

An Intra-Gateway for Entertainment Contents in Digital Home

Jihyun PARK*, Jeonghyun KIM*, Seongmin KIM*, Dowon NAM*

*Digital Contents Research Division, ETRI(Electronics and Telecommunications Research Institute)

138 Gajongno, Yuseong-gu, Daejeon, 305-700, KOREA

juhyun@etri.re.kr, bonobono@etri.re.kr, morethannow@etri.re.kr, dwnam@etri.re.kr

Abstract—In this paper, we propose an intra-gateway server for the entertainment content in digital home environment and show an implemented prototype system which provides the interoperability among different DRMs, different services, and different content formats. We also define DRM conversion protocol to support the intra-gateway. It is operated on the UPnP protocol, which enables the devices to be used without any modification. The proposed system manipulates DRM applied contents to be played in various devices registered in digital home.

Keywords— digital home, entertainment content, DRM

I. INTRODUCTION

Thanks to development of digital devices and network environment, sharing of contents is occurred frequently at home appliances. But three obstacles are blocking the seamless content sharing in digital home.

The first is incompatibility of various DRMs. Recently, digital content have been protected by several different DRM solutions, which increases users' inconvenience if they have several heterogeneous devices. For example, there may be many kinds of devices in digital home environment, and those devices may have the different DRM in one another. So, content protected by one DRM cannot be consumed by other devices with different DRM due to the lack of DRM interoperability

The second is incompatibility of content service feature. Some contents are provided by streamed manner, and some contents are provided by file downloading. Some devices can consume only the streamed contents while other devices can consume only the downloaded contents. And each consumer device has the limit on the available service. Sometimes service availability depends on the service provider who provides the device. For

example, an IPTV service is available at only the set-top boxes of the designated service provider.

The last is the diversity of content formats and codecs. Almost all the content devices have the limit on content format and codec. It may be significantly diminished if DRM is concerned.

In this paper, we propose an intra-gateway for the entertainment contents in digital home environment and show an implemented prototype system which provides the interoperability for different DRMs, different services, and different content formats. It operated on the UPnP protocol, which enables the devices to be used transparently as the gateway does not exist.

Our prototype system consists of three consumer devices - PC, set-top box, and PMP. And each device has a different DRM in one another. We adopt the different content delivery method among these devices considering device capabilities.

We describe the features of the proposed gateway. It includes content transcode, service adaptation, and DRM adaptation.

II. RELATED WORKS

In this section, we survey techniques for sharing the content in digital home and giving interoperability between devices about the content.

DMP(Digital Media Project) released a comprehensive technology specification for interoperability between DRMs[1]. DRM functions can be decomposed into smaller primitive function, which seem to be implemented into a set of tools called interoperable DRM platform(IDP) toolkit. Unlike MPEG, DMP defines its own DRM formats such as DRM authentication messages, domain

access protocol and so on. Although it seems to be the perfect method that has solved interoperability issues, it has a drawback that it is too difficult for a DRM system to possess the comprehensive architecture proposed by DMP.

Export/Import(EXIM) has solved the interoperability problem by defining a mediate format between DRMs and passing through this mediate format whenever it is necessary to change one DRM content to the other DRM content[2]. That is, one DRM A changes contents of its own DRM format into the defined mediate format using an export module, and then the other DRM B changes this mediate format into content of its own DRM format using an import module. EXIM has a merit that the involved two DRMs do not have to open each DRM architecture and substance. The mediate format should include the comprehensive items in order to be converted into the license architecture of each DRM. But it is difficult to meet the corresponding license materials between two DRMs.

Coral Consortium assumes the existence of a trusted third party(TTP) connected to the network. The TTP provides interoperability by giving translation operations between different formats – protected content formats, rights, and messages[3]. One drawback of this approach is that it requires all involved devices to be connected to the network, at least once when a device is initially connected to the interoperable service provider. Moreover it is difficult to adapt a new DRM to every DRM installed previously whenever it is added into TTP.

Marlin[4] has made DRM tools that can share the content in digital home using domain. A member joined in a domain can use contents registered in the domain without the access of the domain server. Sharing contents is accomplished using link and node structure. But it is difficult to interoperate with other DRM system, and the domain scheme cannot be used for DRMs which has not adopted the Marlin DRM.

