Interoperability Issues in DRM and DMP Solutions*

Xiaofan Chen[1] , *Tiejun Huang*[2]

[1] Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China
[2] Peking University, Beijing, China
Email: {xfchen, tjhuang}@jdl.ac.cn

ABSTRACT

This paper presents an ongoing Digital Right Management (DRM) standard: Digital Media Project (DMP), which is active as an interoperable DRM solution in recent three years. We start by reviewing the important works of DRM standards at present, mainly focusing on their interoperability issues. Then we describe the core techniques in DMP and explain how they fit into an interoperable DRM system. We also give a report on the development of the reference software of DMP – Chillout, which is an open source project. Finally, we outline several tasks that we will undertake in the next step of DMP to optimize this technical standard.

1. INTRODUCTION

The daily commerce of digital music and movies is coming towards us with tremendous speed. Spurred by this huge new profit, companies begin to develop technologies to deliver their media content to the subscribers in a secure manner. "Secure" here demands integrity, confidentiality and authorization [1]. Integrity means that the media content should arrive to the end user without being tampered. Confidentiality means that privacy should be assured during transmission. Authorization means that only authorized consumers can perform legal actions to the media content according to the contract (named license). These three elements constitute the basic goals of Digital Rights Management.

There have already been DRM applications in the media Content Industry. Apple's iTunes [2] and Microsoft Windows Media DRM [3] are examples of successful proprietary DRM systems. Each of the two systems supports its own DRM format, but cannot be merged into the other one. And there is not a device that can play both of the two formats. Besides the two systems, some other proprietary DRM applications are emerging with their own formats into the market at any moment. What is more, different countries and regions may legally adopt different cryptographies. How to make these different systems cooperate is becoming a tough issue.

2. CURRENT EFFORTS IN BRINGING INTEROPERABLE DRM SYSTEMS

Rob H. Koenen [4] described three different ways to address full DRM interoperability. 1) Full Format Interoperability. This means that the interchanging representation of the media content must be the same and every device in the value chain performs strictly as the standard defines. This philosophy achieved great success for mp3 and DVD. But is rigid and lack of robustness and renewability. The crack of DVD security system is an example. 2) Connected Interoperability. This means that there are third party service providers who are on line and are doing the negotiation and transformation job almost transparently for the end users. This requires the end user to have the ability to link to the Net. 3) Configuration-Driven Interoperability. This allows end user devices to download and configure new modules that can support the formats which come from the other systems.

Koenen and the Coral Consortium [5] built the experimental Networked Environment for Media Orchestration (NEMO) [6]. NEMO chooses the Connected Interoperability way for different DRM formats to cooperate. By 2006, Coral had shown its interoperability with Microsoft Windows Media DRM and OMA DRM [7], both of which do not need to make modifications to their own technologies. But the NEMO focuses only on the transformation of existing DRM technologies. In that case different types of DRM solutions may still flood into the market. In that case the transformation work of the NEMO system may expand without control. NEMO servers take all the work of transformation, which may turn to a heavy burden of the servers and the networks.

There is another way out. Moving Picture Experts Group (MPEG) and Digital Media Project (DMP) combine

* Authors of this paper have been actively involved in the standardization of DMP Interoperable DRM Platform II and the development of its reference software – Chillout.

the Full Format Interoperable Standard and the Configuration-Driven Interoperable Scheme together, and produce significant multimedia DRM Standards that could be implemented universally.

In June, 2000, MPEG-21 "Multimedia Framework" standard (ISO/IEC 21000) was officially started. Since then, a large collection of technologies that enable multimedia DRM have been provided into this multimedia framework. However, the collection of technologies is just "tools". MPEG-21 is not designed to fit in the role as an integrated multimedia solution, like MPEG-1 and MPEG-2. So it is necessary to draw a new MPEG-A standard on the application level to make a combination of the various MPEG technologies. So comes the MPEG-A Multimedia Application Format (MAF) [8].

