IEC/TS 62579

Edition 1.0 2010-05

TECHNICAL SPECIFICATION

colour inside

Multimedia home server systems – Conceptual model for domain management

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

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 It also gives information on projects, withdrawn and replaced publications.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/TS 62579

Edition 1.0 2010-05

TECHNICAL SPECIFICATION

Multimedia home server systems – Conceptual model for domain management

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE V

ICS 33.160; 35.240

ISBN 978-2-88910-932-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MULTIMEDIA HOME SERVER SYSTEMS – CONCEPTUAL MODEL FOR DOMAIN 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 62579, 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.

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

Enquiry draft	Report on voting
100/1626/CDV	100/1676/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 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

Compared with analog media, digital contents can be copied easily and the copies don't decline in quality. So it is certain that digital contents should be protected.

But, compared to the rights of private records on analog media, it is hard for users to enjoy their digital contents freely. The concept of a domain has been defined in several organizations for the purpose of improving user convenience. Domains enable users to consume and manage their digital contents in a manner which is more like enjoying analog contents. Users can enjoy digital contents, which are stored on a device, not only on the device where they are stored on but also on other devices within the same domain such as home or school, etc. From a standpoint of copyrights, it means that the contents are allowed to be consumed with a copy control technology on limited devices. A domain manages both user convenience and contents protection. Depending on the scenario of the operated domain, the limit and the boundary on domain configuration can be flexible.

MULTIMEDIA HOME SERVER SYSTEMS – CONCEPTUAL MODEL FOR DOMAIN MANAGEMENT

1 Scope

This Technical Specification defines the conceptual model of domain management, which includes terms, requirements and reference models. The domain is a set of devices, users, and/or other entities which can share contents. Entities within a domain are allowed to play, copy and move content and usage rules to other entities within the same domain.

Some existing systems have been proposed in this field of domain, but various vocabularies and models are specified. This situation causes confusion and misunderstanding of systems, and disturbs interoperability. This Technical Specification is intended to standardize the vocabularies and clarify the models.

All kinds of digital content, including broadcast content which needs to be protected, are considered in this specification. On the other hand, rights management and content protection technology are beyond the scope of this specification.

NOTE In addition, network protocol and media format for content sharing and exchange are also out of the scope of this specification. Refer also to IEC 62481-1 and IEC 62481-2 for interoperability guidelines..

2 Terms, definitions and abbreviations

2.1 Terms and definitions

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

NOTE These are necessary terms used in the field of domain management.

2.1.1
content issuer
rights issuer or contents holder

2.1.2
content
digital data, such as movies, images, audio and software, etc.

2.1.3
content key
encryption key related to each content

2.1.4
domain
set of devices, users, or other entities which can share contents and associated usage rules

2.1.5
domain ID
unique identifier which is related with a domain

2.1.6
domain key
secret information shared among entities in a domain

2.1.7
domain management server
server which issues or manages a domain ID and a domain key

2.1.8
domain join
process of including an entity in a domain, which enables the entity to obtain a new domain ID or domain key

2.1.9
domain leave
process of excluding an entity from a domain, which ensures that the domain ID and domain key in the device are deleted

2.1.10
domain merge
process of integrating multiple domains into a new domain with a unique domain ID

2.1.11
domain divorce
process of dividing a domain into multiple domains with different domain IDs

2.1.12
domain separate
process of dividing a domain into multiple domains with the same domain ID temporarily

2.1.13
user ID
unique identifier for the user; it could be a user account

2.1.14
user key
secret information shared among only the domains, devices or other entities bound to the user; this information is generated by RI

2.1.15
usage rule
collection of permissions, keys and other attributes which are related to protected contents

2.2 Abbreviations

AD	Authorized Domain
ARIB	Association of Radio Industries and Businesses
CAS	Conditional Access System
CL	Content License
CPCM	Content Protection and Copy Management
CRL	Certificate Revocation List
DVB	Digital Video Broadcasting
DRM	Digital Rights Management
HANA	High-Definition Audio-Video Network Alliance
KMB	Key Management Block
LAD	Localized Authorized Domain
OMA	Open Mobile Alliance
RMPI	Rights Management and Protection Information
RO	Rights Object
RRT	Round Trip Time
RI	Rights Issuer
TTL	Time to Live
USI	Usage State Information

3 Use cases

3.1 Purpose of description of use cases

This clause is for information only and describes how domain management is specified and how the scenario of domain is assumed in existing specifications on DRM. This leads to what a domain management standard should contain.

In general, users can consume content without restriction of the location on all home electric appliances, cell phones, mobile devices or car devices in the domain. The devices can share content according to a permission system, which includes the use situation and the quality, in each domain.

3.2 Example 1: A domain in ARIB TR-B27

A device is allowed to copy content and a certain part of the usage rule to storage media. The content is played according to the restriction of the usage rule, as shown in Figure 1.

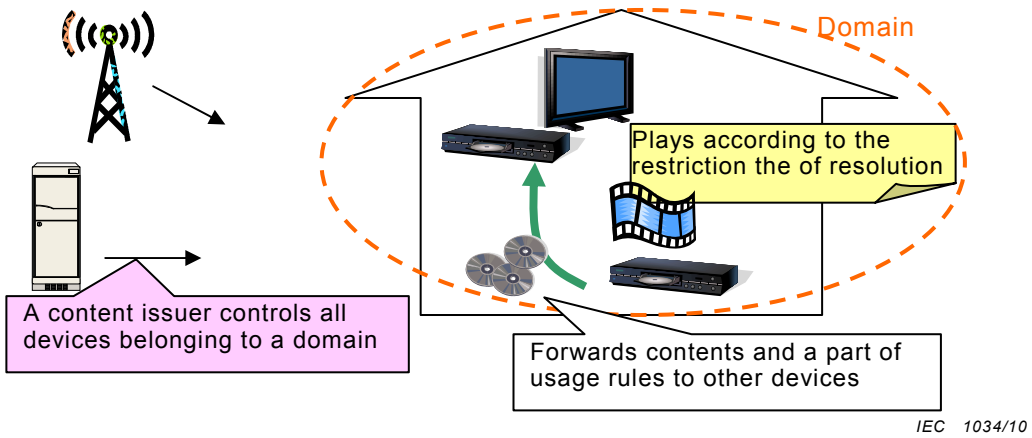


Figure 1 – Domain in ARIB TR-B27

3.3 Example 2: A domain in DVB CPCM

Users can get content available in LAD such as home network. After a certain time or event, the content can be played on all other devices within the same domain, as shown in Figure 2.

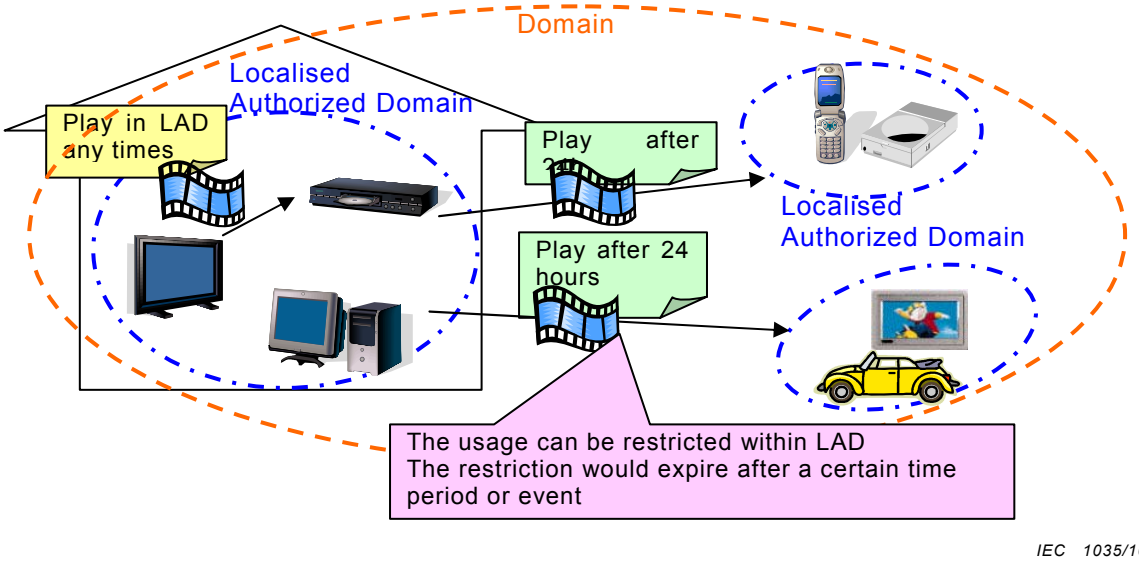


Figure 2 – Domain in DVB CPCM

3.4 Example 3: A domain in OMA DRM V2.0

A device forwards content and the associated usage rule to a cell phone.