III. SYSTEM OVERVIEW

Figure 1 shows one example of the proposed system. Like figure 1, there may be many content consuming devices in digital home. But currently

the DRM applied contents cannot be easily shared among the devices because of the lack of the interoperability of DRM. This causes users' inconvenience. The aim of the proposed system is to enable the sharing of the contents protected by DRM in digital home.

The proposed system integrates DRM systems with home network using the intra-gateway server. It manages home devices through UPnP AV[5], and establishes a domain. It enables content sharing among different DRMs. Consequently, it is possible for various devices in digital home to consume any content in the domain even when DRM of each device is different from others.

DRM conversion is performed through our DRM conversion protocol. The detailed description of the protocol is in section IV.

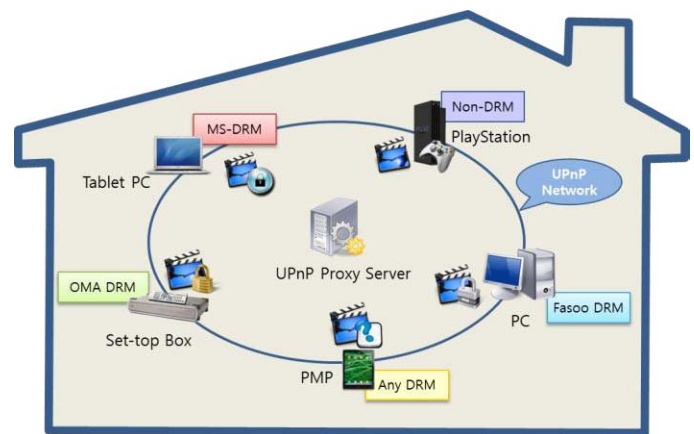


Figure 1. Structure of the prototype system

IV. DRM CONVERSION PROTOCOL

DRM-enabled content cannot be consumed in the same manner as DRM-free content unless all devices in a digital home have the same DRM. Therefore the DRM conversion between the media server and the media renderer is required if DRMs of two devices are different each other. In the proposed system, the DRM conversion conforms to DRM conversion protocol. DRM conversion protocol defines structure and messages which includes the content encryption, metadata, and license.

Our interoperable architecture is composed of two DCAs(DRM Conversion Agents) having would

be transferable content and its related information, and the interworking process like Figure 2.

Basically, the interworking process is a set of procedures in which two DCAs are mutually authenticated, process preparation works for the transmission and transmit interworking data (i.e. content, metadata and usage rights) from DRM A to DRM B through a secure communication channel.

Rules and policies supervise the interworking process. Each DRM has its own rules and policies for the interchange of the content.

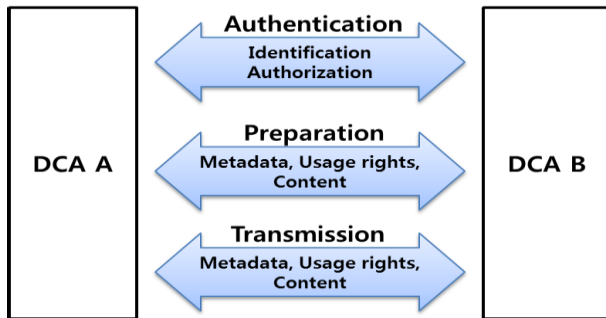


Figure 2. DRM Conversion Protocol

Table 1 shows some important messages of the proposed DRM conversion protocol.

TABLE 1. DRM CONVERSION PROTOCOL MESSAGES

Protocol messages	Description
AuthenticationHelloRequest	Request for starting authentication protocol
AuthenticationHelloResponse	Response for AuthenticationHelloRequest
AuthenticationRequest	Request for authentication process
AuthenticationResponse	Response for AuthenticationRequest
NegotiationRequest	Request for negotiation process for preparation
NegotiationResponse	Response for NegotiationRequest
TransmissionHelloRequest	Request starting transmission protocol
TransmissionHelloResponse	Response for TransmissionRequestHello
IdentificationRequest	Request for identification of requester
IdentificationResponse	Response for IdentificationRequest
TransmissionRequest	Request for starting data transmission
TransmissionResponse	Response for TransmissionRequest

A. Authentication

Each DRM should judge whether the other party is a proper target for achieving DRM interworking. It is a preliminary step before data conversion and transmission, and usually accompanied by the mutual authentication process.

