Title	Medianet: A framework to unify different distribution channels
Type	Report
Date	01/10/2004
Status	Final Version
Ref. / File	Medianet position paper
Author(s)	DIEHL Eric, et al.

1 Introduction

1.1 Scope and background

This document presents the solution that Medianet explores to reach a high degree of interoperability between different types of Digital Rights Management (DRM) systems and Conditional (CA) Access systems. The targeted devices are distribution channels of content for home-networked devices, including consumer electronic devices.

Section 2 presents the problem. Section 3 is an extremely brief state of the art of the currently explored approaches. Section 4 presents the approach studied by Medianet.

1.2 Abbreviations

CA	Conditional Access
CSS	Common Scramble System
DRM	Digital Rights Management
DVB	Digital Video Broadcast
DVD	Digital Versatile Disk
ECM	Entitlement Control Messages
EMM	Entitlement Management Messages
IPMP	Intellectual Property Management and Protection
OMA	Open Mobile Alliance
REL	Rights Expression Language
STB	Set Top Box

Table 1: List of used abbreviations

1.3 References

[1] CHENG S., RAMBHIA A., ***DRM and Standardization—Can DRM be standardized?***, in Digital Rights Management: Technological, economic, legal and Political Aspects, edited by BECKER E., et al., Springer Verlag, 2003

[2] FRANK A., ***The copyright crusade II***, Viant Media Entertainment, 2002

[3] KERCKHOFF A., ***La cryptographie militaire***, Journal des sciences militaires, vol 9, January 1883

[4] McCORMAC J., European Scrambling Systems: circuits, Tactics and Techniques, Third Edition, Waterford University Press, 1993

[5] RUMP N., ***Can Digital Rights Management Be Standardized?***, in IEEE Signal Processing Magazine, March 2004, Vol 21, N°2

[6] DVB CM CP Copy Protection at http://www.dvb.org/index.php?id=83

[7] DVB TM CPT Copy Protection technical at http://www.dvb.org/index.php?id=62

[8] http://www.smartright.org/

[9] http://www.xrml.org/

[10] http://odrl.net/

[11] http://www.openmobilealliance.org/

[12] "OPIMA Specification v1.1", OPIMA, June 2000

[13] "Overview of the MPEG-4 Standard", ISO/IEC JTC1/SC29/WG11 N4668, March 2002

[14] Kim J.H., Hwang S.O., Yoon K.S., Park C.S., "MPEG-21 IPMP", ICITA 2002, 2002

[15] "MPEG-Rights Expression Language WD v3.0", ISO/IEC JTC 1/SC 29/WG 11/N4816, May 2002

[16] "MPEG-21 Overview v.5", ISO/IEC JTC1/SC29/WG11/N5231, October 2002

[17] "MPEG-21 Requirements v.2", ISO/IEC JTC1/SC29/WG11 N6264, December 2003

[18] Rob H. Koenen, Jack Lacy, Michael Mackay, Steve Mitchell, "The Long March to Interoperable Rights Management", Proceedings of the IEEE, Vol. 92, No. 6, June 2004.

2 Position of the problem

The home network is the next paradigm for consumer electronic devices and IT. Only home networks will allow a successful triple play convergence. Through home networks, consumers will have access to numerous delivery channels. We may foresee three types of content providers:

- Broadcasters deliver content through broadcast channels. They may use terrestrial, cable or satellite carriers. Traditionally, Conditional Access (CA) systems protect content from piracy.
- Broadband providers deliver content through Internet connection. They use unicast or multicast models. Traditionally, Digital Rights Management (DRM) systems protect content.

- Telecom mobile operators deliver content to mobile phones, for instance through Universal Mobile Telecommunication System (UMTS). DRM systems protect content.

Figure 1 illustrates the environment of this paper. The Medianet security framework, in line with the global project objectives, aims at introducing some interoperability among the different potential distribution channels.

