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

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*