TECHNICAL SPECIFICATION

IEC TS 62045-1

First edition
2006-12

Multimedia security – Guideline for privacy protection of equipment and systems in and out of use –

Part 1: General

Reference number
IEC/TS 62045-1:2006(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

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

TECHNICAL SPECIFICATION

IEC TS 62045-1

First edition
2006-12

Multimedia security – Guideline for privacy protection of equipment and systems in and out of use –

Part 1: General

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE P

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MULTIMEDIA SECURITY – GUIDELINE FOR PRIVACY PROTECTION OF EQUIPMENT AND SYSTEMS IN AND OUT OF USE –

Part 1: General

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 62045-1, 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
100/1103/DTS	100/1162/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 list of all the parts of IEC 62045, under the general title *Multimedia security – Guideline for privacy protection of equipment and systems in and out of use*, can be found on the IEC website.

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 publication may be issued at a later date.

INTRODUCTION

There has been an increase in consumer products of multimedia that store the user's private data and privacy information. For instance, a digital TV tuner has a kind of IC card which stores the user's information and sometimes includes credit information. Also, from a wider viewpoint, digital cameras or digital video recorders store the private data of users, and digital audio players, cellular phones and PCs are banks of private data.

This private information should be protected from unauthorized or illegal access and use.

When the user discards such products, private data remains stored and this should be protected or deleted. In addition, when a user lends his product to others, private information should be protected. For instance, even if all the contents in the memory of digital video recorders or digital cameras are deleted, these data can be recovered easily with some software technology.

As consumer products of multimedia include storage and computer architecture, this problem will be raised in many aspects of usage. All products should have privacy protection methods.

This technical specification describes the system model and general methods for the user's privacy protection of data storage, equipment and systems, both in and out of use. Equipment and systems have their own structure in each application, therefore, the other part of this technical specification defines a dedicated method for privacy protection for the specific application. Also, the implementation of the privacy protection method depends on each design.

MULTIMEDIA SECURITY – GUIDELINE FOR PRIVACY PROTECTION OF EQUIPMENT AND SYSTEMS IN AND OUT OF USE –

Part 1: General

1 Scope

This part of IEC 62045 gives the guideline for methods for the protection of the user's privacy in consumer equipment and systems, both when the equipment or systems are in use and out of use.

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.

IEC 60958-3, *Digital audio interface – Part 3: Consumer applications*

IEC 61880-2, *Video systems (525/60) – Video and accompanied data using the vertical blanking interval – Analogue interface – Part 2: 525 progressive scan system*

IEC 61883-6, *Consumer audio/video equipment – Digital interface – Part 6: Audio and music data transmission protocol*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
data storage
all kinds of data-storing functions, which are devices or systems including hard disk drive, optical disc and memory devices and others

3.2
data encryption
conversion of data into code or cipher

3.3
data access
reading, writing or use of data stored in data storage

3.4
access control
control for condition of use or entry to system or data

3.5
private data
data that is property of the user

3.6
social engineering
cracking techniques that rely on human rather than hardware and software weaknesses

4 Privacy of user

4.1 Privacy protection

The reason for protecting the user's privacy is that the privacy of the user is the property of the user. The manufacture of equipment and systems, and the service providers have the responsibility of safeguarding the user's privacy.

4.2 Definition of privacy

Privacy, as defined in this specification, is the private information of the user or private information created by the user that is produced or accompanied with user's usage, operation and behaviour with multimedia equipments or systems. Using the equipment, system and service, these activities produce private information that is stored or transferred. This privacy has attribution and origination.

Attribution is specified depending on its nature as shown in Table 1.

Table 1 – Privacy attribution

Privacy attribution	Description	Example
Identification of user	User can be identified with this information	Name, address, telephone number, e-mail address Social information, credit card information, social number Biometrics data of user
Creation by user	Information that is the property of user	Document, photograph, video, music
Provided by user	Information provided by user operation	Broadcasting programme, downloaded contents, cookie, usage record

The identification of the user is fundamental information of the user. The user can be identified by this information, and others can access to the user or the property of user with this information.

Creation by the user is a property of the user. This information should be protected from others.

Provided by the user is also a property of user. This is provided by user operation or behaviour.

The origin of that information is specified as shown in Table 2.

Table 2 – Origin of information

Origin	Description
Direct information	Provided direct by user
Indirect information	Provided indirectly by user's use of equipment or systems
Accompanied information	Data accompanied by the user's use of equipment or systems

Direct information is provided by the user intentionally and consciously, or unintentionally and unconsciously. When the user inputs his private information or recalls his information, that information is provided direct by the user's operation or behaviour.