With a successful home network approach, consumers will continue to have time shifting for any content, but consumers will have also space shifting [2]. Alice should be able to access her content from any of her devices regardless of the source of content. Alice should be able to view on her TV the movie she bought and downloaded on her mobile phone. Obviously, Alice should be able to view on her TV the movie she just bought from her PC on Internet. She should also be able to view on her PC her regular satellite subscription programs.

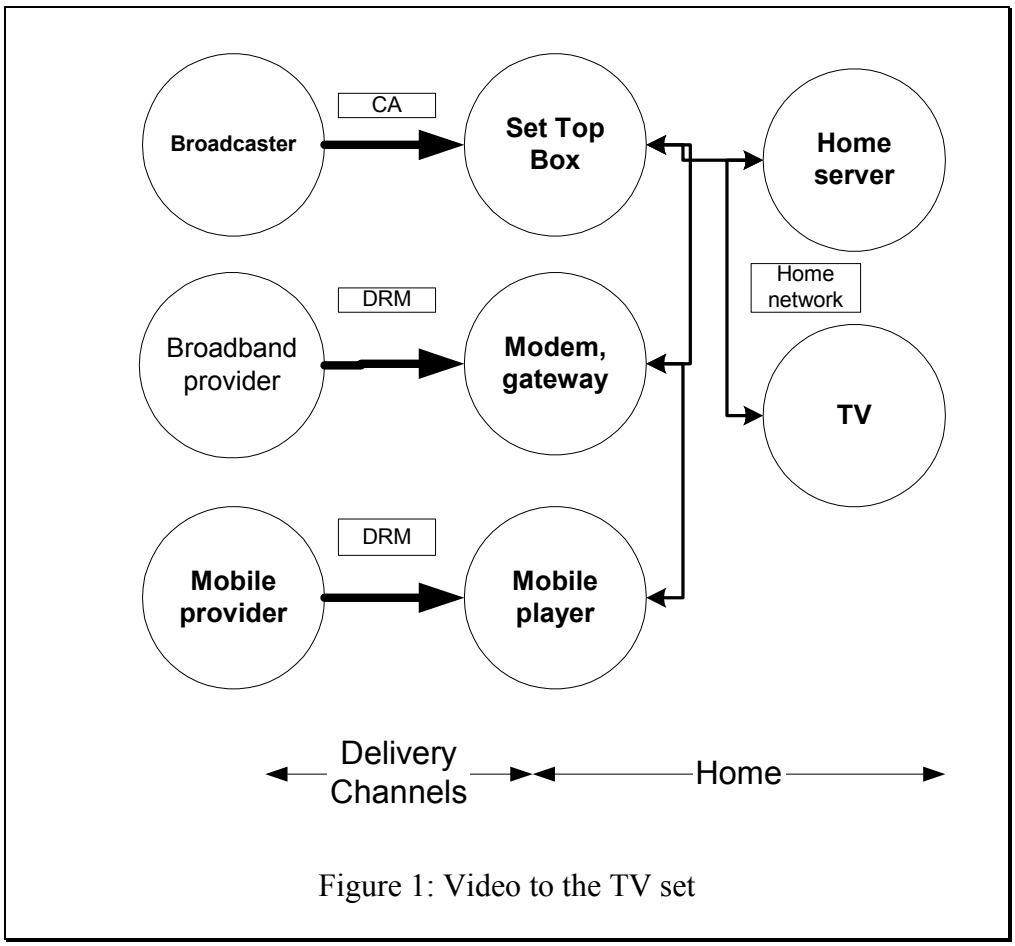

Figure 1: Video to the TV set

To enable these scenarios, several levels of interoperability need standardization. Unless standardization is reached, Alice should, at the minimum, have separate receivers and players for separate content owners or distributors, even if the media format is identical [1].

Unfortunately, Alice is enamoured with her player[1]. Furthermore, player implied personal investment. Thus, the lack of standardization will kill the adhesion of consumers to the future digital world.

Several targets of standardization are possible. Medianet focuses on one of them: security management and content protection.

