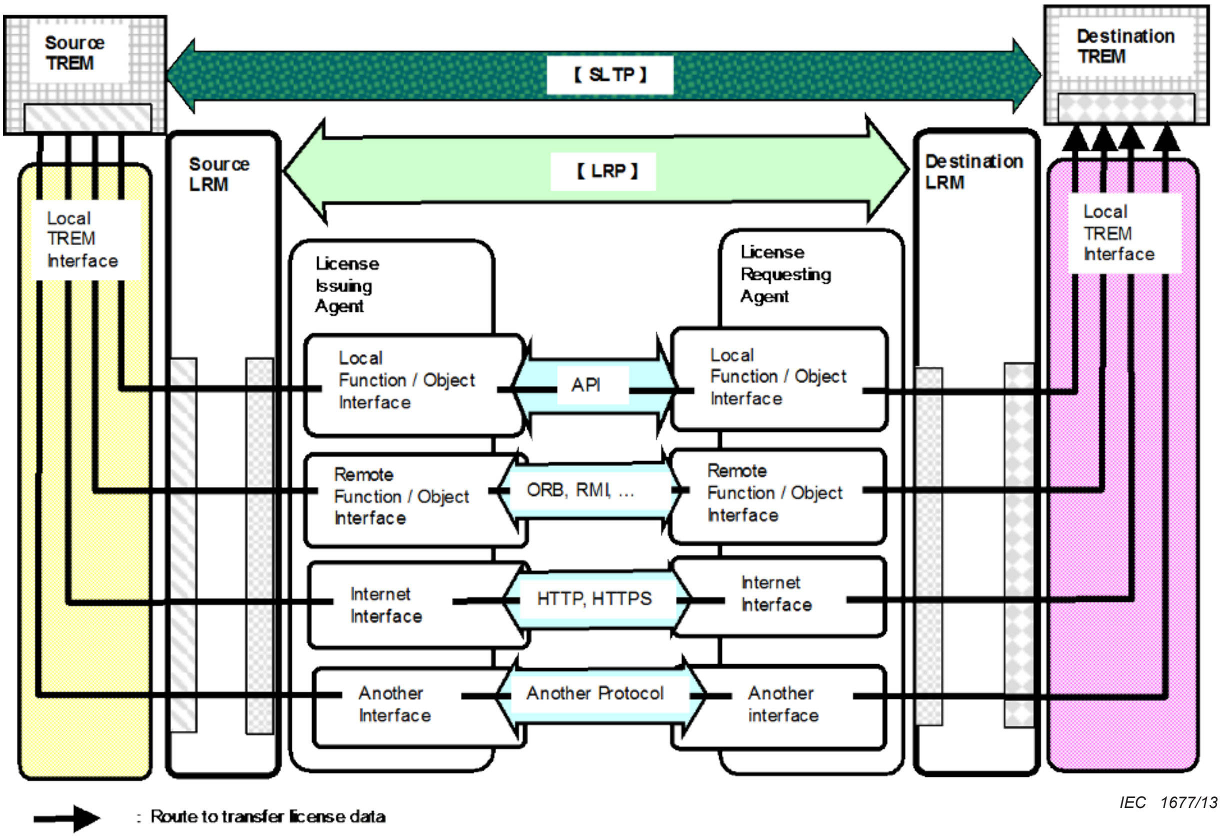


Figure 6 – Implementation model of interconnection

In this implementation model (see Figure 6), the license requesting agent and license issuing agent implement the following functions:

- the interfaces of communication protocols to transfer LRP messages;
- the procedure to exchange LRP messages defined by LRP.

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

7.4 License information model

7.4.1 General

Digital rights permissions data is a code or expression language which has various sets of permission information and permission conditions for digital content transmission. Digital rights permissions data and license information can be distributed independently to client systems.