Indirect information is provided by the user's use of equipment or systems intentionally and consciously, or unintentionally and unconsciously. When the user uses equipment or systems, this behaviour causes communication of information including the user's private information.

Accompanied information is information other than that made by the user, which is created by equipment or systems having a relation with the user's use or behaviour. For instance, when the user uses equipment, the equipment may record a log. This log will include private information regarding the user.

4.3 Characteristics of privacy

4.3.1 Characteristics of privacy general

Privacy defined as private information has the characteristic of protection.

4.3.2 Information attribution

The information to be protected is specified by a judgment of what is important information for the user who has the right to that information. Information itself is the object to be protected and also indirect information is the object. Three kinds of information are specified as shown in Table 3.

Table 3 – Information attribution

Information attribution	Case
Original information	All the original information Part of the original information
Derivative information	Secondary information from original information Proxy information of original information
Access information	Access information to original or derivative information

Original information is principal information primarily provided by the user. All of this information is private and, in some cases, part of the original information is the subject of protection.

Derivative information is produced from original information by the user or other persons, there are two cases of this information. Secondary information is produced from the original information and it includes private information of original information. Proxy information is a proxy of the original information, it includes information of the relation with the original information.

Access information is a key or authentication information used to access to the original information or derivative information. This is not private information in itself but the subject of protection.

4.3.3 Rights holder

The rights holder who has the rights of private information is defined by a judgment of what authorized person or organization control or has the rights of that information to protect their rights or property. Basically the rights belong to the user, but there will be other cases where part or all of the rights belong(s) to others or other organizations. Rights holders are shown in Table 4.

Table 4 – Rights holder

Rights holder	Condition
User	User rights
Manufacture	Manufacture rights
Contents provider	Contents provider rights

The manufacturer provides consumer products including the property of manufacture.

The user can take advantage of that property but the rights belong to the manufacturer.

The contents provider has the rights of the contents.

4.3.4 Protection execution

Protection should be executed depends on each condition as shown in Table 5.

Table 5 – Protection execution

Protection execution	Description
Always	To be protected whether user desires or not, and is aware or not
Automatically	To be protected automatically depending on operation
On request of the user	To be protected when user desires
Never	Not to be protected because of other conditions (see note)
On request of other than user	To be protected because of other conditions (see note)
NOTE Legal or security reason will affect conditions irrespective of user preference.	

Always is applied for principal information of properties of user, that information should be protected always.

Automatically is provided by equipment or systems in appropriate timing of operation by use.

On request of the user is controlled by the user, information should be protected by the request of the user.

Never may apply because of legal or security reason regardless of user preferences.

On request of other than user is controlled by legal or security reason.

4.3.5 Access rights holder

In some cases, persons other than the user can access the user's information. When the user accepts access from others, others can use them. An authorized supervisor can access user's information.

NOTE For security reasons, for instance, the police may access user's information in the framework of investigation.

Table 6 – Access rights holder

Access rights holder	Description
User	User
Others	Persons other than user
Authorized supervisor	Person authorized other than user (see note)
NOTE Legal or security reasons will affect conditions irrespective of the user's preference.	

5 Methods for privacy protection

5.1 System model

5.1.1 Definition of system model

The system model consists of body of equipment or systems and communication paths as shown in Figure 1.

Privacy information is data that is stored in storages. These are:

- data storage;
- equipment with data storage device;
- systems involving these data storage and equipment.

Storage device, equipment or systems have plural paths of data access that is categorized by attribution. These are:

- data interface;
- user interface;
- reproduction;
- other paths.