3 The current approaches

3.1 Current trends in DRM standardization

Several initiatives cope with the interoperability issue of DRM. Many taxonomies exist for interoperability. An interesting one is given by [18]. Nevertheless, we will use a more simplified classification: The vertical approach and horizontal approach.

- The vertical approach solves the interoperability by defining one unique format and type of solutions used by every device. The format may be closed and proprietary or open.
- The horizontal approach solves the interoperability by defining some common interfaces and mechanisms while the definition of remaining elements stay open. The solution is necessarily open.

3.1.1 Vertical approach like OMA

The vertical approach solves the interoperability issue by using one unique complete solution, for instance for one given market. Open Mobile Alliance (OMA) is a good example [11] of a vertical but open approach. OMA targets mobile phones and can be used by mobile appliances. Nevertheless, this interoperability means that every device and every content provider have to support OMA.
Microsoft's DRM is obviously another example. We may believe that Microsoft could solve the interoperability issue by creating a de-facto standard.

3.1.2 Horizontal approach like MPEG21 IPMP

The horizontal approach solves the interoperability by standardizing some elements of DRM.

- Many efforts occurred on the Rights Expression Language (REL). There are two leading solutions: the eXtended rights Markup Language (XrML) [9] and the Open Digital Rights Language (ODRL) [10].
  This approach is not sufficient. To access the description of rights, device must first access the payload of license. If the license is protected by an unknown method, then device cannot use this interoperability layer.
- MPEG-4, and later MPEG21, normalized a framework (Intellectual Property Management Protection (IPMP)) that allows a content to define the different tools needed for its access, and a way to search and activate these tools [1].
  This approach may be interesting in computer domain. In the CE world, devices are

[1] An extreme example is Apple's iPod. Often, the iPod is perceived more than a basic device

limited in terms of external connections and processing power by opposition to normal computers, making the MPEG approach more difficult. It is hard to have a CE device downloading IPMP tools from a remote location and install them on the device to access protected content. However MPEG envisages also scenarios which are also adequate to the CE world, in which all the needed IPMP tools are installed on the CE device "a priori" and no download is necessary to access a given protected content. MPEG supports either the connected and disconnected scenarios. More information on the MPEG solutions can be found in [13], [14], [15], [16], [17].

- Another example is the OPIMA [12] approach. OPIMA defined a black-boxed architecture and identified some of its elements, such as content rendering modules, encryption and watermarking tools, but provided no details on how these components worked. OPIMA also defined two API's: an Application services API and an IPMP services API. The Application services API defines how an external application can interact with the OPIMA virtual machine (OVM), while the IPMP services API defined how the IPMP tools could interact with the OVM. IPMP tools can be downloaded and installed on the OVM, but the main difference between OPIMA and MPEG-4 or MPEG-21 IPMP, is that the IPMP tool only contains the mean to access to access and interpret content rules, it doesn't contain encryption or watermarking tools. An important concept in OPIMA is that content never leaves the OVM in an unprotected way.

3.2 The DVB approach

In the 80's, Digital Video Broadcast (DVB) organization faced an interesting problem. DVB wanted to normalize the design of Set Top Boxes for satellite distribution in order to reduce their price though economy of scale. Thus, DVB standardized the use of MPEG2 as the format of the transport stream (DVB-TS), and the signalling (DVB-SI). This was sufficient for free-to-air operators, but not suitable for Pay TV operators. They needed to control the access to broadcast content. DVB attempted to normalize the conditional access (CA) system. At the start, this failed. DVB is consensus driven. CA providers could not reach consensus. Every CA provider wanted its own format of license, its own key management, and its own algorithms[2]. DVB decided to narrow the scope of standardization. They seek a common acceptable ground. This approach was extremely successful.

DVB standardized the following elements:

- The scrambling algorithm that protects the actual content; every protected DVB content is scrambled using DVB Common Scrambling Algorithm (DVB-CSA).
- The placeholder and signalling of data structure that carries the descrambling keys. This data structure is called Entitlement Control Message (ECM)
- The placeholder and signalling of data structure that carries the user's associated rights. This data structure is called Entitlement Management Message (EMM)
- The Interface between the STB and the Conditional Access Module

[2] A standard of CA, EUROCRYPT, already existed coming from the early years of DMAC and D2MAC. But players such as NDC, or NAGRA did not want to support it [4].

