IEC/TS 62224

Edition 1.0 2007-11

TECHNICAL SPECIFICATION

Multimedia home server systems – Conceptual model for digital rights management

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 It also gives information on projects, withdrawn and replaced publications.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

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

FOREWORD 4
INTRODUCTION 6

1 Scope 7
2 Normative references 7
3 Terms, definitions and abbreviated terms 7
3.1 Terms and definitions 7
3.2 Abbreviated terms 12
4 Notation 12
4.1 Numerical values 12
4.2 Notations for keys 12
4.3 Notation list 13
5 Requirements 13
5.1 Viewpoint of content user 13
5.1.1 Content usage environment 13
5.1.2 Content distribution services 15
5.1.3 Integrity of content 15
5.2 Viewpoint of rights holder 16
5.2.1 Overview of requirements for content protection 16
5.2.2 Licence service model 16
5.2.3 Threats and counter-measures 17
5.2.4 Evaluation criteria 19
6 Design considerations 19
6.1 Security model 19
6.1.1 Overview of security model 19
6.1.2 Secure licence transaction protocol (SLTP) model 20
6.1.3 Certification authority 21
6.1.4 Key revocation and termination of TREM 22
6.2 Interconnection model 22
6.2.1 Generic interconnection model 22
6.2.2 Licence relay protocol (LRP) model 24
6.2.3 Implementation model of inter-connection 25
6.3 Licence information model 26
6.3.1 Access conditions 26
6.3.2 Generic licence format (GLF) model 26
6.4 Protected content format (PCF) model 27
7 Issues to be standardized 27

Annex A (informative) Example of algorithms for cryptosystem and hash 28
Annex B (informative) Example of conversion of licence information in DRM based upon SLTP into that of existing DRM 29

Bibliography 31

Figure 1 – Requirements in the target ubiquitous content usage environment 14

Figure 2 – Licence service model to consider the threats 17
Figure 3 – Example of protection level control 19
Figure 4 – Security model of content protection 20
Figure 5 – Basic procedure of SLTP model 21
Figure 6 – Overview of issuing TREM class certificates 22
Figure 7 – Revocation of certificates and termination of TREMs 23
Figure 8 – Generic interconnection model for content protection 23
Figure 9 – Implementation model of inter-connection 25
Figure 10 – Example of GLF structure 27
Figure B.1 – Example of static conversion of licence information 29
Figure B.2 – Example of dynamic conversion of licence information 30

Table 1 – Expression of numerical values 12
Table 2 – Notations used in this model 13
Table 3 – Threats and counter-measures in the licence service model 17
Table 4 – Types of access condition 26

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