디지털 방송 서비스를 위한 암호화 툴 전송 시스템

조극양* · 황경민* · 정회경*

The Cryption Tool Transfer System for Digital Broadcasting Service

Ke-Rang Cao* · Kyung-min Hwang* · Hoe-kyung Jung*

요 약

디지털 콘텐츠 시장의 성장은 다양한 콘텐츠 소비 장치의 개발을 유도하였고, 디지털 콘텐츠의 소비를 더욱 촉진시켰다. 그러나 디지털 콘텐츠의 안전한 소비를 위해서는 단말에서의 디지털 콘텐츠 보호를 위한 암호화 툴의 관리가 필요하다. 또한 각 단말의 특성에 적합한 유동적인 암호화 툴 전송 프로토콜이 표준화되지 않아 단말에서의 암호화 툴 관리 상호운용성 부재가 발생한다.

이에 본 논문에서는 디지털 방송 콘텐츠 보호와 소비를 위해 암호화 툴의 전송 프로토콜을 정의하였으며, 이를 기반으로 보호관리 툴 서버와 보호관리 툴 클라이언트를 설계 및 구현하였다.

ABSTRACT

The growth of digital content market inducted to develope consuming device of various content. And through this, digital content consuming is more Promoted. But digital content cryption tool need to handle to protect and consume digital content safely. Also, interoperability of cryption tool management is impossible, because of not standardized transfer protocol between device. In this paper, we defined transfer protocol of cryption tool for protecting and consuming digital content. And in this base, we designed and implemented transfer server/client system.

키워드

MPEG-21, 디지털 방송, IPMP, XML

Ⅰ. 서 론

PC, 셋탑박스 등에서만 소비가 가능했던 디지털 콘텐츠는 최근 각종 단말기기 성능의 발달로 단말에서의 소비가 가능해졌고 이는 광범위한 소비시장 구축을 앞당기고 있다. 그러나 디지털 콘텐츠는 불법 복제를 통해 원본과 동일한 품질의 콘텐츠를 복제 가능하다는 취약점을 가지고 있으며 또한 인터넷을 통한 무분별한 불법 복제 콘텐츠의 유통으로 디지털 콘텐츠 시장의 질서를 어지럽히고 있다. 이를 해결하기 위해 국내외 DRM(Digital Right Management) 개발 업체들은 디지털 콘텐츠를 보호할 수 있는 DRM 툴을 개발하였지만, 제작업체들 간의 DRM 상호운용성이 확보되지 않아 또 다른 문제를 야기하였고 이에 국제 표준화 단체인 MPEG(Moving Picture Experts Group)에서 디지털 콘텐츠 유통을 위한 MPEG-21 표준화를 진행하기에 이르렀다. 그러나 다양한 디지털 콘텐츠의 소비를 위해서는 단말에서의 디지털 콘텐츠 보호를 위한 암호화 툴의 관리가 필요하다. 또한 각

* 배재대학교 컴퓨터공학과 (교신저자 : 정회경)

접수일자 2008. 05. 30

단말의 특성에 적합한 암호화 툴 전송 프로토콜이 표준화되지 않아 상호운용성 부재가 발생한다.

이에 본 논문에서는 단말환경에서 암호화 툴 전송을 위해 암호화 툴의 전송 프로토콜을 XML 메시지로 정의하였으며, 이를 기반으로 보호관리 툴 서버와 보호관리 툴 클라이언트를 설계 및 구현하였다.

Ⅱ. 관련연구

2.1 MPEG-21 Multimedia Frameworks

MPEG에서 진행하고 있는 표준화 전략은 디지털 콘텐츠의 제작에서부터 유통 과정을 통하여 최종 소비자에게까지 전달되는 동안 디지털 콘텐츠를 안전하게 보호 관리하는 기술 표준 제정을 목표로 하고 있다. 이를 위해 MPEG-21 Multimedia Frameworks를 그림 1과 같이 7가지 기본 요소 기술로 구분하여 표준화를 시작하였으며, 현재 18개의 영역에서 표준화 작업이 진행되고 있다[1].