DVB does not standardize the payload of ECM (resp. EMM). DVB does not standardize the method protecting the ECM (resp. EMM). Each CA provider uses its own data structure and proprietary protection means.

On these bases, DVB offered two paths towards interoperability:

- Simulcrypt, where each set-top box recognizes and uses the appropriate ECM and EMM needed for authorization,
- Multicrypt allowing multiple CA systems to be used with one set-top box by using different CA modules.

This approach is one of the key successes of DVB. It allowed designing cost effective DVB compliant scrambler-encoders, or DVB chips sets for STBs. The markets choose their preferred solution. Nowadays, it is clear that Simulcrypt allowed a fair competition between CA providers.

The next step is the standardisation of content protection within home network. Currently, DVB-CP/CPT [1], [7] attempts to define a Content Protection and Copy Management System. DVB-CP/CPT acknowledges the need to support all the previously mentioned delivery channels.

3.3 SmartRight™ approach

The SmartRight consortium [8] proposes an innovative approach that provides content protection within home network and supports any CA and DRM systems. SmartRight defines a standard set of scrambling algorithms. These algorithms are the dominant algorithms used in standardised content protection (DVB-CSA, Triple DES, AES). It defines also a uniform protection method for the descrambling keys.

Through this approach, SmartRight succeeded to create the notion of Personal Private Network. The Personal Private Network is the set of devices linked through digital connections that belong to a same family. The devices may be wired, or wireless. The devices may be in proximity or in remote locations. Within her Personal Private Network, Alice can access any of her legal contents from any TV sets or mobile players.

4 Medianet approach

4.1 The solution

Medianet intends to apply an approach similar to DVB's one but adapted to its specific environment. The controlled access of content can be analysed following a layered model. Figure 2 illustrates this model

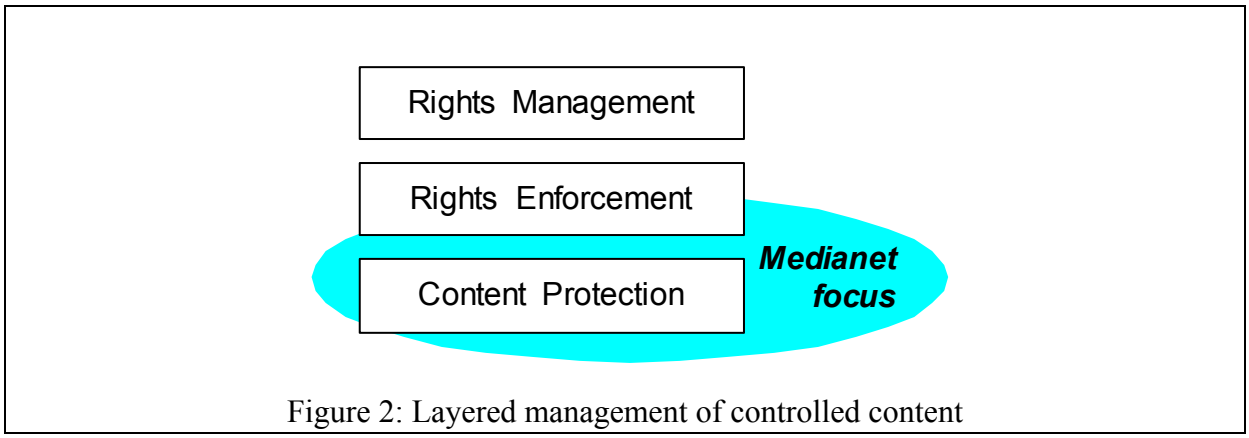

Figure 2: Layered management of controlled content

Medianet simplified model has three layers:

- The Rights Management layer defines the conditions needed to access the content. The description of these rights uses a REL. We will call the data structure describing these rights the license. In simplified terms, this layer is about managing digital rights.
- The Rights Enforcement layer has several roles:
  - The protection of the digital rights associated to the content
  - The verification of the user's right to access the content according to the requested digital rights.
  - The protection of the descrambling keys

  In simplified terms, this layer is about digitally managing rights.
- The Content Protection layer defines how the content should be protected. It defines the scrambling algorithm3, the size of descrambling keys, and their crypto period. In simplified terms, this layer is about creating and opening a secure container. An additional feature is an optional watermark. The workload of the watermark depends on the upper layers.