Digital rights permission data shall be detected whether or not those have been falsified by any one, so the distribution format data should involve digital signature. The digital certificates for the public key which correspond to the private key used for the digital signature shall be distributed from a CA (certificate authority). The CA can be a root CA or the intermediate CA traced through its root CA. Each TERM shall verify the digital signature by using the digital certificates. The digital certificates can be verified by tracing the root CA. The concrete standard of the signature should depend on each service system.

7.4.2 Digital rights permissions data

Digital rights permission data has some components and elements under their components. An example of the syntaxes is shown in IEC 62227:2008.

8 Issues to be standardized

To realize DRM systems conforming to the model shown in Figure 1, it is necessary to specify the following, considering that the specifications are processed in the equipment such as general home appliances, PC, home servers and mobile phones and so on:

a) SLTP (secure license transaction protocol);

b) LRP (license relay protocol);

c) evaluation criteria for TREM (by which the CA judges whether to authorize the TREM or not).

The above-mentioned specifications shall satisfy the requirements described in Clause 6.

Annex A
(informative)

Example of algorithms for cryptosystem and hash

The SLTP specifies neither cryptosystems nor hash algorithms. In case of implementation of this model, it is necessary to specify security evaluation criteria for algorithms. For example, the following cryptosystems and hash algorithms may be used.

- Symmetric key cryptosystem:
  - Triple DES cryptosystem with two keys, EDE and outer-CBC Mode specified in [1][1], [2] and [3].
  - AES CBC mode, see [7].
- Public key cryptosystem:
  - Cryptosystem using elliptic curve over binary field (163 bits) NIST recommended parameters, see [8].
  - Cryptosystem using elliptic curve over prime field (256 bits) NIST recommendation parameter, see [6].
  - RSA public key cryptosystem, see [10].
- Hash algorithm:
  - SHA-1, SHA-256, SHA-384, SHA-512, see [5].

The following algorithms can be used to realize the encryption, decryption and digital signature function using the elliptic curve cryptosystem:

- Encryption and decryption: EC-DH (Elliptic curve DH) and Triple-DES or AES specified in [8].
- Digital signature: EC-DSA specified in [8].

The following key length for each cryptosystem is recommended in this model.

- Symmetric key cryptosystem: more than 112 bits;
- Public key cryptosystem:
  - elliptic curve cryptosystem: more than 160 bits,
  - RSA cryptosystem: more than 1 024 bits.

[1] Numbers in square brackets refer to the Bibliography.

Annex B
(informative)

Example of conversion of rights information in DRM based upon SLTP into that of existing DRM

The SLTP is an open interoperable specification and implements highly expandable PKI based DRMs, so any manufacturers of existing DRMs can implement the TREM that converts the rights information in SLTP DRM into that of the existing DRM. The TREM converting the rights information shall implement both SLTP and existing DRM protocol.

Figure B.1 and Figure B.2 specify the examples of the conversion of the rights information.

Example of Conversion of Rights Information in DRM based upon SLTP into That of Existing DRM

(1) Static Conversion :