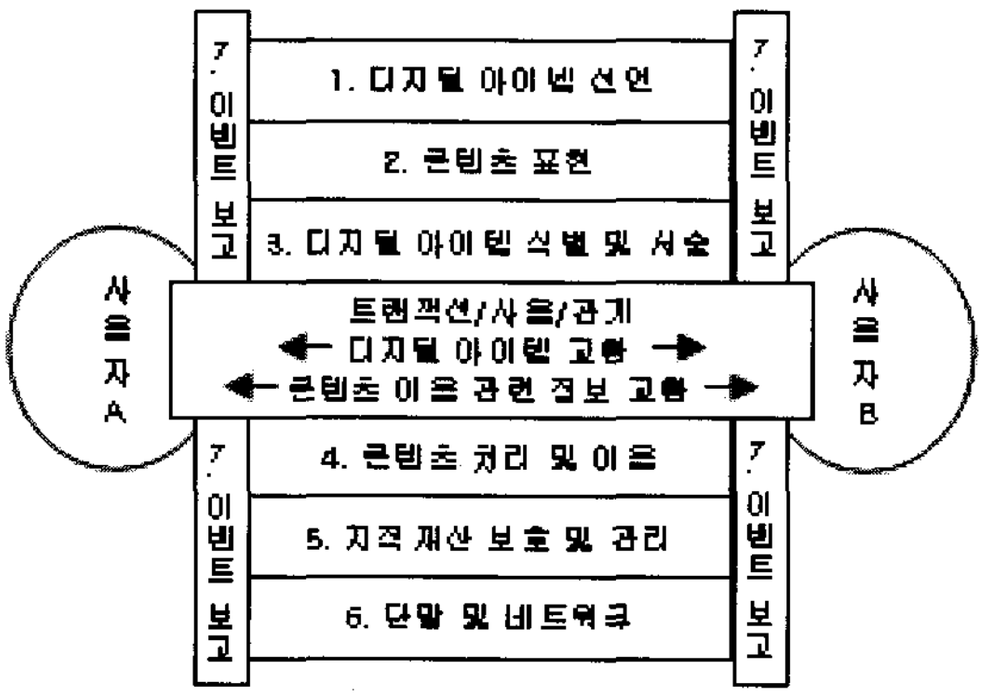

그림 1. MPEG-21 Multimedia Frameworks의 중요 요소 기술 구성도

Fig. 1 Element of MPEG-21 Multimedia Frameworks

2.2 MPEG-21 IPMP(intellectual Property Management and Protection)

이는 MPEG-21 Multimedia Frameworks의 제 4부 규격으로 디지털 아이템이 네트워크 상에서 생성, 변형, 전달, 소비 단계를 거치는 과정에서 디지털 아이템을 안전하게 취급하여 외부의 위험 요소로부터 보호하는 것이다. 그리고 디지털 아이템이 다양한 종류의 네트워크 및 단말기로 처리되는 동안 사용자들에게 저작권과 디지털 아이템에 대하여 동의를 표현하고, 라이프 사이클이 소멸되기 전까지 지속적으로 안전성과, 확신성을 제공한다.

이 분야는 암호화 알고리즘, 키, 키 관리 등의 IPMP 툴의 검색 방법과 툴 간의 메시지 교환 및 툴과 터미널 간의 메시지 교환 방법을 표준화의 대상으로 하고 있다. 특히 IPMP와 관련되어 표준화가 함께 진행되고 있는 세부 분야로는 저작권 표현 언어(REL:Rights Expression Language)와 저작권 사전(RDD : Rights Data Dictionary)이 있다[2,3].

MPEG-21 IPMP Components 스키마 구조는 디지털 아이템 선언의 구조에 따라 보호된 DIDL의 엘리먼트들인 <Component>, <Resource>, <Item> 등과 같이 기존의 DID(Digital Item Declaration) 규격에 IPMP 요소를 포함하는 확장된 개념으로 기술되도록 규격화 하였다.

IPMP DIDL은 Item 엘리먼트로 정의된 디지털 아이템 전체를 포함하며 포함된 디지털 아이템의 보호에 관련된 Info 엘리먼트 정보와 해당 아이템의 식별을 위한 Identifier 엘리먼트 식별자를 제공한다. 이 구조를 기반으로 IPMP DIDL은 DIDL로 구성된 디지털 아이템에 대해 IPMP를 확장하여 표현이 가능하며 이를 통해 디지털 아이템에 대한 보호가 가능하다. DIDL 엘리먼트에서 IPMP 엘리먼트로 확장한 것을 표 1에 나타내었다.

표 1. DIDL에서 확장된 IPMP DIDL 엘리먼트

Table. 1 Extended IPMP DIDL Element From DIDL

DIDL 엘리먼트	IPMP엘리먼트
<Container>	<ipmpdidl:Container>
<Item>	<ipmpdidl:Item>
<Descriptor>	<ipmpdidl:Descriptor>
<Choice>	<ipmpdidl:Choice>
<Condition>	<ipmpdidl:Condition>
<Fragment>	<ipmpdidl:Fragment>
<Selection>	<ipmpdidl:Selection>
<Component>	<ipmpdidl:Component>
<Anchor>	<ipmpdidl:Anchor>
<Resource>	<ipmpdidl:Resource>
<Annotation>	<ipmpdidl:Annotation>
<Assertion>	<ipmpdidl:Assertion>

DID에 IPMP를 확장하는 개념에 해당되는 예를 그림 2에 표현하였다.

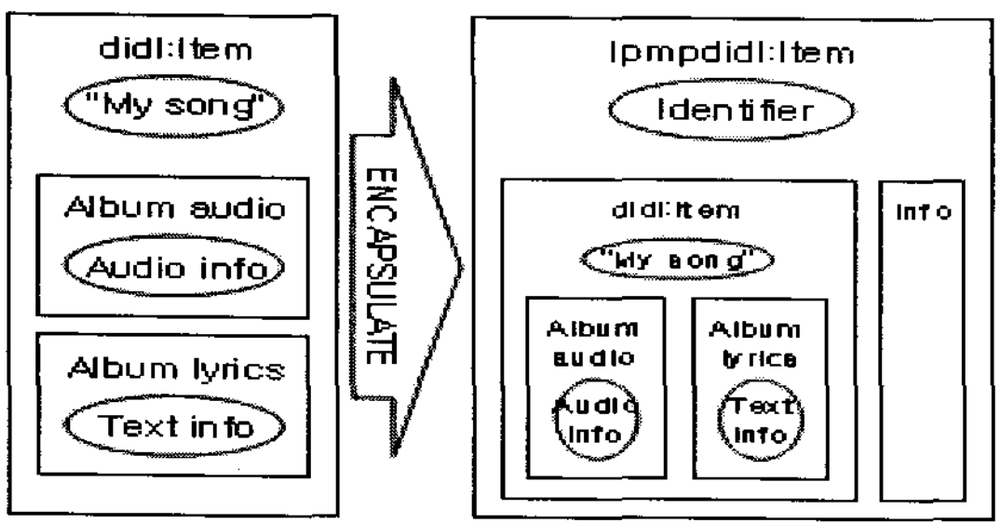

그림 2. IPMP DIDL 프로세싱의 예
Fig. 2 Exam of IPMP DIDL Processing

그림 2의 왼쪽은 오디오 데이터와 가사정보를 포함하고 있는 "My song"이라는 이름을 가진 디지털 아이템을 나타내고 있으며, 오른쪽은 IPMP DIDL을 통해 캡슐화된 모습을 나타내고 있다. 캡슐화된 "My song" 디지털 아이템은 didl 엘리먼트를 표 1에 명시된 ipmpdidl 엘리먼트로 대체하여 표현되며, 기존의 DIDL로 표현된 디지털 아이템 전체를 포함하고 캡슐화에 사용된 정보를 ipmpdidl:ifno 엘리먼트에 명시하여 접근 권한을 보유한 사용자에게 제공된다.