DMP is a not-for-profit open organization leaded by Leonardo Chiariglione, who is also the chair of MPEG, with the mission to promote continuing successful development, deployment and use of digital media in an interoperable way [9]. In July 2006, MPEG accepted a proposal from DMP entitled Media Streaming MAF (MS MAF), which is based on DMP's Interoperable DRM Platform II (IDP-2) [10]. In the following sections, we will briefly describe IDP-2 and its implementations, and explain how the devices interoperate in the media value chains.

3. DMP IDP-2 KEY TECHNOLOGIES TO ENABLE INTEROPERABLILITY

3.1 Architecture of Devices in the DMP Media Value Chain

Figure1 describes the architecture of DMP Devices. In DMP, Devices are defined as a combination of hardware and software or just an instance of software that has a certificate and allows a User to execute Functions. Devices interoperate with each other need to have mutual authentication first by an exchange of their own certificates provided by the CA via the Device Identification Device (DID). Each Device plays a logical function: Content Creation Device (CCD) encapsulates one or more pieces of media resource (may be encrypted), together with the Representation (with a License Template embedded in it) written in Digital Item Declaration Language (DIDL) [11], into DMP format; Content Identification Device (CID) then puts a unique content Identifier into the Representation of the content, signs the Representation, and stores the content Identifier and signature in its database for later verifications; License

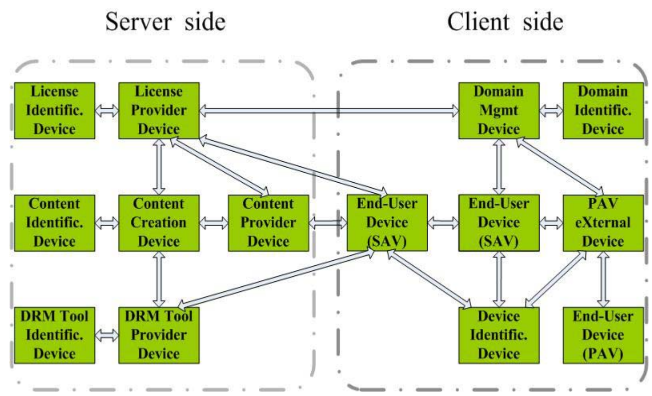

Figure 1 Devices in the value chain

Provider Device (LPD) creates a real License from the License Template of a DMP media content (already created by CCD) for a specific End-User SAV and may embed it within the DMP media content, telling the user device to operate exactly as the contract permits; Content Provider Device (CPD) then sells the content and deliver it to the end-user's device; Stationary Audio Video Device (SAV) at the end-user's side parses the DMP content and tries to decrypt the resource inside a secret place called DRM Processor; If the resource is encrypted and protected in an alien DRM scheme and there isn't any corresponding DRM tools embedded within the content, the DRM Processor will try to download the right DRM Tool according to the DRM Tool Information embedded in the content Representation, from DRM Tool Provider Device (TPD); At the same side of the SAV, the Domain Management Device (DMD) manages the consumer devices, including SAV and Portable Audio Video Device (PAV) in the home network.

3.2 DMP Content Representation

MPEG-21 utilizes the XML technology [12] in its Digital Item Declaration Language (DIDL), which can be processed by machine and is open for interoperability. DMP profiles and refers part of the MPEG-21 technologies and other technologies and develops part of its own schemas. The information written in the grammar of DMP Schema gives an all-around description of the DMP Content, including Content Identifier, Metadata, Resource information (Resource id, Resource URL, etc.), and DRM Information (License, IPMP Info, etc.) All of this descriptive information together forms the DMP Content Information (DCI). See figure 3.