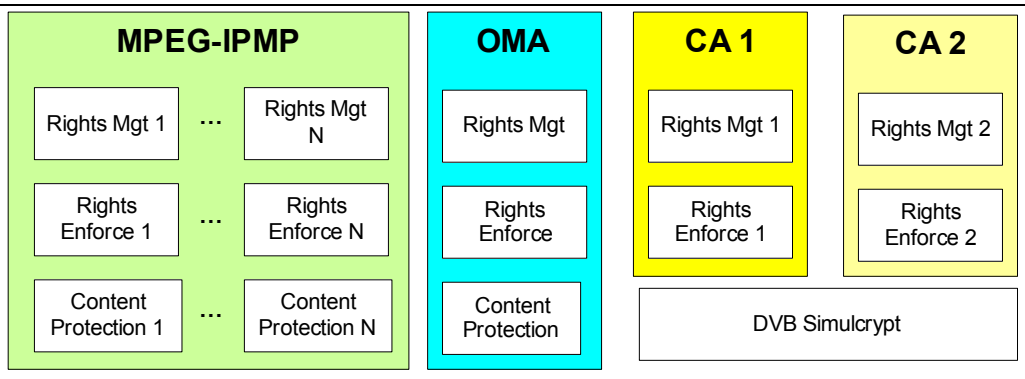

Figure 3: Mapping of current standards to the three layer model

Figure 3 provides as reference the mapping the solutions described in section 3 to this three layer reference model.

[3] In this document, although it is an encryption algorithm, the process protecting content is called scrambling. The process protecting the keys and rights is called encryption. This is an efficient semantic method to discriminate the protection from content from protection of licenses.

Like DVB, Medianet proposes to standardize the content protection layer, and a method to cope with the Rights Management and Rights Enforcement layer. This standardization should encompass all the distribution channels and the home network distribution.

Figure 4 illustrates the expected result. Several Digital Rights Management (DRM1, DRM2, DRM3) and Conditional Access Systems (CA1) share a common protection layer with a home network copy protection scheme (Home CP). The receivers (or acquisition points) will hold the DRM and CA. They will use the home network copy protection to transfer securely content to the displays. Because they all use the same content protection scheme, content will only be descrambled by the rendering unit, i.e. the end of the video chain. This protection layer has to be compliant with existing solutions such as OMA 2.0, or DVB. Therefore, we foresee that the scheme will support several content protection formats.

As a next step we may also consider so-called content roaming, i.e. content transfer from DRM x to DRM y. In this case, generic solutions for the Rights Management and Rights Enforcement layer are required.

Medianet does not preclude other standardization efforts. For instance, in Figure 4, DRM1 and DRM2 share the same REL. They could even share the same device.