The content and the usage rule are immediately usable on the cell phone without connecting to the content issuers, if the conditions (start and end time) are satisfied.

Devices not connected to the network can obtain content and usage rules via the connected device, using direct device-to-device connection, as shown in Figure 3.

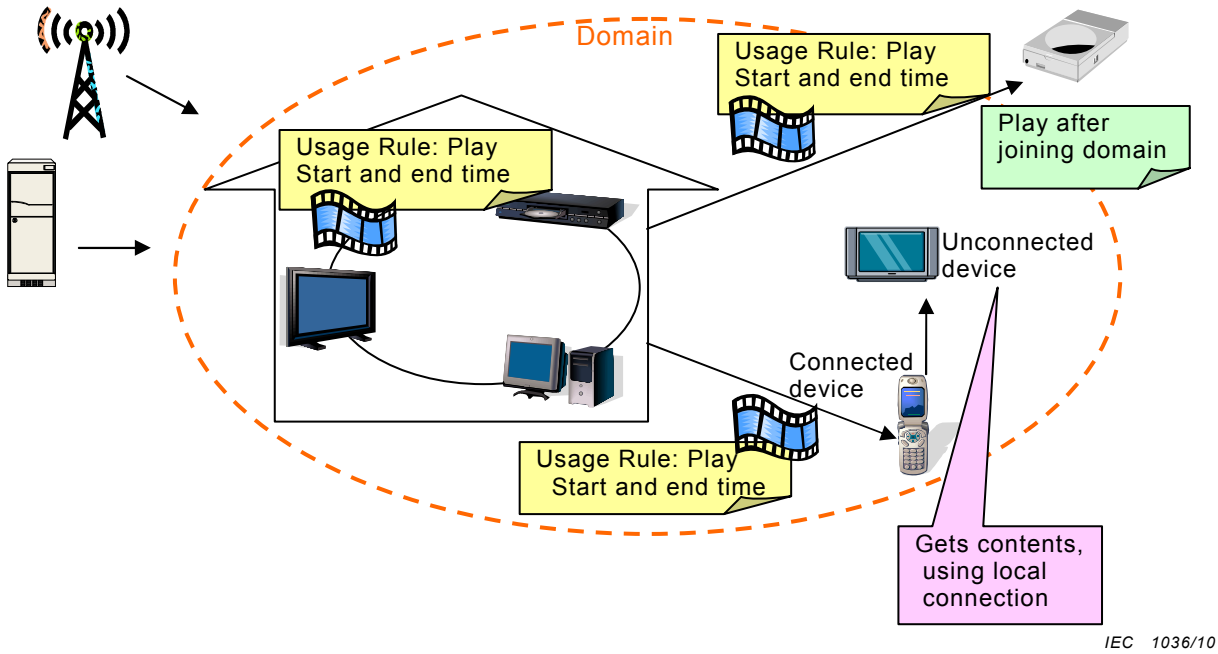


Figure 3 – Domain in OMA DRM V2.0

3.5 Example 4: A domain in permission code

A device that belongs to the domain is permitted to act as a receiver for the permission codes (for example, play freely and copy up to 7 times, etc.).

A domain can be characterized as collective of permission receivers. A domain is also a permission receiver, as shown in Figure 4.

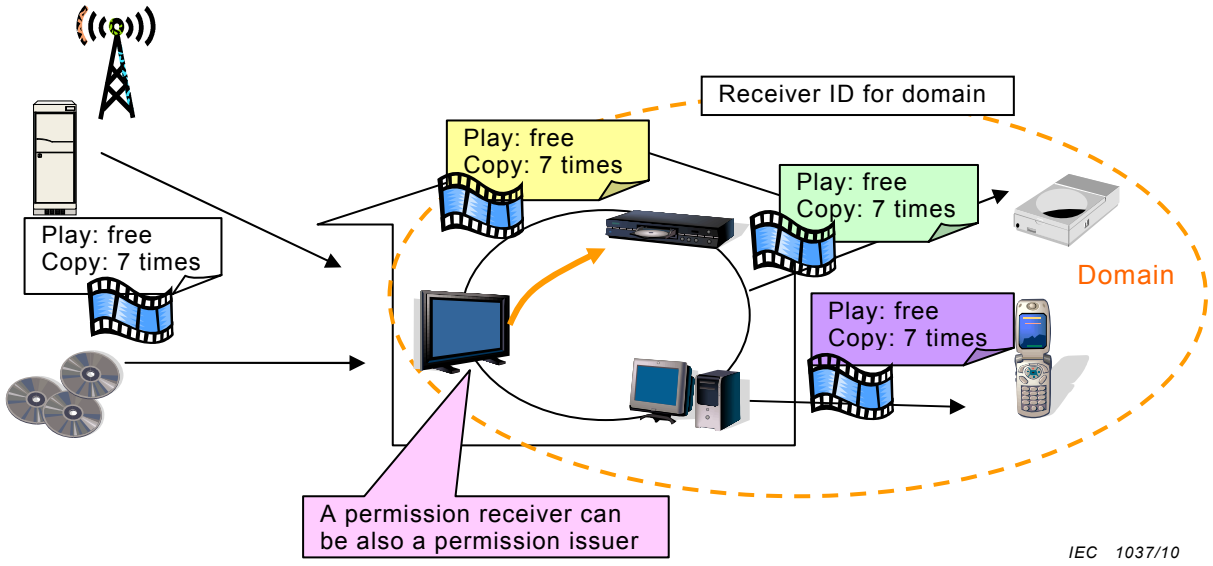


Figure 4 – Domain in permission code

3.6 Example 5: A common domain in Marlin DRM

Multiple users can share content they have obtained provided that they are registered with the same common domain, as shown in Figure 5.

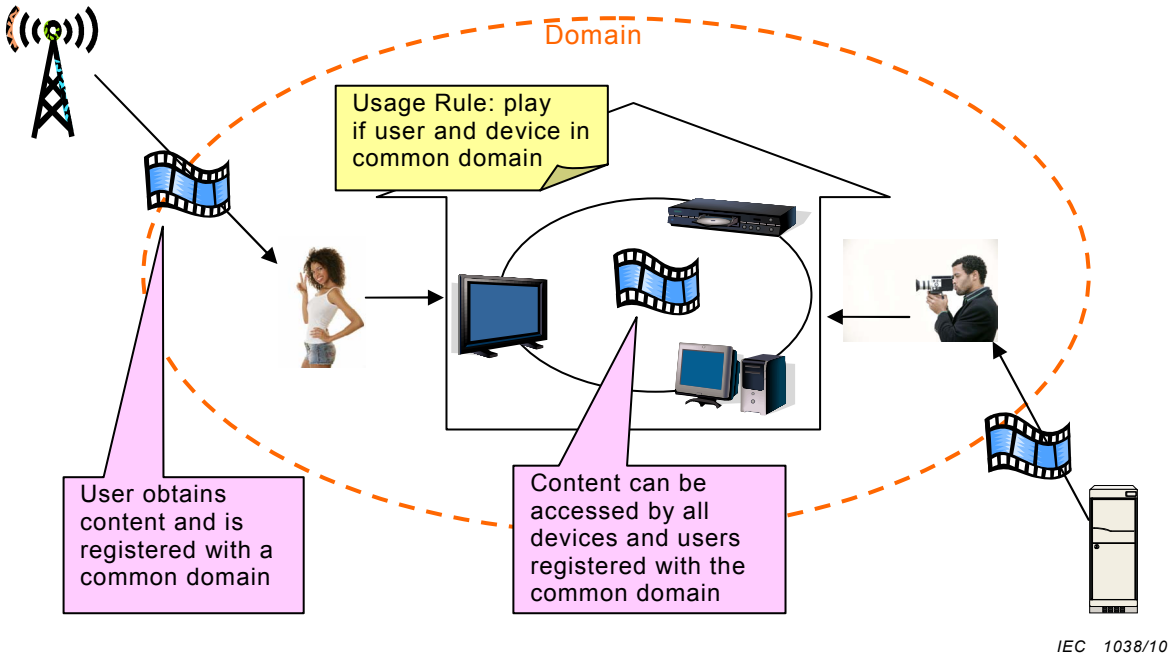


Figure 5 – Common domain in Marlin DRM

4 Conceptual model

4.1 Definition of a domain

A domain is a set of devices, users, and/or other entities which consume content according to common usage rules. Devices in a domain are allowed to share content and the associated usage rules within the same domain, as shown in Figure 6.