2.3 MPEG-21 REL(Rights Expression Language)

REL은 RDD와 함께 MPEG-21 지적 재산권 관리 및 보호(IPMP)의 세부 요소로 분류된다. REL은 MPEG-21 Multimedia Frameworks 내에서 디지털 콘텐츠 이용, 유통, 관리 및 사용 규칙 등에 관한 표현 언어로 저작권 처리 관련 용어에 대하여 신뢰도 높은 시스템을 제시한다. 또한 표준화된 용어를 제공함으로 타 시스템간의 상호 운용성의 증대 및 유연성과 함께 확장성을 제공하는 것이 목표이다.

REL은 ContentGuard사의 XRML이라는 저작권 언어를 기반으로 XRML 2.0에서 대부분의 정보를 포함하여 확장 및 개발되었다. REL의 스키마는 REL Core, REL Standard Extension, REL Multimedia Extension로 구성된다[4,5,6].

Ⅲ. 암호화 툴 전송 시스템 설계

전체 시스템 아키텍처는 보호관리 툴 서버, 보호관리 툴 클라이언트, 툴 전송 XML 메시지 정의로 구성된다. 보호관리 툴 서버는 암호화 툴을 통합 관리하며 보호관리 툴 클라이언트로부터 툴 전송을 요청 시 해당 툴을 정의된 툴 전송 XML 메시지로 생성하여 보호관리 툴 클라이언트로 메시지를 전송한다. 전체 시스템 아키텍처는 그림 3과 같다.

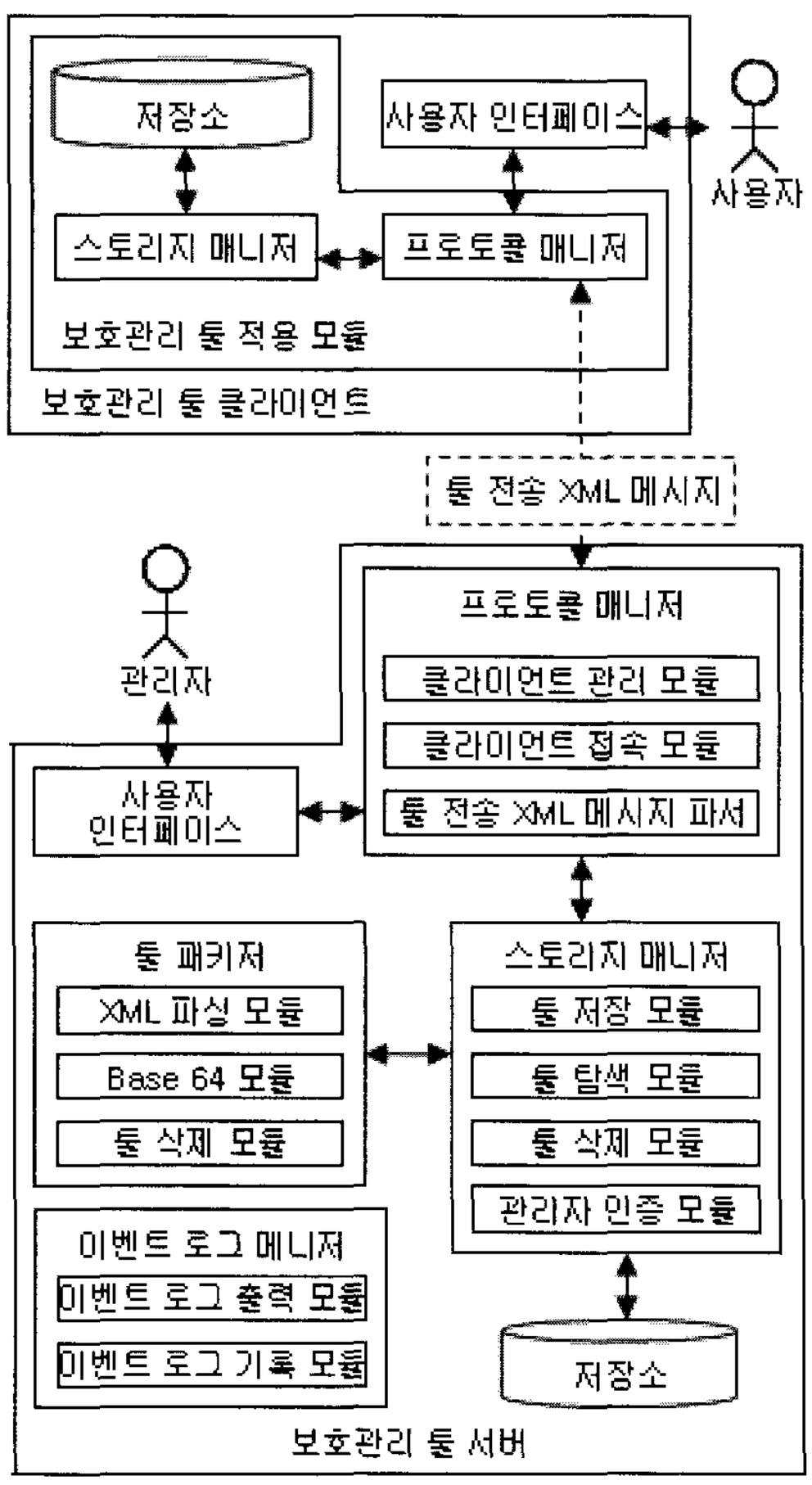

그림 3. 보호관리 툴 전송 서버/클라이언트 전체 아키텍처
Fig. 3 Architecture of Tool Server/Client

3.1 보호관리 툴 서버

보호관리 툴 서버는 관리자로부터 툴을 등록/수정/삭제 등 툴 관리를 위한 인터페이스를 제공하며 보호관리 적용 모듈에서의 툴 요청에 따라 툴을 탐색하여 패키징된 툴을 전송한다.