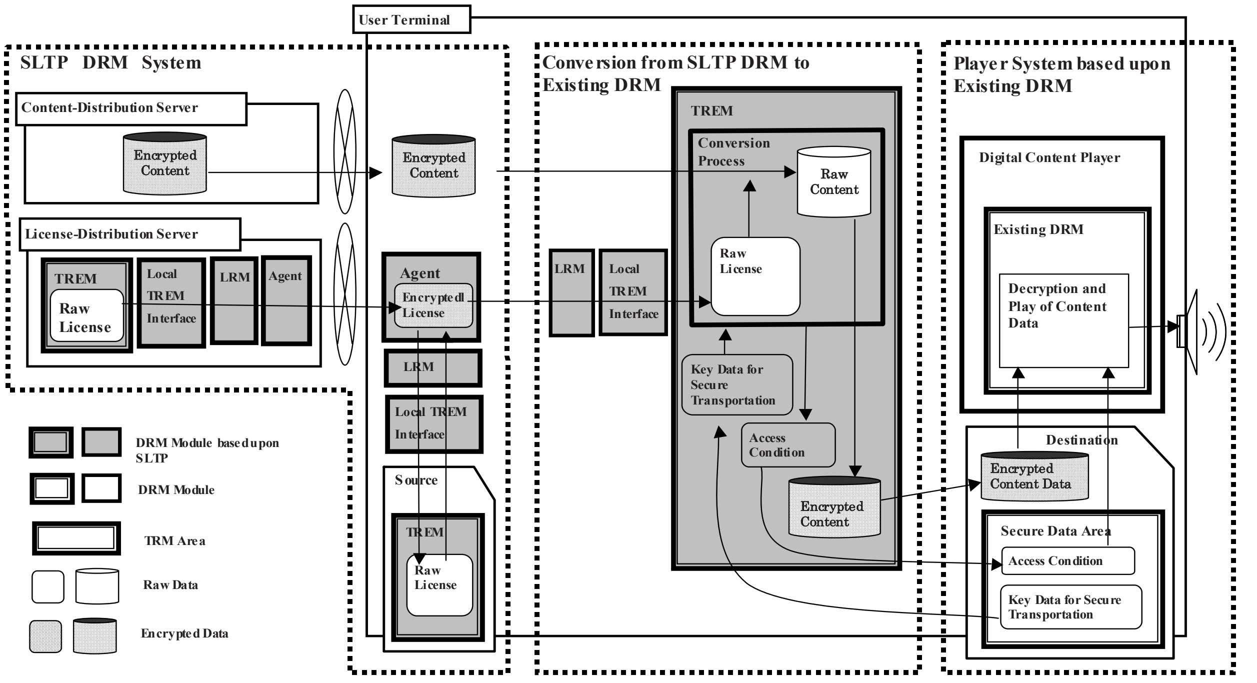


Figure B.1 – Example of static conversion of rights information

Figure B.1 specifies an example of static conversion of rights information. First, the rights information (license) is distributed from the SLTP license server and stored into the TREM that is implemented in a storage medium through the LRP containing the SLTP. Next, the rights information (license) is transported from the TREM in the storage medium to the other TREM implementing the conversion through the LRP containing the SLTP. Finally, the rights information is converted to that of the existing DRM in the TREM implementing the conversion.

Example of Conversion of Rights Information in DRM based upon SLTP into That of Existing DRM

(2) Dynamic Conversion :