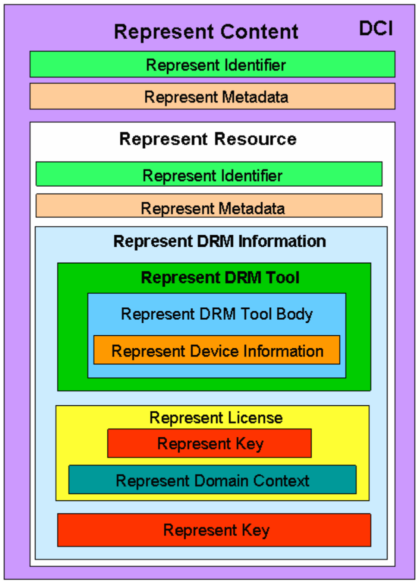

Figure 2 DMP Content Information (DCI) Hierarchy

DCI scheme is designed to be open and interoperable with other technologies. For instance, Metadata in DMP profiled the TV-Anytime Metadata [13]. Below is an example of metadata in the DCI:

```
<dmp2rc:Metadata>*
        <dmp2rc:StructuredData>
                <!-- TV Anytime metadata -->
         </dmp2rc:StructuredData>
</dmp2rc:Metadata>
```

Besides TV-Anytime, DMP can also support other metadata brands to be put inside the structure of DCI:

```
<dmp2rc:Metadata>
        <other brand's metadata/>
</dmp2rc:Metadata>
```

We know from section 3.1 that the End-User SAV can download and configure new DRM Tools from TPD to tackle new DRM formats. In that way the DRM Tools' URL should be put into the corresponding place of the DCI so that the SAV can find it. In another case, DRM Tools themselves can be put into the DCI, inside element <dmp2_ipmpinfo:Tool>. New DRM Tools being provided or referenced in the DCI makes DMP's interoperability with other DRM scheme quite convenient.

* dmp2:rc is the prefix of the Metadata element. It associates with the namespace declaration: 'xmlns:dmp2rc="urn:dmp:idp2:Represent:Content:2006:02' at the of the xml file. The following xml elements' prefixes may be different but similar.

3.3 DMP Content Package as file

DMP inherits MPEG-4 part12: ISO Base File Format [14] and defines DMP Content Format (DCF). The typical thing is that all the data are organized as boxes in one file. Particularly, "ftyp" box holds the File's brand, the "xml"/ "bxml" box holds the DCI in text or binary format [15], and the "mdat" box stores the audio/video resources. Different DRM standards may have different File Formats and different boxes, but we can seek out the exact data according to the semantics of the file structure. For example, the data that is picked out of DCF's "mdat" can be recognized by other DRM systems as the media resource, if those systems have made some simple configurations in the file parsing modules.

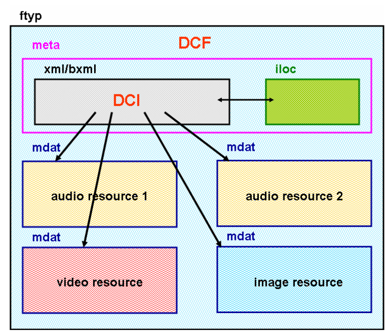

Figure 3 DMP Content Format

4. DMP IDP REFERENCE SOFTWARE -- CHILLOUT

Chillout is the name of the DMP Reference Software, released as Open Source Software under Mozilla Public License 1.1.

Chillout is based on Java2 Platform. Java Security provides the APIs for encryption, decryption, hash, etc. Device Identification Device uses EJBCA to arrange certificates for Devices.

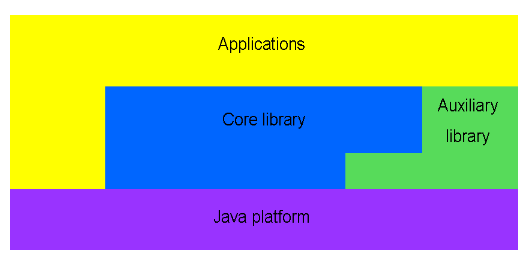

Figure 4 Chillout Development Layers

As the schemas of DCI are ready, we use Java Architecture for XML Binding to turn the schemas into Java classes. We call these classes Core Library classes (Figure

5). Using them, we can set/get the elements in the DCI, and develop DCIMaker and DCIParser, which are put into the Auxiliary Library. There are also other Auxiliary Library classes, SecurityManager for instance, which encapsulates the Java Security APIs, and are invoked by Applications who need security processing. The Applications in the up level are DMP Devices -- CPD, LPD, SAV, etc. They utilize Web Service to communicate with each other via the DMP protocols. (Figure 1)

Currently the experimental system runs. The server devices (CPD, LPD, CID, DID, and Darwin Streaming Server) are running in JDL lab, China. The End-User SAV can access them and play governed media content according to their Licenses. In IBC2006 Amsterdam, a demonstration of Chillout is given and achieved a great success. The next steps for Chillout are to finish TPD and develop Domain Management Device.