All DCAs are required to be identified by corresponding DRM with unique identifier for later

authorization process on the interworking process. This step includes verifying authenticity of the identifier by cryptographic mechanism. To improve efficiency of the verifying process, some registration function is involved in this step.

Every identified DCA is required to be authorized by corresponding DRM system with the identifier for further interworking process. Even though some DCA is identified and verified properly, it can be rejected in the authorization process if the DCA does not meet the requirements described in the interworking policy. The interworking policy can be managed in forms of whitelist or blacklist.

SSL/TLS[6] or proprietary authentication schemes are able to be used as mutual authentication method. During the authentication process, it is assumed that the X.509 digital certificates of DCA A and DCA B are sent to each other based on the agreed authentication method.

B. Preparation

Each DRM needs to convert content protection scheme, expression way of the metadata and usage rights before these are transmitted. It is a preliminary step before data transmission and usually accompanied by exchanging some information such as usage rights, metadata format, bit rates and resolution on each DRM's preferences.

Content preparation is responsible for converting cryptographic algorithm for content protection. The several pre-defined standard encryption algorithms are able to be considered. If the communication channel for data transmission is protected well, content can be transmitted with plain text. Bits rates or resolution of the content can be changed after exchanging information between two involving DRMs in this step

Usage rights preparation is responsible for converting expression way of usage rights. Some standard or preferred expression ways of usage rights known to both parties are used for converting. Converted usage rights have to maintain the same semantics as defined in the original usage rights.

The standard expression ways are the predefined ones that every DRM have to know. And the preferred expression way can be determined after

exchanging information between two DRMs in this step.

Metadata preparation is responsible for converting expression way of metadata information. Some standard or preferred expression ways of metadata known to both parties are used for converting. Converted metadata has to maintain the same semantics as defined in the original metadata.

Preparation requires a negotiation process to get common exchangeable format and secure channel method. Preparation protocol should be processed right after authentication protocol within same connection session.

C. Transmission

After preparation step, content, metadata and usage rights which are converted form are transmitted from DCA A to DCA B through a secure communication channel. Transmission requires a secure channel to exchange data. Before this protocol is started, a secure channel should be established between DCA A and DCA B based on the result of the negotiation process. This protocol is required to start with the identification process first through the secure connection channel because transmission protocol can be invoked directly without authentication and negotiation process based on previous registered and negotiated information.

V. INTRA GATEWAY SERVER

An UPnP supporting device can consume the contents of the remote devices like its own contents. The control point can recognize media servers and media renderers in home network. A user can browse the list of contents of a media server by selecting the media server on UPnP environment. And then he can consume content at any media renderer device.

If DRMs are involved, DRM conversion should be supported for content sharing. The methods of DRM conversion can be classified into client-centric approaches and server-centric approaches.

In the client-centric approach, DRM conversion is processed at each user device. It is more efficient approach. However, DRM client and DCA must be

installed for DRM conversion. This is not feasible for the mobile devices because the DRM conversion requires high performance hardware.

In the server-centric approach, some DRM conversion server performs the DRM conversion in behalf of each client device. Each DCA must be installed in the DRM conversion server. In this paper, we call it intra-gateway server because our target is the closed UPnP network environment of digital home.

The existing content sharing application based UPnP cannot be used in the server-centric approach because UPnP hardly supports DRM conversion. We add UPnP proxy functions into the intra-gateway server in order to support the content sharing of DRM contents without modifying the UPnP module of each device.

The devices in the proposed prototype system consist of user devices for consuming content, an intra-gateway server, and content providing devices. When the devices are classified by three roles defined in UPnP AV, the user devices have the role of a media renderer and a control point while the intra-gateway server has the role of a control point and a media server. And the contents providing devices has the role of a media server. Figure 3 shows the internal flow of the intra-gateway server.

