Chapter 1 Introduction

Digital rights management (DRM) provides content providers with the means to protect their proprietary music or other data from unauthorized copying and other illegal uses. DRM technology protects digital content by encrypting it and attaching to it usage rules that determine the conditions under which a user can play back the content. Usage rules typically prevent copying or limit the number of times that the content plays.

Many existing DRM systems in the market may no longer sustain, due to the rapidly growing computer technology. This is one of the serious problems encountered in digital content delivery business. It is therefore desirable to establish a robust flexible DRM system. Furthermore, the need to deliver content anytime, anywhere in the world, and at any device, demands an industry-wide standard to guarantee interoperability. So, MPEG group determine IPMP (Intellectual Property Management and Protection) norm to meet many DRM system. IPMP-X is the extension to the old MPEG-4 IPMP hook. IPMP-X is a DRM architecture and provides a normative framework with a set of communication protocols to support many DRM requirements. .

1.1 The Role of IPMP in DRM system.

DRM system consists of a lot of processing chains that its functionality maybe include IP asset creation, capture ,IP asset management and IP usage module. But IPMP doesn’t define all the components of DRM system. It only defines one of the processing chain in the DRM system (see figure 1-1). Its purpose is to define a complaint terminal platform such that for various terminal systems there is a

consistent usage environment for the right associated with content. This will allow the DRM systems and manufactures have a standard to follow and guarantee its interoperability. Its advantages are described in the section 1.3.

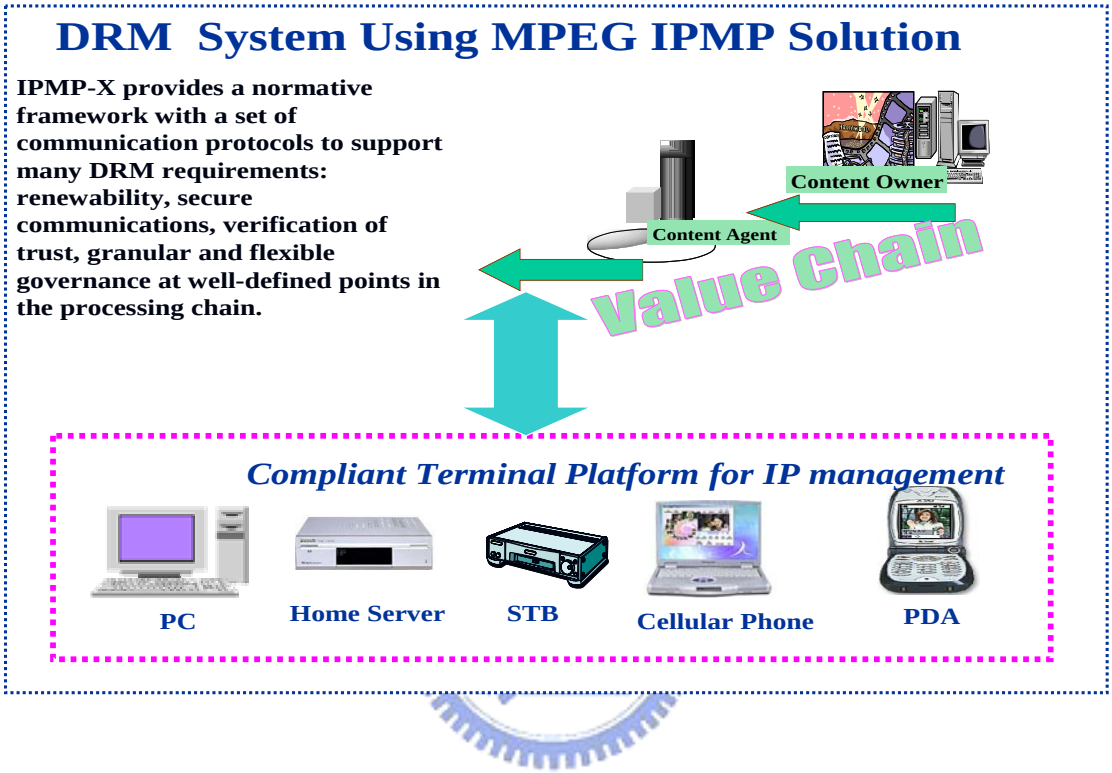

Figure 1-1 DRM System Using MPEG IPMP Solution

1.2 Why IPMP-X

IPMP-X provides a normative framework to support many of the requirements of DRM solution, as for example renewability, secure communications, verification of trust, granular and flexible governance. A large part of what every DRM application needs is supported normatively, allowing DRM solution providers to concentrate more on the services and features of their DRM solution as opposed to worrying about lower level functionality.