사용자 인터페이스는 관리자가 직접적으로 서버에 접촉할 수 있는 통로로서 사용자 인터페이스를 통해 관리자는 툴 등록/수정/삭제 등 툴에 대한 관리가 가능하며, 서버 운용을 위한 구동 관련 작업 수행이 가능하다.

프로토콜 매니저는 클라이언트 접속 모듈을 통해 외부의 클라이언트들과의 통신에 관련한 모든 작업을 담당하며 클라이언트 관리 모듈은 접속된 모든 클라이언트들에 대한 접속을 관리한다. 툴 전송 XML 메시지 파서는 접속된 클라이언트로부터 전송되는 모든 메시지를 파싱하여 요청된 작업을 수행한다. 메시지는 현재 서버에 보유된 툴 리스트가 작성된 XML 메시지와 요청된 툴들을 패키징한 XML 메시지로 나뉜다.

툴 패키저는 관리자가 툴 등록 시 툴 전송에 최적화된 상태로 툴을 패키징하는 작업을 수행한다. 이때 바이너리 형태로 저장된 툴은 BASE64 부호화 알고리즘을 통해 부호화된 코드의 형태로 XML 툴 메시지에 삽입되어 저장된다.

스토리지 매니저는 툴 패키저로부터 병합된 XML 메시지를 툴 저장소에 저장하는 역할을 담당하며 이외에 툴에 대한 탐색, 삭제, 그리고 관리자의 접근 인증을 위한 작업을 수행한다. XML 메시지는 툴 저장소에 저장 시 보다 원활한 툴 탐색을 위한 구조로 저장된다.

이벤트 로그 매니저는 서버에서 발생되는 모든 로그 기록을 저장하며 실시간으로 발생된 모든 이벤트를 출력하여 관리자에게 현재 서버의 상태를 통지한다. 이를 통해 관리자는 서버의 상태를 보다 면밀히 알 수 있으며 서버에 이상이 발생 시 신속한 원인 파악이 가능하다.

툴 저장소는 관리자 로그인에 필요한 관리자의 계정과 비밀번호를 저장하고 있으며, 인증된 관리자로부터 등록되는 모든 툴을 보유한다. 외부로부터 툴에 대한 탐색을 요청 받으면 해당 툴ID를 탐색하여 툴을 반환한다. 또한 필요 없다고 판단되는 툴에 대해서는 관리자의 권한으로 삭제가 가능하다.

3.2 보호관리 툴 클라이언트

보호관리 툴 클라이언트는 서버로부터 툴 정보를 수신하여 필요한 툴을 요청 및 다운로드하는 역할을 담당한다. 특히 보호관리 툴 적용 모듈은 프로토콜 매니저 부분으로서 보호관리 툴 서버와의 툴 전송을 위한 툴 전송 XML 메시지를 생성 및 파싱하여 통신하며 내부 설계 구조는 보호관리 툴 서버에서 설계된 프로토콜 매니저와 동일하다.

3.3 툴 전송 XML 메시지 정의

툴 전송 XML 메시지는 보호관리 툴 서버와 툴 적용 모듈 간의 통신에 필요한 메시지를 고려하여 정의하였으며, GetToolList, GetToolListResponse, GetTools, GetToolsResponse 총 4가지로 나누어 정의하였다. 4개의 메시지 정의를 위해 MPEG-21 IPMP 스키마와 MPEG-21 REL 스키마 그리고 W3C XML Digital Signature 스키마를 사용하여 툴 전송 메시지 스키마를 정의하였다. 정의된 메시지의 스키마 상속 관계도는 그림 4와 같다.

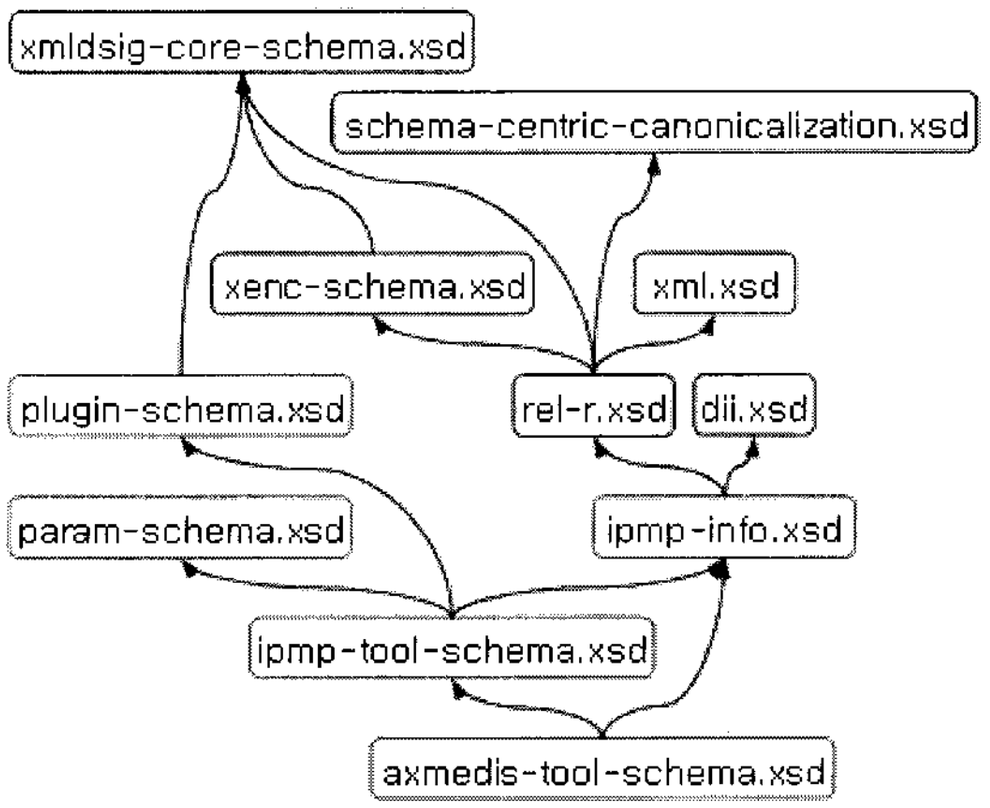

그림 4. 툴 전송 메시지 스키마 상속 관계도

Fig. 4 Diagram of Tool Transfer Message Schema

툴 전송 메시지는 GetToolList 엘리먼트, GetToolListResponse 엘리먼트, GetTools 엘리먼트, GetToolsResponse 엘리먼트 4개로 정의하였으며, 각 엘리먼트에 대한 설명은 표 2와 같다.