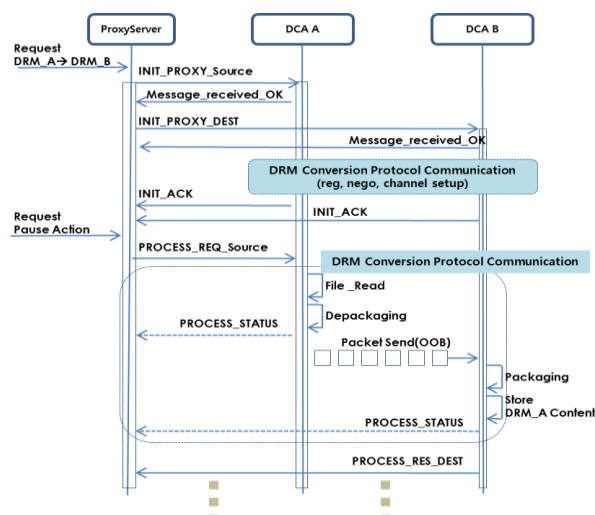


Figure 3. Content Sharing flow with a Proxy server and DCAs

The content sharing steps are as follows:

Step 1 : Every entertainment device in digital home is registered at the intra-gateway server firstly.

Information such as device description and DRM description should be stored before the device is used for consuming contents.

Step 2 : The control point of the intra-gateway collects and cache the information related to media server devices and their content. When the status of device is changed, the control point updates related information.

Step 3 : A content consuming device connects to the intra-gateway server. At this time, it invokes the Browser action of the intra-gateway server. The intra-gateway server checks whether the connected device is registered or not.

Step 4 : A user selects one content. The control point in the user device invokes the SetAVTransportURI action of the media render.

Step 5 : The requested address is substituted with the address of the media server which has the requested content.

Step 6 : The requested content is converted by DCA.

Step 7 : The converted content is sent to the user device.

VI. IMPLEMENTATION

Figure 4 shows a screen-shot of the application for managing the content sharing. The icons in the upper side represent the devices connected in the prototype digital home. The mid-left shows the information of the selected device and DRM. The two windows at the lower-right are source DCA and target DCA.

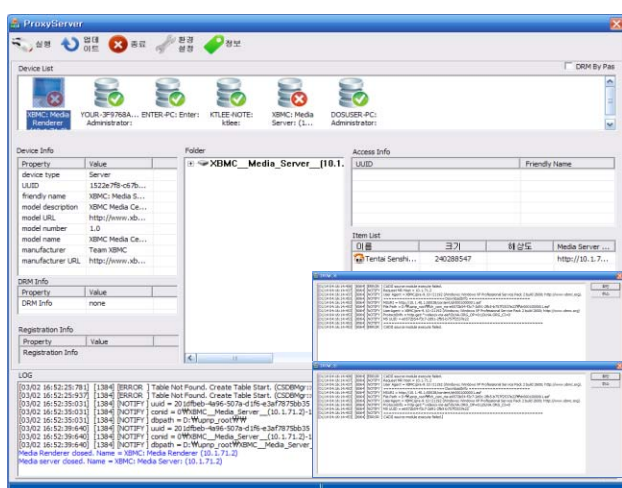


Figure 4. Manager application of the intra-gateway server

VII. CONCLUSION

In this paper, we proposed an intra-gateway for the entertainment contents in digital home environment and showed an implemented prototype system which provides the interoperability for different DRMs, different services, and different content formats. It operated on the UPnP protocol, which enables the devices to be used transparently as same as the gateway does not exist. The proposed system manipulates DRM applied contents to be played in various devices registered in digital home.

For the DRM interoperability, we defined a DRM conversion protocol. DRM conversion protocol defines structure and messages which includes the content encryption, metadata, and license. The interworking process of the proposed protocol is a set of procedures in which two DCAs are mutually authenticated, process preparation works for the transmission and transmit interworking between DRMs through secure communication channel.

We also showed the prototype system consists of three consumer devices – a PC, a set-top box, and a PMP - which have the different DRM in one another. We adopt the different content delivery method among these devices considering the device capabilities.

With the proposed system, inconvenience of the protected contents can be removed, and content protection technologies can be used more widely. As the result, the illegal use of the contents will be decreased.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MCST/KEIT. [10035229, Development of contents protection and distribution technology on DRM-free environments]

REFERENCES

- [1] DMP (Digital Media Project), <http://www.dmpf.org>.
- [2] Yeonjeong Jeong Junghyun Kim Kisong Yoon, "Audio DRM Conversion between Different DRM Content Formats," ICCE 2008, pp. 1-2, Jan. 2008.
- [3] Coral, "Coral Consortium Core Architecture 3.0," <http://www.coral-interop.org>, June 2006.
- [4] MARLIN, <http://www.marlin-community.com/index.html>.
- [5] UPnP, <http://www.upnp.org>
- [6] RFC5246, <http://tools.ietf.org/html/rfc5246>