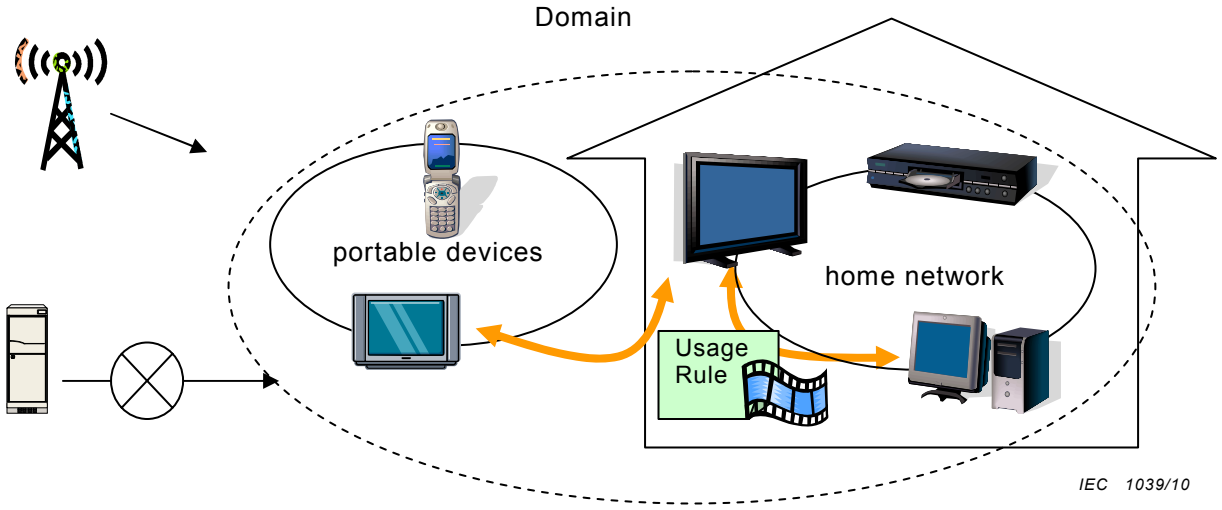


Figure 6 – Overview of a domain

4.2 Forming a domain

A domain which groups a set of devices, users, and/or other entities together facilitates content management in simple situations where no differentiation is required as to the identity of the user. However, for situations where content is licensed based on the identity of the user (e.g. delivery through mobile operator) a domain needs to provide for easy content access government, based on the relationship of users with each other. In this case, a domain can also be formed by associating a set of entities to a user entity and a common usage rule for consuming content is then bound to the user entity instead of each individual entities. This implies that all entities linked to the user domain are automatically governed by the same common usage rule issued to the user entity. In addition, an entity can be part of multiple user domains, e.g., a shared PVR in the living room can be part of two users' domains, hence it is allowed to consume content purchased by both users. Additionally, a multi-device, multi-user domain model enables entities to join multiple domains and allowing a domain to contain multiple entities, e.g., a household with 2 shared devices at home such as a PC and a PVR. Each of these devices is linked to every user in the family, hence any content purchased by a family member can be used on both family devices. However, this is not very efficient. An alternative approach is to unite all users in a common domain and associate all shared entities with the common domain, e.g., all family members are bound to a common domain called family domain and the PVR and PC are members of this family domain.

There is a domain policy that is used to express the rules for forming a domain and registering and deregistering entities to and from domains. The parameter for domain management can be found in 4.4.2.

4.3 Components of a device which can join a domain

Figure 7 shows the typical components of a device which can join a domain.

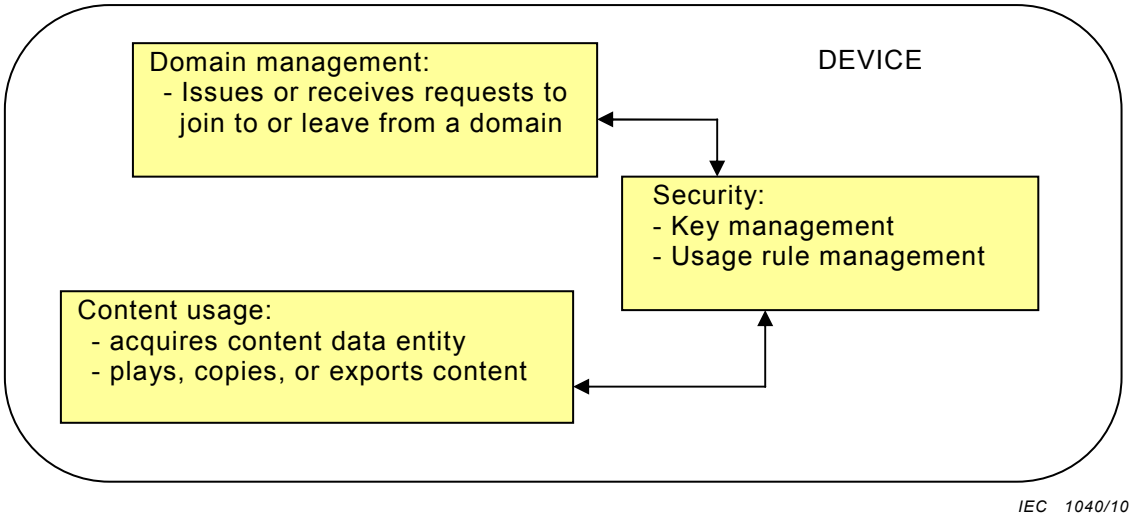


Figure 7 – Components of a device

The following list explains the components:

- Domain management: issues and receives requests to join a domain or leave a domain, and exchanges such requests with other devices.
- Security: manages domain keys, usage rules, and other information to be protected securely.
- Content usage: acquires content data entity via broadcasting or network, and controls usage of content (for example playback, duplicate, export, and so on).

4.4 Requirements

4.4.1 Abstract domain model

This subclause presents the general domain model. Domain management should be modelled using five basic elements, namely: Content (C), User Identity (P), Authorized Domain (AD), Local Authorized Domain (LAD) and Device (D). Figure 8 illustrates the relationship between these basic elements. Various domain models (c.f. Clause 5) can be built based on this abstract domain model.

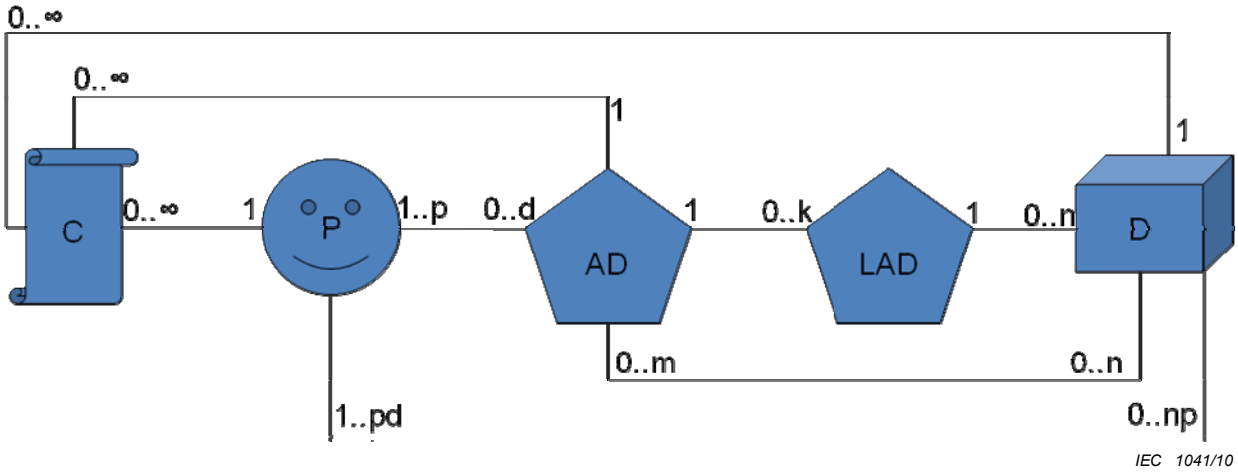


Figure 8 – Relationship between the basic elements of a domain model

Acquired content (C) can be bound to a device (D), an authorized domain (AD) or a user entity/identity (P). For content that is bound to a device, only the particular device is permitted to use it. An authorized domain (AD) can consist of many devices, hence by binding content to an AD simplifies the content authorization usage as only a single binding is needed to enable multiple devices that are members of the AD to access the contents. Furthermore, content can be bound to a user entity where it is purchased through a user account. Similarly, a user entity or identity (P) can be linked to multiple authorized domains or multiple devices. This allows for more flexibility in that the contents can be played by all devices that are bound to the user entity, i.e., enabling the user's owned devices to play the purchased content. This also enables the user remote access to his own contents regardless of his location as long as the device playing the content is bound to the user entity/identity (P). Conceptually, the user entity/identity is perceived as a domain that groups a set of devices together based on the identity of the user. Users can also share their contents with each other through binding of their respective identity (P) to a common authorized domain (AD). Conversely, they can un-share their contents by explicitly removing the binding of their identities from the common domain. This enables the users to keep track of their rights in an effective manner.