5. DMP'S NEXT PHASE

There is still a lot of work to be done for DMP in the following IDP-3. We are going to support nested DCIs because a DCI may have a hierarchical relationship with one or more different DCIs. And we will define Represent Right Data (RDD) ontology to support usage control of Content throughout the media Value Chain. DMP Represent Rights Expressions is based on MPEG-21 Rights Expression Language and supports various Rights and Conditions for SAV such as 4C Entity's Copy Control Information (CCI) [16] and TV-Anytime's Rights Management and Protection Information (RMPI) [17].

6. CONCLUSION

In this paper, we analyze an important issue in today's DRM systems – interoperability. Then we introduce DMP, an active interoperable DRM standard, and describe its key technologies that enable its interoperability. We present the experimental project to implement DMP -- Chillout, and discuss some issues that need to be done in the next phase for bringing the Interoperable DRM Platform III.

7. ACKNOWLEDGEMENT

We are grateful to all of the DMP and Chillout friends. The work is supported by the AXMEDIS (Automating Production of Cross Media Content for Multi-channel Distribution) Project.

REFERENCES

1. Yu, H. "Digital multimedia at home and content rights management", *IEEE, Proceedings 2002 IEEE 4th International Workshop on Networked Appliances*, pp. 49-56, 2002
2. Apple FairPlay DRM, http://www.apple.com/iTunes.
3. Microsoft Windows Media DRM, http://www.microsoft.com/windowsmedia/drm/.
4. Rob H. Koenen, Jack Lacy, Michael Mackay, Steve Mitchell, "The Long March to Interoperable Digital Rights Management," *Proceedings of the IEEE*, vol. 92, issue 6, pp. 883-97, 2004.
5. Coral Consortium Corporation. Coral Consortium Whitepaper[EB/OL].[2006-08-01].http://www.coral-interop.org/.
6. W.B. Bradley and D.P. Maher, "The NEMO P2P Service Orchestration Framework", *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS'04)* - Track 9. pp. 90290c, 2004.
7. Open Mobile Alliance, http://www.openmobilealliance.org/
8. KP Diepold, FW Chang, "MPEG-A: multimedia application formats", *Multimedia, IEEE,* pp. 34- 41 2005
9. Digital Media Manifesto, http://www.dmpf.org/manifesto/
10. The DMP IDP-2 Specification. http://www.dmpf.org/project/ga09/idp-2.html
11. ISO/IEC FDIS 21000-2, Information technology – Multimedia framework (MPEG-21) – Part 2: Digital Item Declaration, May 2002 (N4813).
12. W3C, "XML Schema Part 1: Structures Second Edition W3C Recommendation 28 October 2004", http://www.w3.org/2001/XMLSchema
13. ETSI TS 102 822-3-2 v1.3.1 (2006-01); Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 2: System aspects in a uni-directional environment
14. ISO/IEC 14496-13, Information technology — Coding of audio-visual objects — Part 12: ISO Base File Format.
15. ISO/IEC 21000-16, Information technology – Multimedia framework (MPEG-21) – Part 16: Binary Format
16. J. A. Bloom, I. J. Cox, T. Kalker, J.-P. Linnartz, M. L. Miller, and B. Traw, "Copy protection for DVD video," *Proc. IEEE*, vol. 87, pp. 1267-1276, July 1999.
17. ETSI TS 102 822-5 v1.1.1; Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime Phase 1"); Part 5: Rights Management and Protection (RMP) Information for Broadcast Applications.
18. Susanne Guth, Gustaf Neumann, Mark Strembeck, "Experiences with the enforcement of access rights extracted from ODRL-based digital contracts", *ACM Workshop On Digital Rights Management*, pp: 90-102, 2003.