표 2. 툴 전송 메시지 엘리먼트
Table. 2 Tool Transfer Message Element

엘리먼트	설명
GetToolList	툴 서버의 보유 툴 목록 확인을 위한 요청 메시지
GetToolList Response	툴 서버에서 GetToolList 메시지에 대한 응답 메시지로서 툴 저장소에 보유중인 툴의 툴ID들의 목록을 리스트로 작성
GetTools	특정 툴의 툴ID를 리스트로 작성하여 툴 서버에 요청하기 위한 메시지
GetToolsResponse	요청 툴ID와 일치하는 툴 패키지를 조합하여 생성

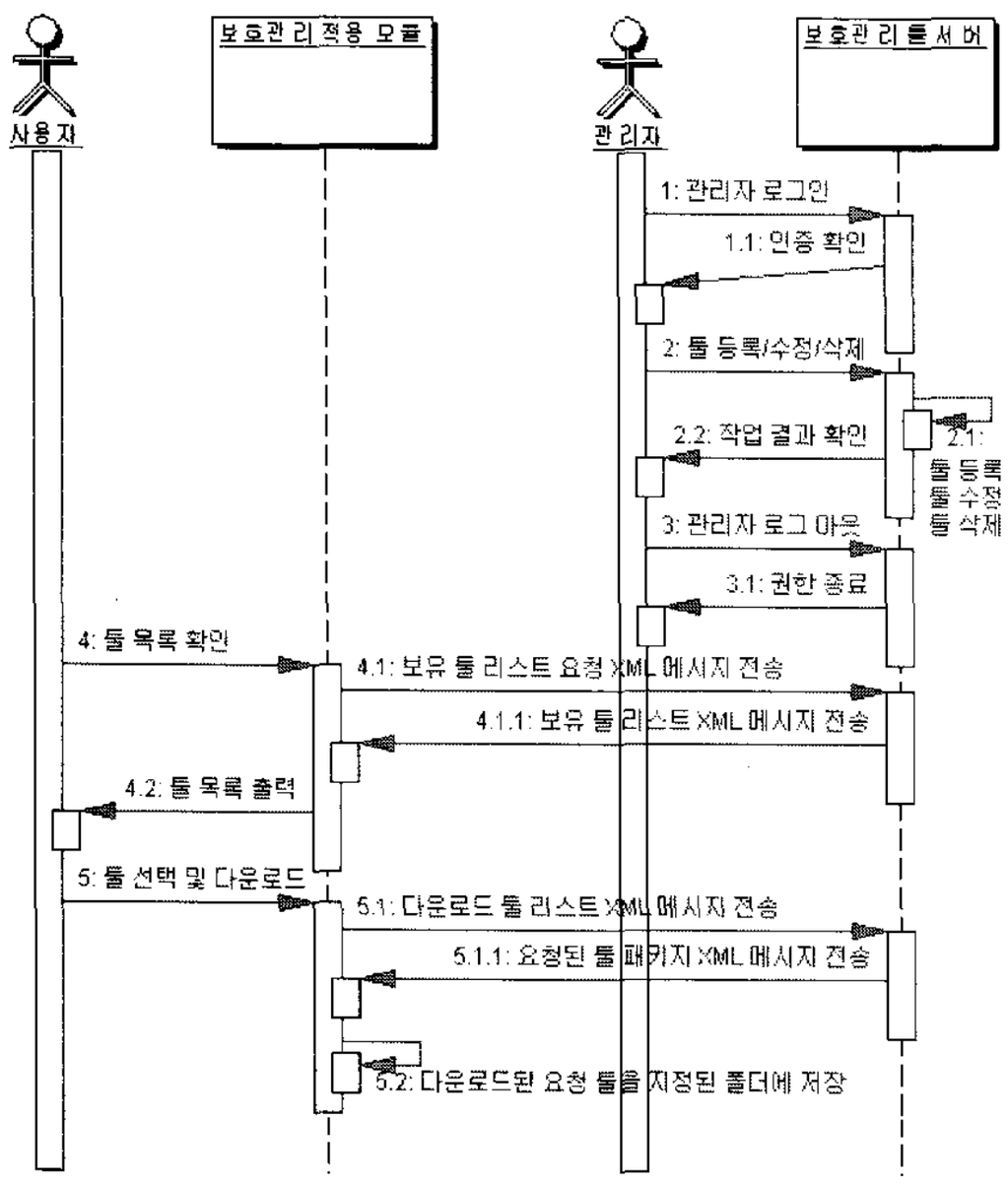

그림 5. 전체 시나리오 시퀀스 다이어그램
Fig. 5 Senario Sequence Diagram

Ⅳ. 암호화 툴 전송 시스템 구현

본 시스템을 구현하기 위해 IBM-PC의 Windows XP 운영체제하에 Visual Studio .NET 2003의 MFC로 개발하였다. XML 파싱을 위해 MSXML 4.0 SDK를 DBMS로는 MySQL을 사용하였다. 보호관리 툴 적용 모듈 및 보호관리 툴 서버의 운용을 위한 전체 시나리오를 시퀀스 다이어그램으로 그림 5에 나타냈다.

4.1 보호관리 툴 서버 인터페이스

보호관리 툴 서버의 인터페이스는 관리자 인증부, 서버 구동 제어부, 툴 관리부, 로그 기록부로 나누어 구성하였다. 구현된 보호관리 툴 서버의 전체 구성은 그림 6과 같다.