An authorized domain (AD) typically refers to the service provider managed domain in which the service provider or the content provider maintains the domain membership. However, there can also be a local domain (LAD) in that its membership is governed by an independent domain management service, or the consumers themselves. A LAD's membership can also be maintained through proximity checks, e.g., devices should be in close proximity with the local domain management server.

This abstract domain model serves as the reference model for implementing a domain management system. A wide variety of implementations can be derived from this abstract model (c.f. Clause 5). As mentioned previously, the main advantage of having a domain is the efficient management of devices. When a license is bound to a domain, devices can be easily added or removed from the domain without affecting the rights of accessing the content, which implies that, by adding a new device into the domain, it is automatically authorized to use the contents, while removing the device from the domain is equivalent to revoking its rights of accessing the contents. Since this abstract domain model is a general description which covers concepts among the domain, it is not necessary to achieve all features described here. Each DRM system would be a subset of this model. The following subclauses describe examples of each DRM system as subsets of this abstract domain model.

4.4.2 Information elements

Parameters associated with the domain management commonly used in this specification are defined in Table 1.

Table 1 – Information elements of a domain

Information element	Description
Device ID	Unique identifier associated to each device.
User ID	Unique identifier associated to each user. This identifier represents the user account.
User key	Secret information shared among only the domains or devices bound to the user. This information is generated by the RI.
Domain ID	Unique identifier associated to each domain. This identifier is generated by the RI or a device which is the first attendance of the domain.
Domain key	Secret information shared among devices belonging to a certain domain. This information is generated by the RI or a device which is the first attendance of the domain.
Period of validity	Period where content usage according to the usage rules issued to a domain is permitted.
Domain shared information	Information which is referred to when a mutual authentication process is running, in order to deny for illegal devices to join. They are for example KMB (Key Management Block) or CRL (Certificate Revocation List), and updated in proper situations. Such information includes the list of devices or keys which shall be accepted or denied.
Characteristics for the composition of a domain	Parameters which characterize the composition of a domain. For example, a maximum number of devices in one domain, or a maximum number of domains a device can be associated with, TTL (Time to Live), RTT (Round Trip Time) or other restrictions in a distance between devices. Others are Owner Timeout Period, Max Domain Timeout Period, and so on. Owner Timeout Period: The maximum time period duration value before a user entity is being disconnected from the Domain because the user entity is no longer regarded as being associated with the Domain. Max Domain Timeout Period: The maximum waiting period duration value after a disassociation of a user entity from a domain, after which it is assumed that no member devices will be able to play content of the user entity any longer. For example, the user may be unable to maintain a connection for a short period, and therefore disconnect the user entity from the domain. Disconnection of the user entity is not necessary in that case (time duration < Owner Timeout Period). If the user and his device have left the wireless home zone for a longer period, that situation justifies disconnection from the Domain (time duration > Owner Timeout Period). Definition of Domain: see 4.1.

4.4.3 Joining and leaving domains

The following conditions are required when joining or leaving domains.

– Each device has its device ID, and can be recognized as an authorized device.

– The content issuer can manage the device composition situation of a domain. Specific methods are assumed as follows:

- the content issuer manages the joining and leaving of each device by registering and de-registering the device from the domain, e.g., linking a device to a domain upon joining. The content issuer recognizes the composition of domain in real-time;
- the content issuer requests a report to the domain as necessary;
- the content issuer delegates the management and the domain manages itself autonomously. Content issuer participates in revocation of devices.

Other than the content issuer that is responsible for managing an authorized domain, users at home can create and manage its local authorized domain (LAD) without involving the content issuer. A device in the authorized domain can maintain the membership of the LAD, when a device requests to join the LAD, a proximity check is performed to ensure that the new device is in the close vicinity. Similarly, when the device moves out of range, the proximity requirement no longer holds, the device is removed from the LAD.

Table 2 shows the parameters of the devices when joining a domain.

Table 2 – Device parameters that join domain

Parameter		Mandatory/Optional
Device ID		M
Domain ID		M
Domain key		M
User ID		O
User key		O
Period of validity		O
RI ID		O
Domain shared information		O
Characteristics for the composition of a domain		O
	Maximum number of devices	O
	Restriction on distance between devices	O
	Owner timeout period	O
	Max domain timeout period	O
NOTE An authentication and key transfer mechanism does not matter. It is essential that a device can obtain an information by taking appropriate measures.		

4.4.4 Usage control by usage rules

Users are allowed to enjoy their contents on their devices within a domain identified by a domain ID. A domain ID is described in a usage rule. All content shared among a domain shall be utilized according to the usage rules which are conveyed in a license that can be bound to the domain, a device or a user, and the usage rules describe the permission and constraints. For example, permission describes which types of content usage (playback, export, and so on) are permitted, and constraint describes how devices are limited in content usage (times of usage, usage start time, time range, and so on).

It is also available as optional requirement that usage rules are inherited to the new domain in case of merger of domains. Here inheritance means issuing new usage rules based on the rules of the original domains.

A device may have the multiple usage rules or belong to the multiple domains. In that case the device should select one usage rule and may report the referred usage rule to the content issuers.

4.4.5 Revocation of a device

It is necessary to provide some methods to revoke certain devices which belong to a domain whether the domain is managed by the content issuer or is a LAD managed by the user. In case of revocation, the domain is updated by re-generation or re-distribution of a new domain key.

4.4.6 Items gathered by content issuer

NOTE This possibility is optional.

Some items or attributes of a domain are very useful for content issuers, see Table 3. A domain may be required to manage such items and to provide a method for content issuer to access. For example, content issuers can recognize the frequency of compromise to the domain key, or they can recognize the revocation of devices, by analyzing the number of domain updates.

Table 3 – Items managed in a domain

Parameters	Mandatory/Optional
Number of devices in a domain	O
Actual usage of content (number of playback, duplicate, referred usage rule and so on)	O
Number of domain updates	O

5 Reference models

5.1 General

This subclause describes various domain models that can be derived from the abstract domain model defined in 4.4.

5.2 Basic model

5.2.1 Overview of basic model

The basic model is characterized by whether an external entity controls domain membership statements or not. The basic model is classified into RI management domain model and autonomous domain model. Either model is adopted whenever a domain is applied.

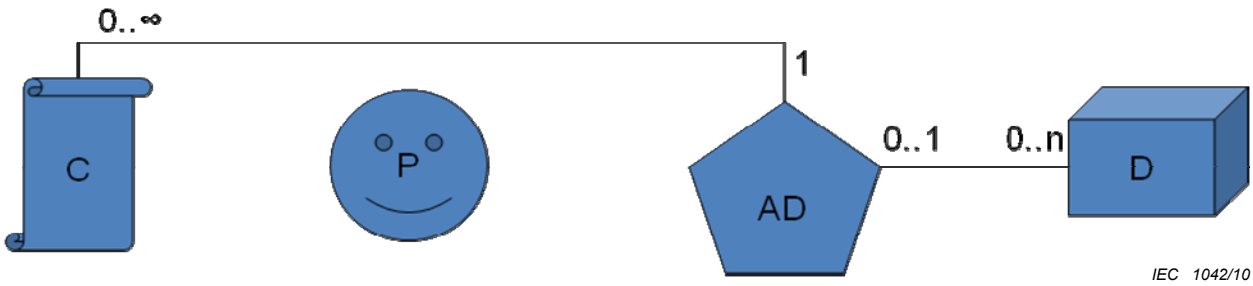
5.2.2 RI management domain model

5.2.2.1 Definition of RI management domain model

In this model, RI recognizes the domain membership state of the devices all of the time. According to the necessary conditions of connecting to RI, we classify RI management domain into five types (5.2.2.2, 5.2.2.3, 5.2.2.4, 5.2.2.5 and 5.2.2.6).

5.2.2.2 Domain assumed in ARIB TR-B27

Contents are bound to an authorized domain (AD) by the RI and they cannot be bound to devices directly. Devices can be part of the AD after they have obtained necessary information for the AD from the right issuer directly via network or broadcast. For example, a user can request for his device's domain membership via telephone, postcard and website in order to obtain the domain ID and the corresponding domain key. Upon joining the AD, the device is allowed to share contents or a part of the associated usage rules with other devices in the same AD, as shown in Figure 9.

