IEC/TS 62224

Edition 2.0 2013-07

TECHNICAL SPECIFICATION

colour inside

Multimedia home server systems – Conceptual model for digital rights management

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

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

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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.