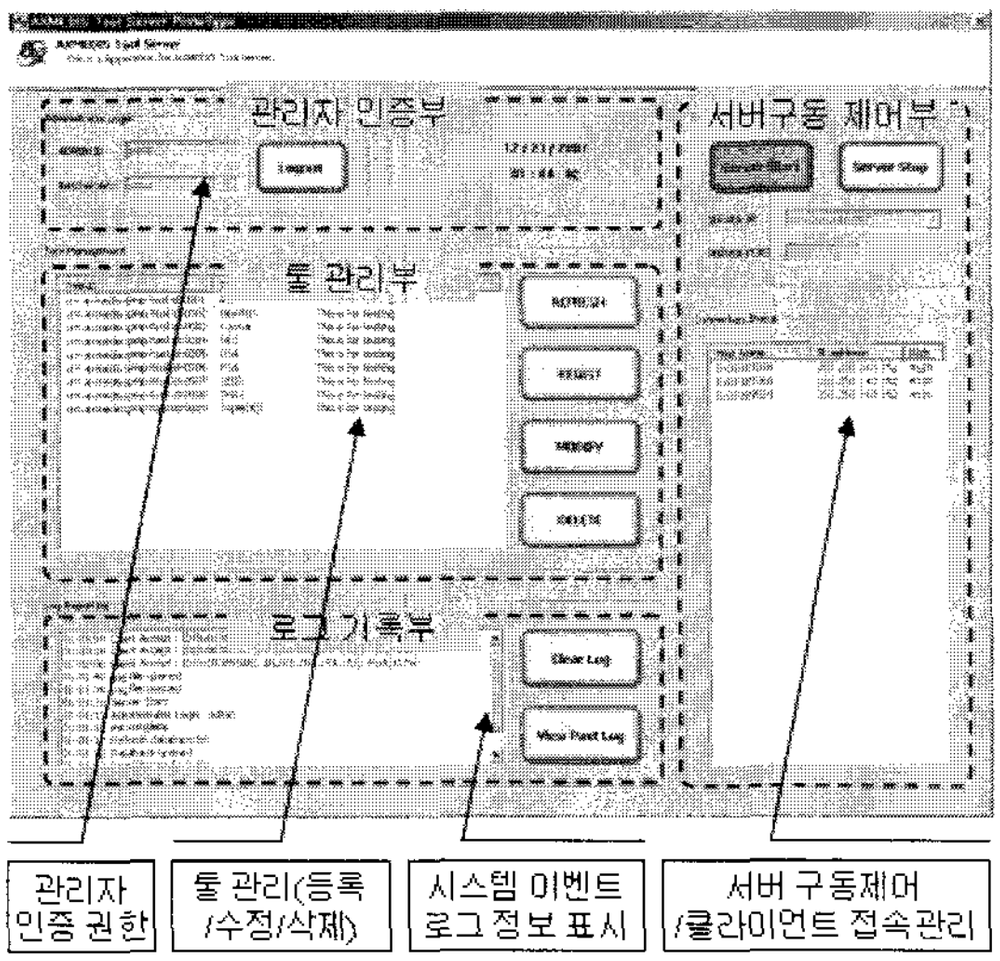

그림 6. 보호관리 툴 서버 인터페이스
Fig. 6 Interface of Tool Server

관리자 인증부는 관리자가 툴을 등록/수정/삭제 등의 툴 관리를 위한 인터페이스를 제공하기에 앞서 관리자의 권한을 가지고 있는지 인증과정을 수행하기 위한 인터페이스이다.

서버 구동 제어부는 보호관리 툴 서버의 구동관련 작업을 제어할 수 있는 인터페이스를 제공한다. 기본적으로 서버를 구동하기 위해 "Server Start"버튼과 "Server Stop"버튼을 구성하였다. 또한 서버의 특성상 다수의 네트워크 카드를 사용할 가능성을 고려하여 다중 IP주소를 지원 가능하도록 콤보박스를 사용하여 Server IP를 선택 가능하도록 하였다. 툴 관리부는 권한 인증을 통과한 관리자에게 툴을 등록/수정/삭제하기 위한 인터페이스를 제공한다.

로그 기록부는 서버에서 발생하는 모든 이벤트 기록을 관리자에게 통지할 수 있다.

4.2 보호관리 툴 클라이언트 인터페이스

구현된 보호관리 적용 모듈을 적용하기 위해 보호관리 적용 모듈 클라이언트를 구현하였으며 서버와의 **XML**메시지 전송을 담당하도록 하였다. 구현된 보호관리 적용 모듈 클라이언트는 그림 7과 같다.