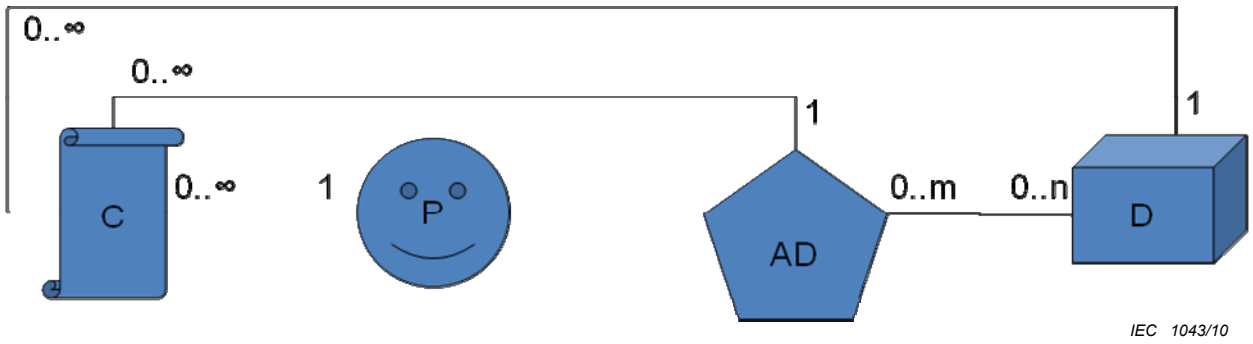


NOTE This model is assumed in ARIB TR-B27.

Figure 9 – Example of RI management domain model

5.2.2.3 Domain assumed in OMA DRM V2.0

In OMA DRM Version 2.0, contents can be bound to either a device or an authorised domain. A device can obtain the necessary information for a domain from the rights issuer (RI) only, but once a device is a member of a domain, it can get content with usage rules from another device without going to the RI. A device is capable of getting content and usage rules by interactive connection. A device can also act as intermediary to assist other devices to join the domain. In OMA, although the binding of content to identities is not part of the specification, it can be performed in the backend system of the rights object issuer where the user entity is represented as a domain, as shown in Figure 10.



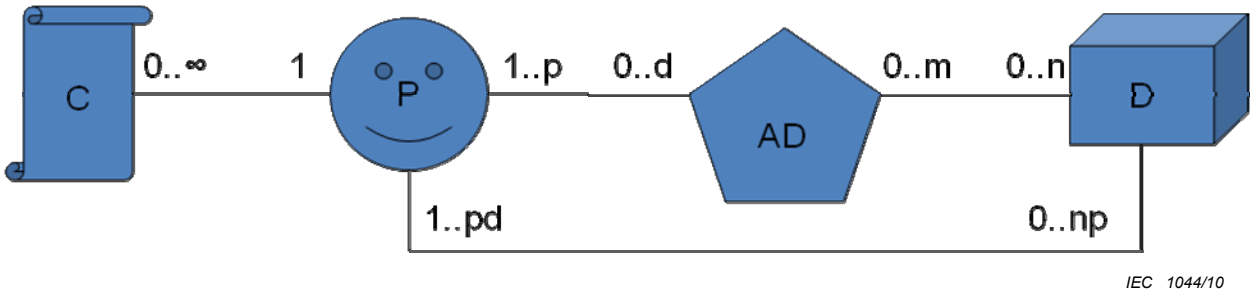
NOTE This model is assumed in OMA DRM V2.0.

Figure 10 – Example of an RI management domain model

5.2.2.4 Domain assumed in Marlin

Marlin enables content binding to identities, domains and devices that can then be linked to the user identities. The RI issues license to the user to access content and manages the domain membership.

As user identity is perceived as a domain itself, the AD in Figure 11 is regarded as a common domain that enables multiple users to share their content. This can be done by linking multiple user identities to the common domain. The advantage of having the common domain is two folds. First is the sharing of content between different users as mentioned previously. Second, devices can be replaced easily without affecting the domain configuration, e.g., a faulty device can be removed from the common domain and it can then be replaced by adding the new device into the common domain. The new device is automatically authorized to access the content licensed to the users to whom the common domain is linked.

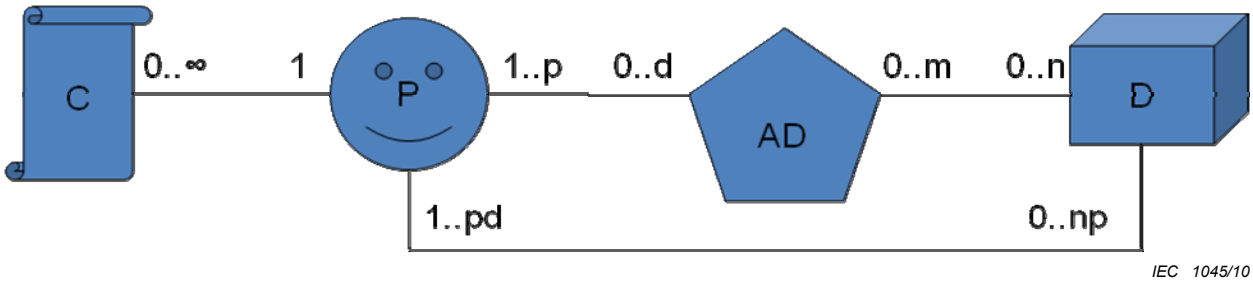


NOTE This model is assumed in the Marlin Domain Model.

Figure 11 – Example of the RI management domain model

5.2.2.5 Domain assumed in Coral

The DRM interoperability system Coral uses the same domain management model as Marlin. It binds content to identities to which devices and domains can be linked, as shown in Figure 12.

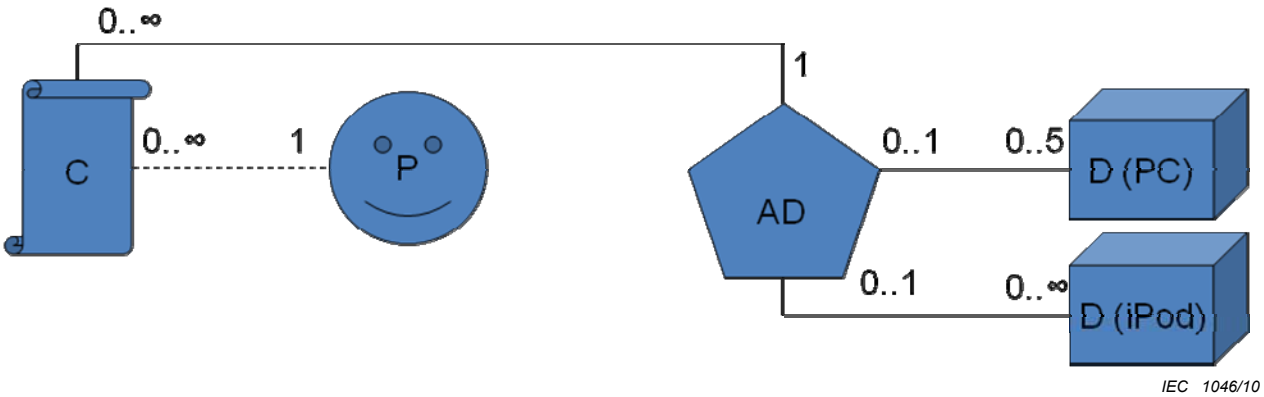


NOTE This model is assumed in the Coral Domain Model.

Figure 12 – Example of the RI management domain model

5.2.2.6 Domain assumed in FairPlay (iTunes)

Fairplay as used in iTunes binds content to a domain to which a limited number of PCs and an unlimited number of iPods can be connected. The backend system tracks the binding of content to a user account, which implies that a user identity is perceived as a domain, as shown in Figure 13.



NOTE This model is assumed in the FairPlay (iTunes) Domain Model.

Figure 13 – Example of RI management domain model

5.2.3 Autonomous domain model

5.2.3.1 Definition of autonomous domain model

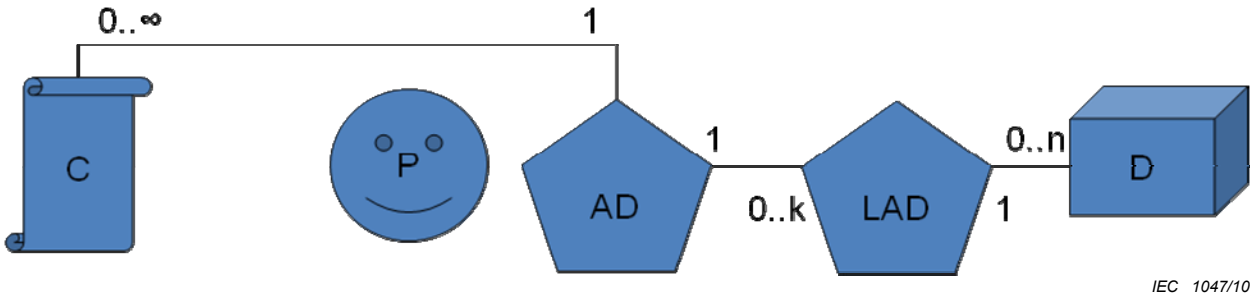
In this domain model, the authority of RI is partially delegated to each device. Each device can represent the role of RI, unlike the RI management domain model. It is supposed that a particular device in a domain works as a domain management server and manages devices in the same domain.

All devices in a domain are also supposed to be equal in the function. This model is regarded as a domain formed autonomously.