MPEG-4 IPMP-X can be used to host any type of media protection at a varied

level of granularity and complexity as required by the specific DRM system employed to protect a given content within MPEG-4 Systems. MPEG-4 IPMP-X may protect any kind of media content included in an MPEG-4 stream, as for example video, audio, computer graphics, text and interactive contents, etc.

1.2 MPEG-4 IPMP-X Benefits[22]

The benefits of MPEG-4 IPMP-X include the following:

(1) Reduction of redundant implementation

Many different DRM solutions use similar or the same components for a number of functionalities. An example could be the use of DES for decryption. If a given terminal supports DES, any DRM solution may use the terminal implemented DES as opposed to providing its own. If two DRM solutions use DES, the algorithm need not be implemented twice. Additionally, a given DRM solution need not know whether or how a given service is provided. It may simply ask if the functionality is provided and if so, use it whether or not the Terminal provides it or a loadable module provides it.

(2)Security:

IPMP-X provides methods to perform mutual authentication and use the secure authenticated channel to support secure communications between terminal/ tool requiring it. Additionally mutual authentication can be used purely to verify existing trust relationships as they may exist or be required in a given DRM solution.

(3) Interoperability:

It is interoperable to identify what is provided by the architecture and what must

be provided by a given DRM solution and by making what must be provided by the DRM solution.

(4) Renewability:

Mutual authentication can be used to verify the validity of certificates and credentials. Additionally, a tool is replaced (renewability) in case of security breach, enabling content owners to safely deploy their assets.

(5) Flexibility:

One can choose which IPMP tool to perform various methods such as watermarking, user authentication or data integrity checking, enabling systems manufacturers to maintain security of their solutions.

(6) Dynamic operation:

The IPMP Tools required to protect a certain content such that it can enable a variety of businesses to flourish based on IPMP-X solutions.

1.4 Security of IPMP-X Tools communication

The details of the design of IPMP tools depend on applications developers. Although IPMP-X is not complicated and in fact only makes normative a number of processes that every DRM implementation needs to perform, some very complicated and intricate protection schemes can be supported with no additional overhead.

To facilitate the cooperation of multiple tools for the protection and governance of content, a message-based architecture is provided by IPMP-X. IPMP Tools

communicate with each other and the terminal by using the standard messages defined in IPMP-X specifications. IPMP-X defines a set of mutual authentication messages that can be used to verify the trust of IPMP Tools/Terminal, and provides a secure channel for the exchange of messages between any pair of IPMP Tools or between IPMP Tools and the IPMP-X compliant terminal.

1.5 Introduction to Application Based on IPMP-X

An simple example illustrates possible uses and design issues associated with IPMP-X framework.

Consider a server that will deliver encrypted MPEG-4 encoded content to an authorized MPEG-4 client. The decryption keys and rules for usage of the content can either be included in the security container or distributed separately. It depends on the requirements of the application.

The client contains an IPMP-X System that includes a certified key pair that is used to establish and maintain a cryptographic peer relationship between client and server. The IPMP-X system includes an encryption/decryption engine, and various cryptographic hash functions to ensure content and license integrity . IPMP-X may contain mechanisms for securely managing various credentials for managing the use of the content.

The server delivers the content decryption keys to the client. The server encrypts with the session key. These keys are delivered via IPMP-ES. The mapping of keys and content is accomplished by IPMP-X descriptors associated with the content. The IPMP-X system extracts the content encryption keys from the IPMP-ESs and route

content to specified IPMP-X Tool. The IPMP-X Tool decrypts content buffers protected with these keys. Once the key issues are dealt with, IPMP-X manager parses the IPMP Message and determine which content streams are protected. After the usage rules are successfully processed, the content is decrypted and the plaintext content buffers are passed to the appropriate decoders and compositor.

In general, this example may require periodic delivery of synchronized cryptographic information. A streaming session may deliver content keys periodically. An IPMP-ES carrying cryptographic information updates and initiates re-keying protocols between the server and the client. IPMP-X system is one appropriate way to meet this requirement. The resulting keys are associated with the content via IPMP-X information. In chapter 5, We will simulate in real world applications, digital TV Conditional Access, DVD copy protection based on IPMP-X framework.

1.6 IPMP Future- MPEG-21 IPMP

The MPEG-21 IPMP will define an interoperable framework for Intellectual Property Management and Protection (IPMP). IPMP became an International Standard supports a well-defined normative framework for managing various DRM system. Now ,all MPEG-4 is still many of them not interworking. This is why MPEG decided to start a new project on more interoperable IPMP systems and tools.

It aims to provide protection in MPEG-21 multimedia framework regardless what format a content is, while ensuring backward compatibility with MPEG-2/4 IPMP framework. MPEG-21 IPMP is expected to leverage on existing MPEG-2/4 IPMP Extensions and trust management is a core issue.It also addresses authentication

of IPMP tools, and has provisions for integrating Rights Expressions according to the Rights Data Dictionary and the Rights Expression Language.