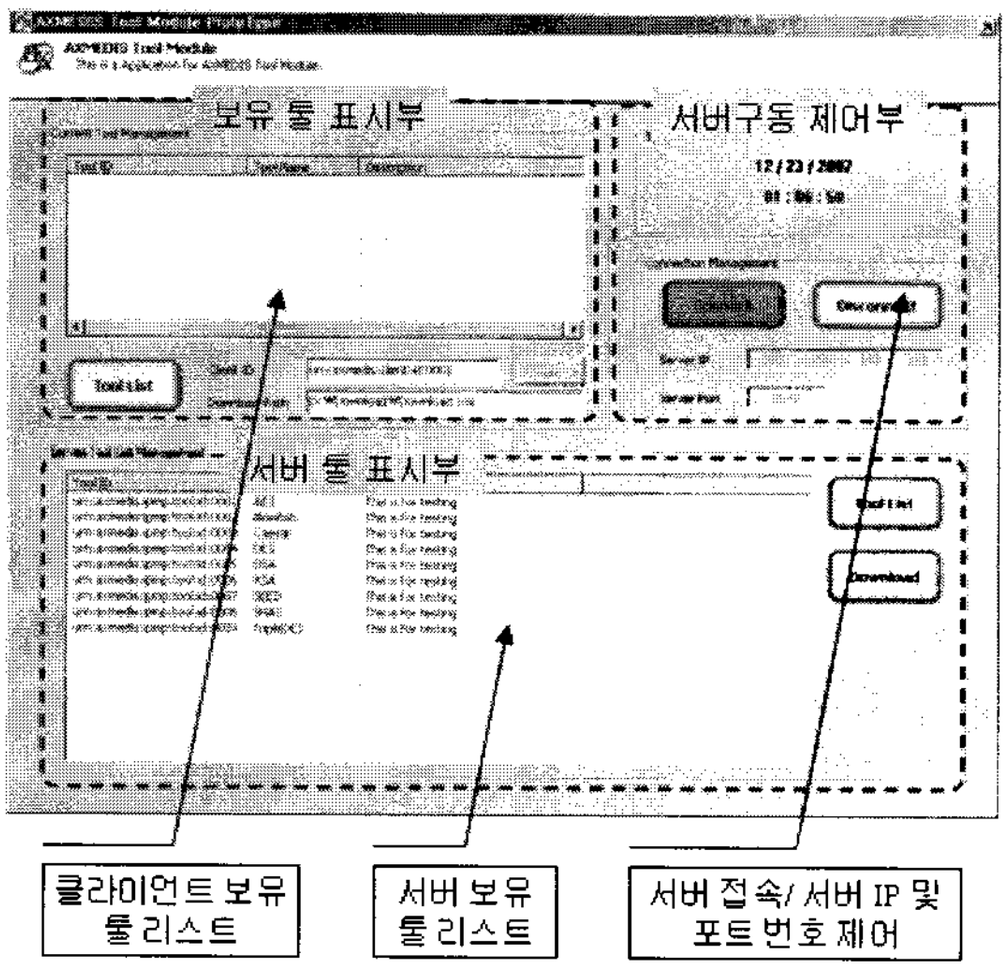

그림 7 보호관리 툴 클라이언트 인터페이스
Fig. 7 Interface of Tool Client

보유 툴 리스트는 사용자에게 현재 보유중인 툴의 정보를 출력하기 위한 인터페이스이다. 사용자는 해당 인터페이스를 통해 보호관리 툴의 보유 현황을 알 수 있으며, 서버와의 접속 시 서버에 클라이언트의 고유 **ID**를 통보하기 위한 클라이언트 **ID**입력창과 툴 다운로드 시 저장될 경로를 지정하는 **"Download Path"** 입력창으로 구성되어 있다. 서버 접속부는 서버에 접속하기 위한 인터페이스를 제공한다. 서버 툴 표시부는 서버에서 보유중인 보호관리 툴의 목록을 출력하며 이를 선택하여 다운로드를 가능하게 하는 인터페이스이다. 이 인터페이스는 서버에서 GetToolsListResponse 메시지를 수신하여 처리되는 서버 보유 툴 **ID**와 기본적인 정보를 출력한다.

전송된 툴 메시지는 ToolPackage 루트 엘리먼트와 두 개의 Tool 엘리먼트와 ToolFile 엘리먼트로 구성되어 있다. Tool 엘리먼트는 보호관리 툴의 이름과 간략한 설명 그리고 툴 사용을 위한 파라미터 값과 유형을 명시한다. ToolFile 엘리먼트는 보호관리 툴의 파일 이름과 크기 그리고 툴 바이너리 파일을 base64 부호화하여 제공한다. 클라이언트는 이 메시지를 통해 보호관리 툴 바이너리 파일과 툴에 대한 정보 그리고 툴 사용법을 추출 가능하다. 보호관리 툴 서버에서 보호관리 툴 클라이언트로 전송된 툴 메시지의 결과를 그림 8에 나타내었다.