5.2.3.2 Domain assumed in DVB CPCM

Similar to ARIB TR-B27, contents are bound to an authorized domain (AD). However, a local authorized domain (LAD) is used. The authorized domain may consist of a number of LADs (defined by proximity requirements). Devices then belong to the LAD. This enables the user to manage its own devices by grouping them into a localized domain. This also facilitates easy addition and removal of devices as the user has the authority to do so. However, this is subject to the conformance to the domain policy.

In this case, a particular device in a domain works as the domain management server and manages the membership of the local authorized domain. This device can decide whether the other device joins the local domain or not, e.g. by using proximity check. An example of an autonomous domain model is shown in Figure 14.



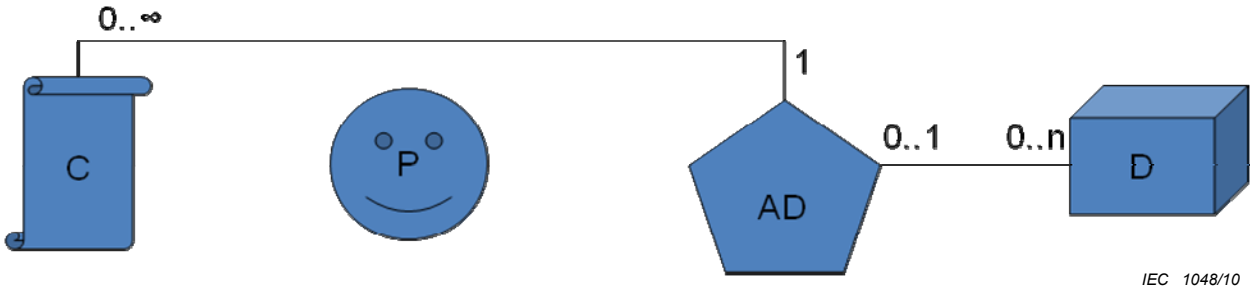
NOTE This model is assumed in DVB CPCM.

Figure 14 – Example of an autonomous domain model

5.2.3.3 Domain assumed in xCP Cluster Protocol

In this domain model, contents are bound to a domain. However, the domain membership can be undertaken by a device in the domain itself. The device can create the necessary information for a domain , such as a domain ID or domain key, by itself. The other devices in the domain can share the information which one device creates. For example, devices in an autonomous domain can hold the joining device list in common and generate a common key from the joining device list. Devices can share the information for a domain by use of the common key. In this model, a device can decide on whether the other device joins the domain or not. The authenticating and authenticated devices shall be on-line during the join process. Even if a device is off-line after that, the other devices have past records, such as the joining device list. Thus, this model is perceived as an autonomous domain because the device in the domain has a part of authority of the right issuer. An example of an autonomous domain model is shown in Figure 15.

NOTE xCP Cluster Protocol has been renamed to ASCCT by its originator, and is being planned to apply to HANA.



NOTE This model is assumed in xCP Cluster Protocol.

Figure 15 – Example of Autonomous domain model

5.3 Enhanced model

5.3.1 Overview of enhanced model

This is the enhanced model over the basic model (see 5.2). The enhanced model is operated by taking management step 5.2.2 or 5.2.3. The enhanced domain models are characterized by the following usage scenarios.

5.3.2 Domain model which extends over multiple domains

5.3.2.1 Regional domain

This domain model is regarded as a geographical domain and covers multiple domains. Contents are shared within the geographical area which is equal to a regional domain. In Figure 16, domain C extends over domain A and domain B geographically. The characteristics on domain C for the composition of the domain should include a regional conditions. Unless domain A has any regional characteristics for its composition of the domain, it is not a regional domain, see also domain B.

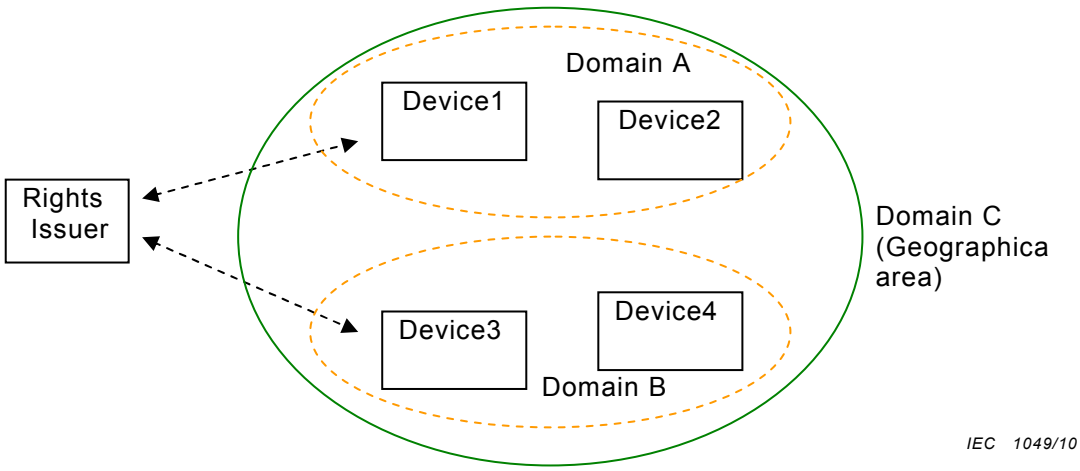


Figure 16 – Regional domain

5.3.2.2 Time stamped domain

This model is operated by time and space. A domain is formed in a place or a space where people gather temporarily and contents are shared within the formed domain. This formed domain is referred to as a time stamped domain.

Then the contents, which are acquired in the time stamped domain, are allowed to be consumed on devices in domain A or domain B, after acquiring usage rules for domain A or domain B, as shown in Figure 17.

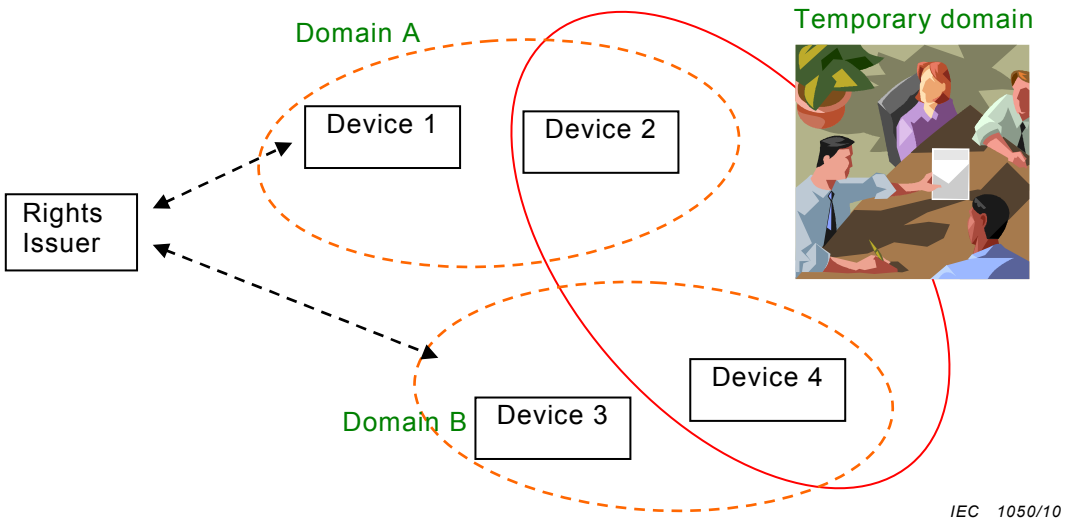


Figure 17 – Time stamped domain

5.3.3 Merged (or divorced) domain model

5.3.3.1 Merged domain

Assuming that there are two user domains, user domain A and user domain B with each domain contains a few devices. As shown in Figure 18, both user domains can be merged into a common domain C, thus enabling all devices in domain C to have access to content licensed to both user A and user B. By binding rights to the user instead of devices, it provides the flexibility of enabling devices belonging to different users to share content. All devices of user domain A and B are merged into a single domain C. The usage rules for both domains now apply to the merged domain, as shown in Figure 18.