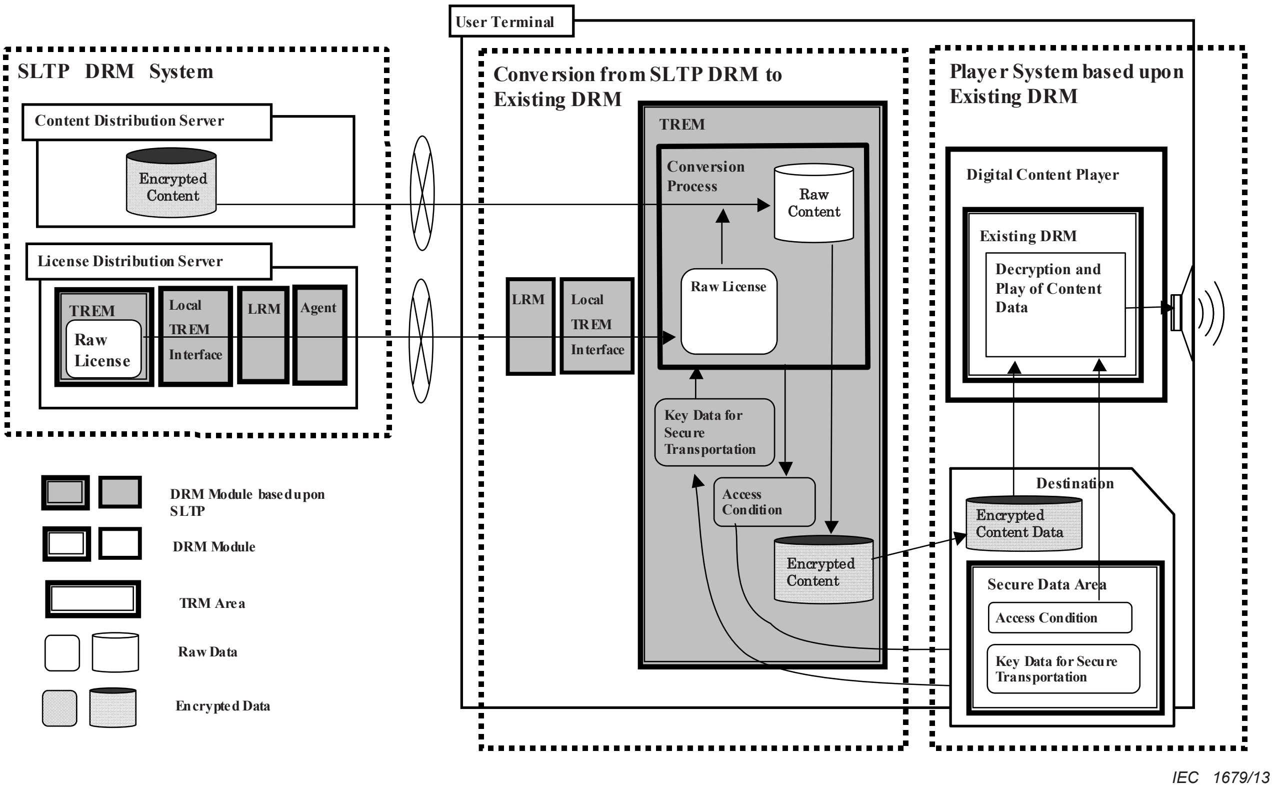


Figure B.2 – Example of dynamic conversion of rights information

Figure B.2 specifies an example of dynamic conversion of rights information. The rights information (license) is distributed from the LRP containing the SLTP license server to the TREM implementing the conversion, and the rights information is converted to that of the existing DRM dynamically in that TREM.

Bibliography

The following documents have served as references in the preparation of this specification:

[1] NIST: *Federal Information Processing Standards Publication 46-3: Data Encryption Standard (DES)*, 1999 October 25.

[2] NIST: *Federal Information Processing Standards Publication 81: DES Modes of Operation*, 1980 December.

[3] FIPS Publication Change Notice – FIPS PUB 81, *DES Modes of Operation – Change No.: 2*, 1996 May 31.

[4] NIST: FIPS PUB 140-2, *Federal Information Processing Standards Publication – Security Requirement for Cryptographic Modules*, 2001 May 25.

[5] NIST: *Federal Information: Processing Standards Publication 180-2: SECURE HASH STANDARD*, 2002. Available at <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>

[6] NIST: *Federal Information: Processing Standards Publication 186-2: DIGITAL SIGNATURE STANDARD (DSS)*, January 27, 2000. Available at <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>

[7] NIST: *Federal Information: Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES)*, November 26, 2001
Available at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[8] IEEE P1363: *Standard Specifications for Public Key Cryptography*

[9] Request for Comments: 1945 – *Hypertext Transfer Protocol* – HTTP/1.0, T. Berners-Lee (MIT/LCS), R. Fielding (UC Irvine), H. Frystyk (MIT/LCS), May 1996

[10] PKCS #1 v2.1: *RSA Cryptography Standard*, RSA Laboratories. June 14, 2002

[11] R. Housley (RSA Laboratories), W. Ford (VeriSign), W. Polk (NIST), D. Solo (Citicorp), April 2002, *Request for Comments: 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Category: Standards Track*

[12] T. Dierks (Certicom), C. Allen (Certicom), *Request for Comments: 2246 – The TLS Protocol Version 1.0, Category: Standards Track*, January 1999

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™