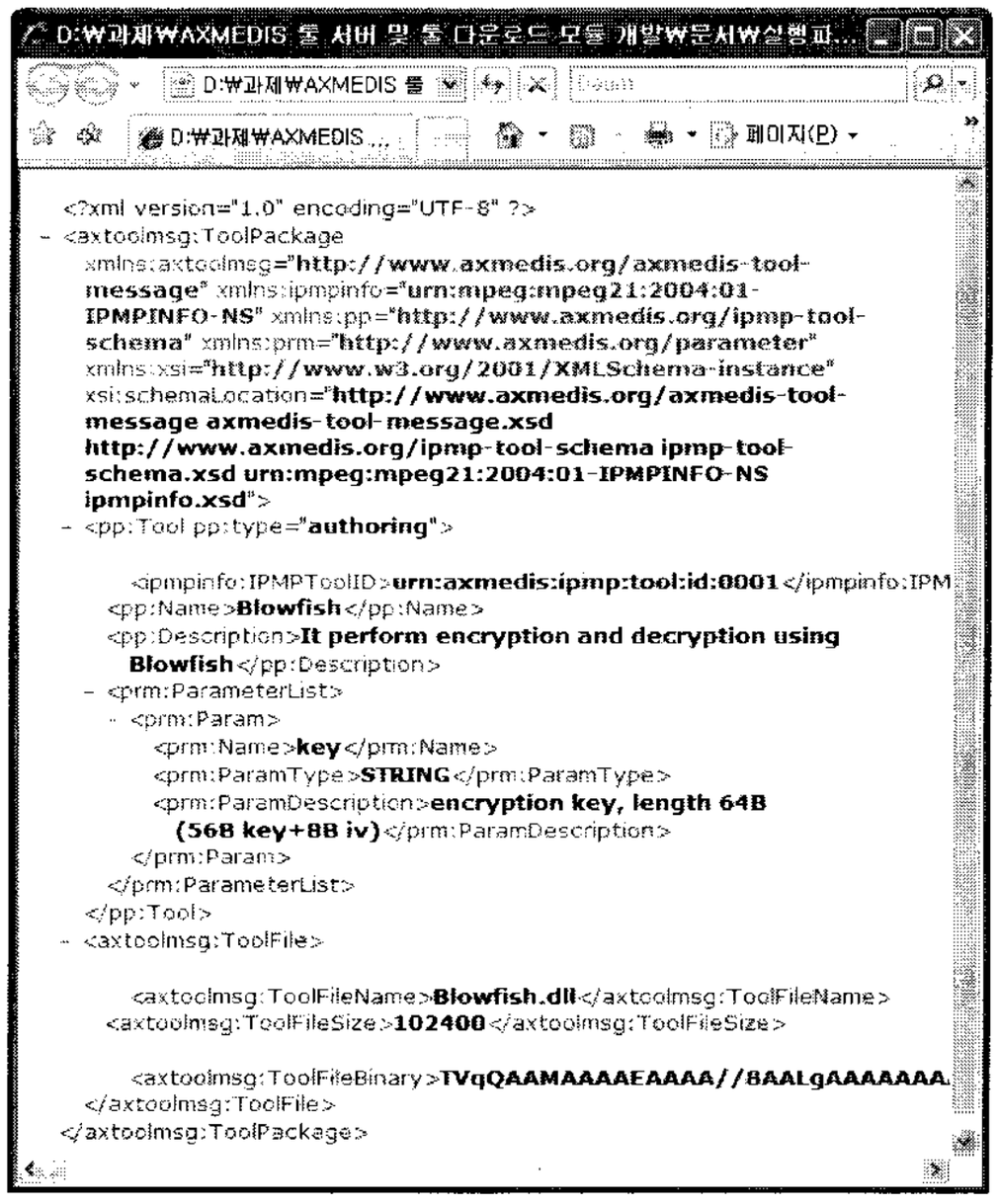

그림 8. 수신된 툴 메시지
FIG. 8 Transfered Tool Message

V. 고찰 및 결론

본 논문은 단말 상에서 디지털 콘텐츠 보호관리 모듈 적용 및 상호운용성 확보를 위한 것으로써 툴 전송 **XML** 메시지를 정의 및 이를 적용한 디지털 콘텐츠 보호관리 적용 모듈과 보호관리 툴 서버 참조 모델을 설계 및 구현하였다.

기존의 보호관리 모듈은 단말 외부에서 독자적인 프로토콜을 통해 적용되는 한계를 가지고 있어 단말상에서의 보호관리 모듈의 효율적이고 상호운용 가능한 툴의 관리에 취약점을 가지고 있다. 이러한 문제를 해결하기 위해 단말의 보호관리 적용 모듈과 보호관리 툴 서버 간의 상호운용 가능한 메시지 표준을 정의할 필요가 있다. 이는 모든 보호관리 툴의 전송이 표준을 준수하도록

유도하며, 툴 전송 XML 메시지를 통해 프로토콜의 제약 없이 다양한 보호관리 툴의 전송이 가능하다.

이에 본 논문에서는 상호운용 가능한 보호관리 툴 전송 XML 메시지 정의를 위해 국제 표준단체인 MPEG에서 정의한 MPEG-21 IPMP, REL, DII(Digital Item Identification) 스키마 구조를 상속받아 메시지를 정의하였으며, 이를 통해 이기종 단말간의 모든 보호관리 툴 전송 상호운용성을 확보하였다. 또한 보호관리 툴 바이너리를 Base64 부호화한 후, XML 메시지화하여 프로토콜에 대한 제약없이 보호관리 툴의 전송이 가능하며 방화벽의 제약으로부터 자유롭다.

본 논문를 통해 이기종 단말과 보호관리 툴 서버간의 보호관리 툴 전송 상호운용성이 확보될 것으로 기대되며 또한 단말기기에 운용 가능한 보호관리 툴의 개발 및 적용을 통해 단말에서의 디지털 콘텐츠 보호 개념이 확장될 것으로 사료된다. 이는 디지털 콘텐츠 시장의 콘텐츠 제공자, 유통자, 소비자의 권익 보호와 양질의 디지털 콘텐츠 생산 기회의 증가를 유도할 것이다.

향후 연구로는 단말간 보호관리 툴 전송을 위한 참조 모델을 제시하여 이기종간의 상호운용뿐 아니라 개발 시에도 혼용하여 사용할 수 있는 크로스 컴파일을 위한 모듈 개발이 필요하다.

참고문헌

[1] 김해광,"MEPG-21 멀티미디어 프레임워크", 한국정보통신기술협회, TTA 저널통권82호, 2003

[2] Rob Koenen, "IPMP in MPEG Standards.", Workshop on DRM for the Web, W3C, INRIA - Sophia Antipolis, France, 22-23. Jan. 2001.

[3] MPEG, "ISO/IEC 21000-4 FCD IPMP Compo- nents", ISO/IEC/JTC1/SG29/WG11/N7196, MPEG MDS Group, April 2005.

[4] MPEG, "REL", ISO-IEC_21000-5_(E)_FDIS

[5] MPEG, "RDD", ISO-IEC JTCl_SC29_M10574

[6] W3C, "eXtensible Markup Language 1.0", http://www.w3.org/TR/REC-xml

[7] AXMEDIS, "Specification of General Aspects of AXMEDIS framework, first update of DE3.1.2 part A", 2006.4.15

[8] AXMEDIS, "Specification of AXMEDIS Object Manager and Protection Processor, first update of DE3.1.2 part B", 2006.5.8

저자소개

조극양(Ke-Rang Cao)

2000년 동북대학교 컴퓨터과학 기술학과(공학사)
2005년 배재대학교 컴퓨터공학과 (공학석사)
2008년~현재 배재대학교 컴퓨터공학과 박사과정
※관심분야 : 유비쿼터스 센서 네트워크, 멀티미디어, IPTV

황경민(Kyung-Min Hwang)

2006년 배재대학교 컴퓨터공학과 (공학사)
2006년~현재 배재대학교 컴퓨터공학과 석사과정
※관심분야 : XML, MPEG-2, XML-Signature, MPEG-21, IPTV

정회경(Hoe-Kyung Jung)

1985년 광운대학교 컴퓨터공학과 (공학사)
1987년 광운대학교 컴퓨터공학과 (공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년~현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, XML, SVG, Web Services, Semantic Web, MPEG-21, 유비쿼터스 센서 네트워크, IPTV