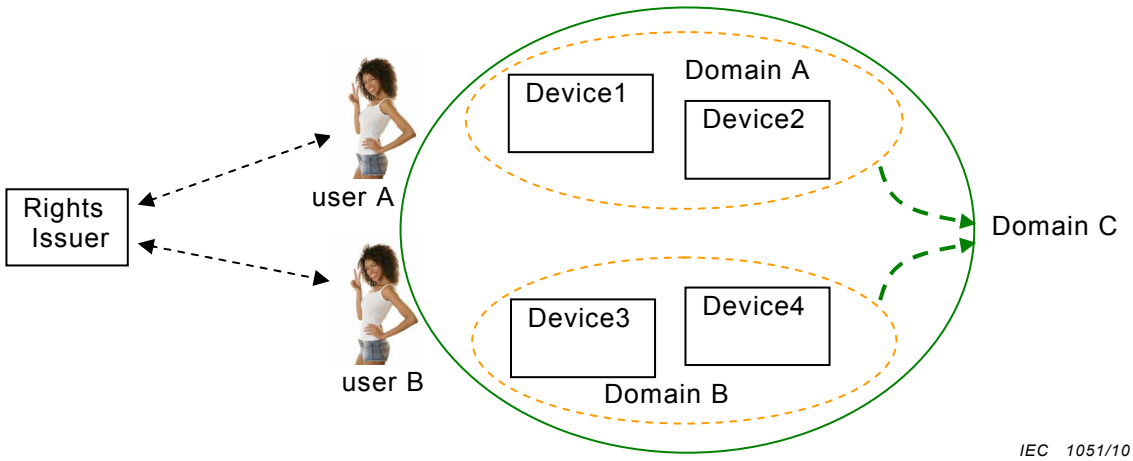


Figure 18 – Merged user domains

In this use case, although both user domains have been merged into a domain C, each user could maintain his or her own user domain at the same time. For example, device 1 is a member of both domain A and domain C. However, when domain A is disbanded, device 1 is still a member of domain C and hence has access to the content licensed to user B.

Merging of domains can also take place at the user entity level only. In this case, the rights and permissions of both user A and B are merged, thus enabling all devices in a common domain C to have access to all contents licensed to user A and B. When a device needs to be replaced, the new device can be added to the common domain C, hence does not need to be linked to all the users, as shown in Figure 19.

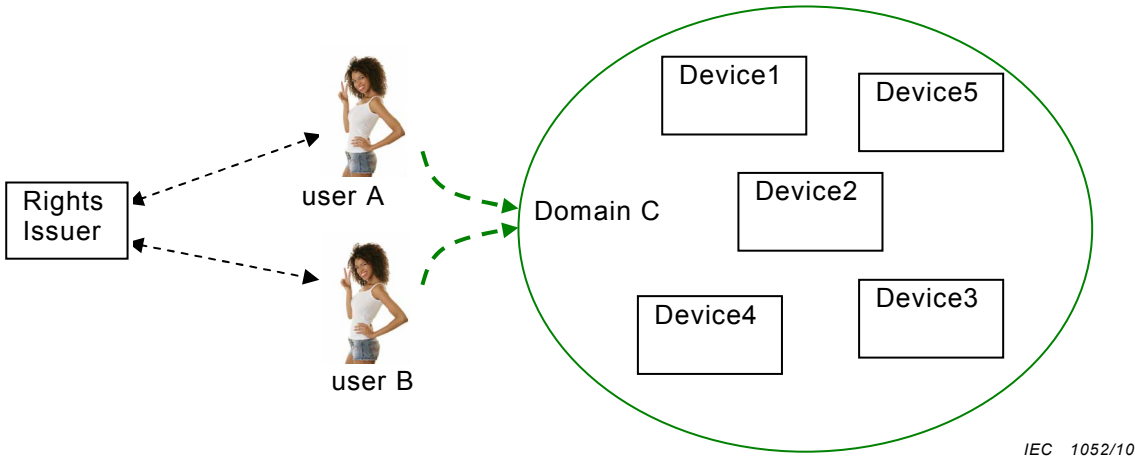


Figure 19 – Merging domains based on user entities

For situations where the right issuer issues licenses to domains instead of user entities, the merged domain C would have the permission to consume the content licensed to both domains A and B. Devices can be a member of both domain A and domain C which have different domain IDs. A device joining a sub-domain automatically becomes a member of the merged domain. However, when domain A has been disbanded, the usage rule for domain A will no longer apply and hence no device can join domain A anymore, as shown in Figure 20.

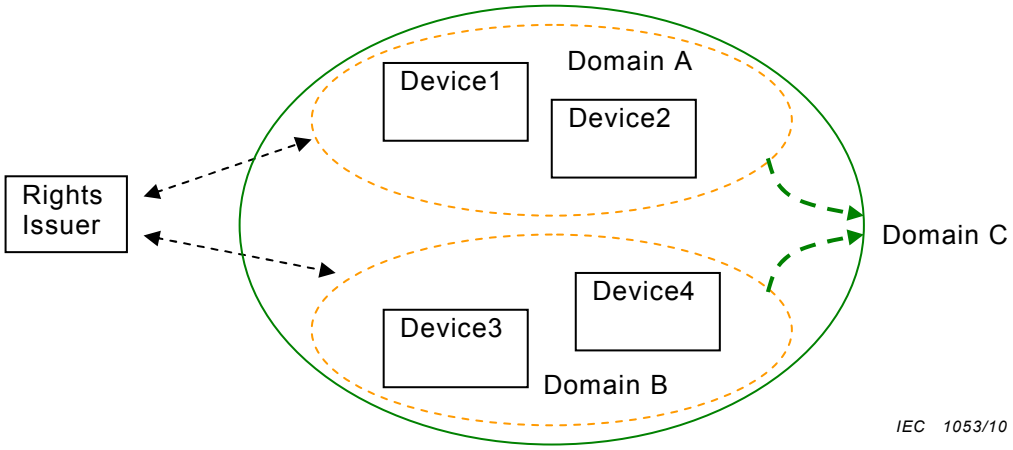


Figure 20 – Merged domain

5.3.3.2 Divorced domain model

In Figure 21, the merged domain C can be divided when a user decides to leave the common domain. This means that if a user leaves, all access rights belonging to the user are

automatically removed from the common domain. For example, when user A leaves, all devices belonging to domain A are no longer members of domain C. Therefore, contents licensed to user A will no longer be accessible to devices of domain B and C. Similarly, devices of domain A cannot access contents licensed to user domain B and domain C since they are no longer a member of domain C, as shown in Figure 21.

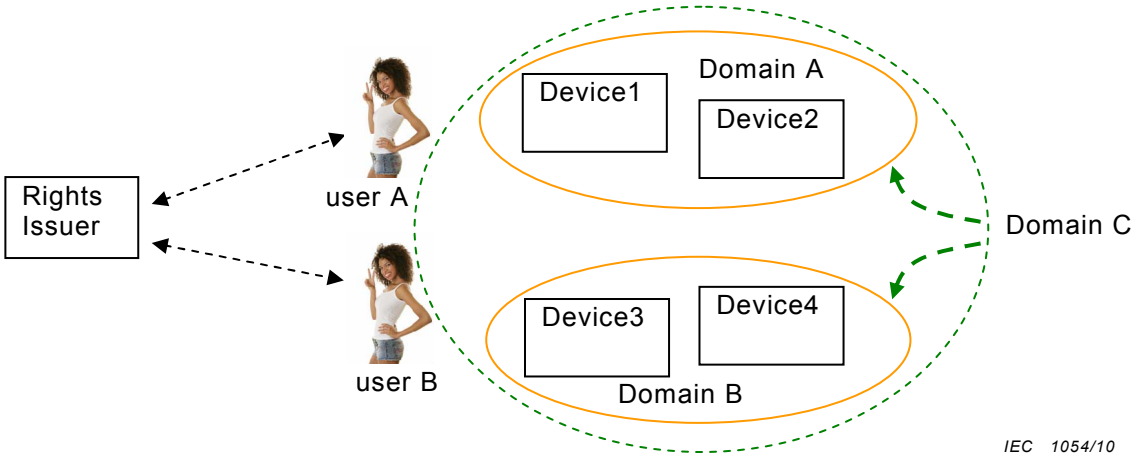


Figure 21 – Divorced user domain

A merged user domain can be divided in such a way that the user entities are split, while the device membership of domain C remains unchanged. Therefore devices of domain C can no longer access to contents licensed to users who have left the merged user domain, as shown in Figure 22.

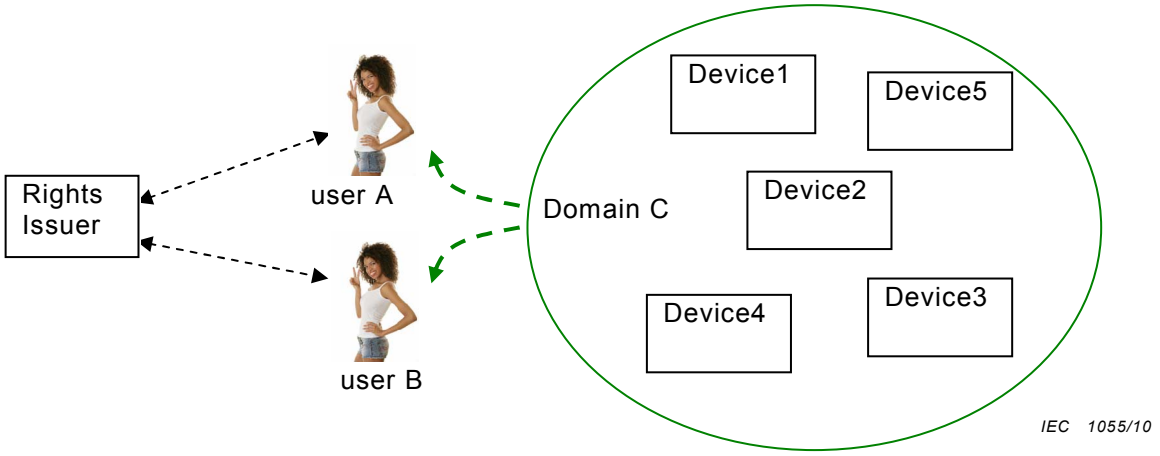


Figure 22 – Divorced user domain based on user entities

For a composition of domains in which rights or licenses are issued to domains directly, when domain C is divided into domain A and domain B, devices in domain A and B will no longer have access to each other's content. At the same time, since domain C has been disbanded, any usage rule for domain C will no longer apply and it is not possible for any device to join domain C anymore, as shown in Figure 23.