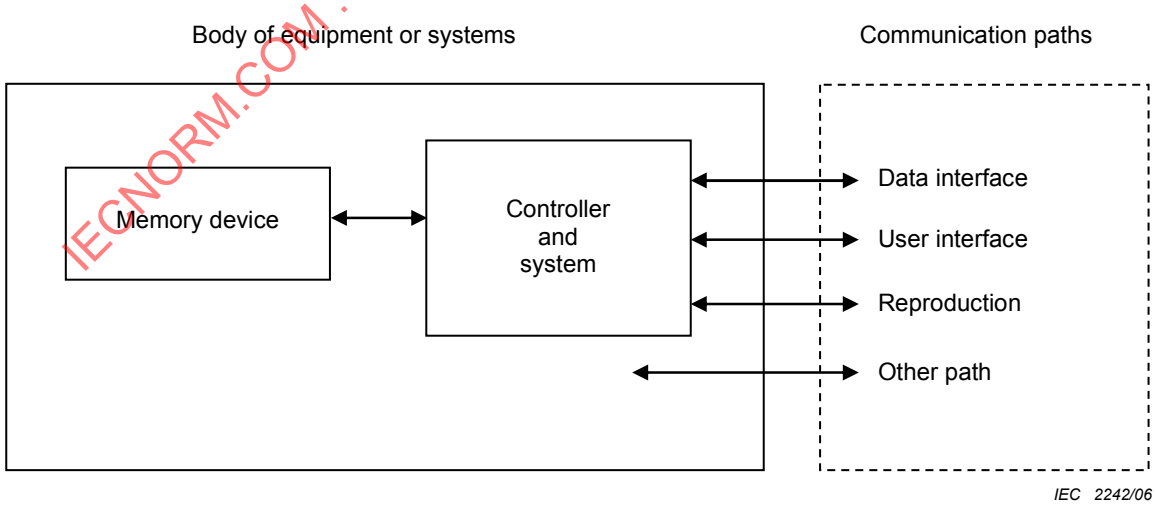

Figure 1 – System model

The privacy information of the user is a kind of data. The data is created through a relationship with data storage, equipment or systems, and it is stored in storage device, or it is not stored. Relationship means possession, operation, usage and end of use. These

activities produce information including privacy of user. Private data will be transmitted or communicated to outside or accessible from outside through communication paths, or data can be reproduced by a function of equipment and systems.

Therefore, the method for protection of these data should be implemented in storage device, equipment or systems or in a combination of these. Also, the method should be implemented in communication paths. Storage device, equipment and systems are able to have a structure from physical layer to application layer. There are many methods for protection of data in each structure layer and the combination of each method. Also access paths have structures from physical layer to application layer.

There is another aspect of privacy protection. A system is operated by the user as a human being, and there will exist a security hole caused by this nature of human operation. This is not a technical but user assistance for this security hole is important. Without knowledge of security user cannot protect privacy if equipment and systems have complete protection methods. This is described in Clause 5.

5.1.2 Communication paths

Communication paths are specified in each case as shown in Table 7.

Table 7 – Communication paths

Communication path	Description	Examples
Data interface	Between data and outside equipment or systems	Network interface, digital interface (for example, IEC 60958-3, IEC 61883-6), video interface (IEC 61880-2), etc.
User interface	Between user and equipment or systems	Operational function, monitor display for operation
Reproduction	Data reproduction path to outside the equipment or systems	Audio and video play, data output
Other path	Other path of data to outside the equipment or systems	Power line, etc.

Data interface is a data communication path to outside such digital audio and video interface, or local area network. As primitive case, data line of memory device is this communication path.

User interface consists of control device and information device such as display device, information can be reproduced or communicated with these devices.

Reproduction may be a main function of equipment or systems, reproduction reveals information to outside.

Other path is other than these three paths, it is not intended to use data communication but it may be possible to obtain information through that path.

5.1.3 Body of equipment or systems

In the body of the equipment or systems, the data of privacy information is stored in the storage functionality. Data storage is storage equipment such as memory devices. Equipment involves data storage inside, for instance, many consumer products include data storage inside. A system consists of these equipment and data storage.

Table 8 – Storage functionality

Storage functionality	Examples
Data storage	Memory, memory card, HDD, optical disc
Equipment	Digital broadcasting tuner, optical disc player and all categories of consumer products
Systems	AV system, home network system

5.2 Case of usage

Cases of usage are specified in three cases as shown in Table 9.

Table 9 – Case of usage

Case of usage	Description
Owner use	Owner user uses own possession
Other use	Others use owner's possession
Out of use	No more use

Owner use is a case of normal usage, the privacy of the user should be protected from others than the user.

Other use is a case where persons other than the owner use the owner's equipment or systems; the owner's privacy should be protected from others, at the same time the privacy of others in use should be protected from the others, including the owner.

Out of use is a case after owner's disuse of equipment or systems, privacy information may remain in that equipment or systems. Privacy data should be deleted or protected before disuse.

5.3 Methods for data protection

5.3.1 Applicable portion and mode

Data storage, equipment and systems and communication paths make up the combination table as shown in Table 10. Each method for data protection is applied to each combination or plural combinations.

Table 10 – Combination table

	Storage device	Equipment	Systems
Interface	a	b	c
User interface	d	e	f
Reproduction	g	h	i
Other path	j	k	l

Appropriate method for data protection for each combination from a to l should be applied. This method is defined in each application. It will be specified in the other part of this specification.

Operation modes are specified as shown in Table 11.