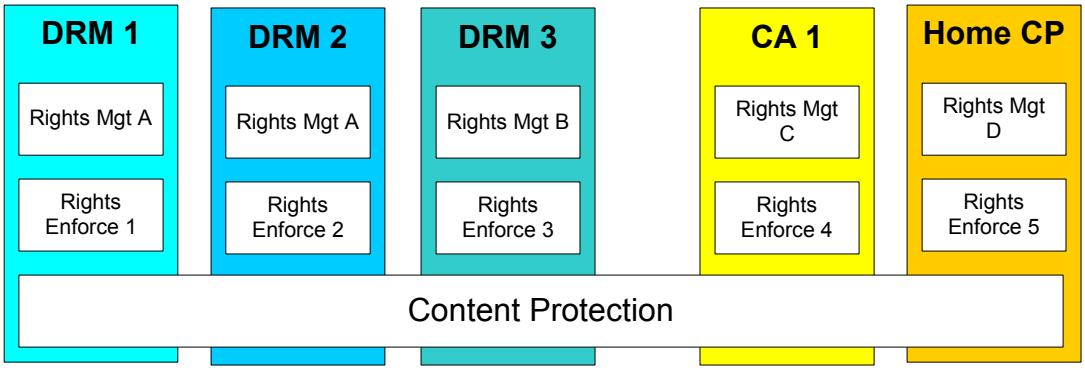

Figure 4: Interoperability layer

4.2 The rationales

- **Compatible with current approaches**

Medianet approach is not orthogonal to other on-going approaches. For instance, layer **Rights Management** needs a REL. Medianet approach does not preclude the use of XrML, or ODRL. Similarly, it would be possible to implement Medianet vision within the MPEG21 IPMP framework. The content protection layer would be a defined toolset.

- **Mass market for chipset that will embed resource consuming processes**

The content protection layer encapsulates all the security processes that may require a lot of resources. Standardizing them will allow the creation of new chipsets that support it, as

currently in the market of Set Top Boxes. Descrambling and real time watermark detection are resource-consuming processes especially for high definition content. The management of digital rights and the digital management of rights are comparatively less resource consuming. They correspond also to a peak activity and not a steady one as descrambling and detection.

It may be argued that using the same security measures everywhere is a weakness. The typically cited example is Content Scramble System (CSS). CSS is the protection scheme of DVD. Since 1999, it is broken. Thus, every DVD can be pirated. In the case of Medianet, it is a wrong assertion. One of the most important laws of security is Kerckhoff's principle [2]: The designer of a cryptographic system should suppose that the adversary knows the details of his algorithms except the secret key. The content layer will find the right tradeoffs to allow easy renewability of key management. It will use only well studied cryptographic algorithms. He actual protection of the descrambling key is the responsibility of the Rights Enforcement layer[4].

- **First layer of interoperability between broadcast, broadband and telecom worlds**

Using the DVB-CP terminology, a consumption point (such as a TV set, or a mobile phone, …) would be able to render content coming seamlessly from broadcast, broadband, or telecom links. It just has to support the content protection layer. It is fully compatible with the promising concept of Authorized Domain.

This is fully inline with Medianet global position about facilitating end-to-end services.

- **Creation of an environment open to a fair competition between DRM systems**

Medianet framework will allow content providers to select their preferred DRM solution(s). The content protection will be the same and supported by the players. It just has to deliver the right gateways or modules. Consumers have the insurance that their players (rendering devices) will be compatible with any merchant[5].

- **First step towards roaming for contents**

Content roaming is one of the next interesting paradigms. Many scenarios can be drawn. For instance, enjoying your latest movie on the device of a friend incorporating a different type of DRM system. Having a common protection layer is an enabling factor for roaming. Leaving mainly the rights management layer and the rights enforcement layer as points of interoperability concerns. A connection based interoperability type of solution [18] seems very suitable to solve these concerns.

5 Conclusions

Medianet will propose a security framework common to DRM and CA based on a common content protection layer. This approach is fully in line with the overall goal of Medianet.

[4] It should be noted that in case of CSS, it is not the scrambling algorithm itself that was broken, but the secret keys themselves that have been disclosed.

[5] Today, when a French consumer buys a TV set, he knows that he will be able to view content on it from Canal + or TPS, provided he has the right STB. The same will occur on the ADSL connection.

This approach is complementary to other current standardization approaches (MPEG21, REL, …). Furthermore, it introduces some interoperability between three distribution channels: broadcast, Ethernet, and mobile telecom.

Medianet will propose its framework as a contribution to an enhanced interoperability for DRM and CA. Working together with other standardization efforts, we will be able to create the conditions for a future fair digital world for consumers, content providers, and content owners.

Furthermore, standardization of the protection layer is the first step towards roaming. Once this layer is designed, we may start to analyse the roaming problem.