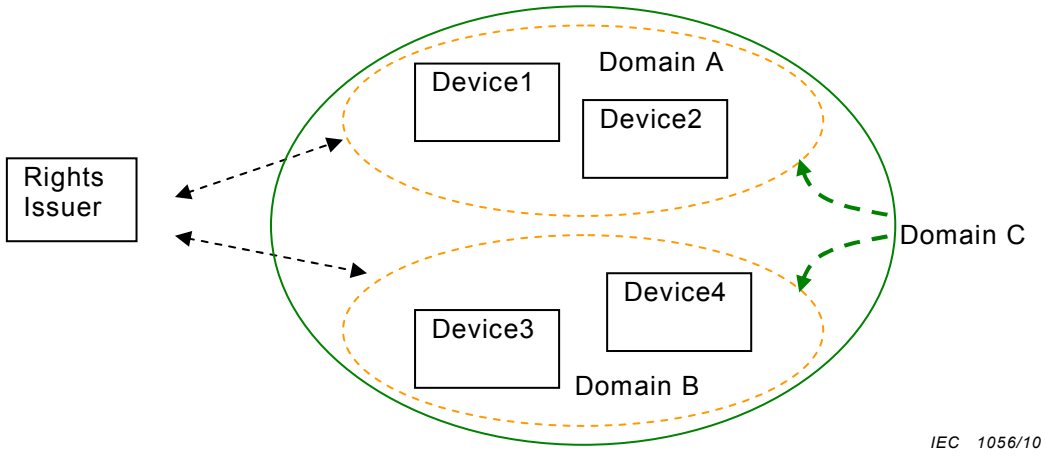


Figure 23 – Divorced domain

If a device works offline or some devices in a domain cannot connect to the rest of the devices, the domain is referred to as separated domain. A separated domain consists of multiple domains with the same domain ID.

Annex A
(informative)

Existing domain specifications

A.1 General

This annex compares items used in existing DRM related specifications to requirements specified in this Technical Specification.

A.2 Domain in DVB CPCM

The following applies; see also Table A.1.

- Reference Model: Basic model – Autonomous domain
- Requirement

Table A.1 – Domain specifications in DVB

	Parameter	Correspondent item in specification
Joining / Leaving domain	Device ID	CPCM_instance_id
	Domain ID	ADID (Authorized Domain ID)
	Domain key	ADS (Authorized Domain Secret)
Usage control by Usage Rule		USI in CL
Revocation of a device		CPCM revocation list (at the time of establishing of SAC (Secure Authenticated Channel))

A.3 Domain in OMA DRM V2.0

The following applies; see also Table A.2.

- Reference Model: Basic model – RI management domain
- Requirement

Table A.2 – Domain specifications in OMA

	Parameter	Correspondent item in specification
Joining / Leaving domain	Device ID	Hash of the Device's public key info
	Domain ID	Domain ID
	Domain key	128 bit AES
Usage control by usage rule		RO
Revocation of a device		Domain update by RI

A.4 Domain in ARIB TR-B27

The following applies; see also Table A.3.

- Reference Model: Basic model – RI management domain

- Requirement

Table A.3 – Domain specifications in ARIB

	Parameter	Correspondent item in specification
Join to / leave from domain	Device ID	CAS Card ID
	Domain ID	Domain ID
	Domain key	Domain Key
Usage control by Usage Rule		RMPI
Revocation of a device		RI's request for deleting domain information

A.5 Domain in permission code

Refer to IEC 62227. The following applies; see also Table A.4.

- Reference Model: Out of scope
- Requirement

Table A.4 – Domain specifications in permission code

	Parameter	Correspondent item in specification
Joining / leaving from domain	Device ID	–
	Domain ID	Permission Actor Identifier
	Domain key	–
Usage control by Usage Rule		Permission Code
Revocation of a device		–
NOTE Concrete technology of domain management is out of scope of this Technical Specification.		

A.6 Domain in Marlin DRM

The following applies; see also Table A.5.

- Reference Model: Marlin
- Requirement

Table A.5 – Domain specifications in Marlin

	Parameter	Correspondent item in specification
Join to / leave from domain	Device ID	Personality NodeID
	Domain ID	Domain NodeID
	Domain key	Scuba Keys
Usage control by usage rule		
Revocation of a device		Device Exclusion as defined in Marlin Starfish specification

A.7 Domain in iTunes FairPlay

The following applies; see also Table A.6.

- Reference Model: FairPlay
- Requirement

Table A.6 – Domain specifications in iTunes

	Parameter	Correspondent item in specification
Join to / leave from domain	Device ID	Computer ID
	Domain ID	User account / User ID
	Domain key	User key
Usage control by usage rule		Maximum of 5 PCs and unlimited number of iPods
Revocation of a device		

A.8 Domain in Coral

The following applies; see also Table A.7.

- Reference Model: Coral
- Requirement

Table A.7 – Domain specifications in Coral

	Parameter	Correspondent item in specification
Join to / leave from domain	Device ID	Unique ID for each device
	Domain ID	Domain ID
	Domain key	Using the key of the underlying DRM system
Usage control by Usage Rule		–
Revocation of a device		–
NOTE Coral is designed to enable interoperability between various DRM systems. It is not a DRM system itself.		

A.9 Domain in xCP Cluster Protocol

The following applies; see also Table A.8.

- Reference Model: Cluster Protocol
- Requirement

Table A.8 – Domain specifications in Cluster Protocol

	Parameter	Correspondent item in specification
Join to / leave from domain	Device ID	Unique ID for each device
	Domain ID	Cluster ID
	Domain key	Calculated from cluster ID and MKB (key management block) by each device
Usage control by Usage Rule		Expiration of contents by time and/or access count
Revocation of a device		Use KMB to revoke devices without legitimate AACS device keys
NOTE Cluster ID is a random number generated by the first xCP device that joins the domain, and kept securely in each device.		

Annex B
(informative)

Management for simultaneous information in a domain

Contents can be consumed on each device in a domain. A domain may be required to manage the simultaneous information in a domain.

The example methods to manage the simultaneous information in a domain are the following.

- Example 1

  A device which receives a usage rule first can indicate a part of the usage rule or usage condition to the other device. In other words, a device receiving a usage rule first can also be an issuer of permission.

- Example 2

  Devices belonging to a domain can transfer and share the information such as the joining device list or contents use condition. All devices in a domain hold the information in common.

Bibliography

The following documents provide additional or detailed information on each organization.

IEC 62227, *Multimedia home server systems – Digital rights permission code*

IEC 62455, *Internet protocol (IP) and transport stream (TS) based service access*

IEC 62481-1:2007, *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 1: Architecture and protocols*

IEC 62481-2:2007, *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 2: DLNA media formats*

[DVB] "*Content Protection & Copy Management Specification*" DVB Document A094 Rev.2, The Digital Video Broadcasting Project (DVB).

For all the DVB publications refer to
http://www.dvb.org/technology/standards/

DRM Architecture, Approved Version 2.0 Open Mobile Alliance (OMA)

DRM Specification, Approved Version 2.0 Open Mobile Alliance (OMA)

DRM Rights Expression Language, Approved Version 2.0 Open Mobile Alliance (OMA)

For all the OMA publications refer to
http://www.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx

[xCP Cluster Protocol] "xCP: Peer-to-Peer Content Protection; A new protocol for implementing an authorized domain"

[Marlin] "*Marlin - Common Domain Specification*" Version 1.1.1 Marlin Developer Community

For all the Marlin publications refer to
http://www.marlin-community.com/develop/downloads

[Coral] "Coral Domain Architecture Specification" Version 4.0, Coral Consortium

For all the Coral publications refer to
http://www.coral-interop.org/

Fairplay, Apple (www.apple.com)

[ARIB] "*Digital Broadcasting System based on Home Server*" TR-B27 Ver 1.0, Japanese version only

For all the Arib publications refer to
http://www.arib.or.jp/english/html/overview/rb_ej.html

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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