

MPEG-2/4 IPMPX 기술동향

An Analysis of MPEG-2/4 IPMPX with Consideration of Interoperable DRM Platform

최범석(B.S. Choi)
홍진우(J.W. Hong)

방송콘텐츠연구팀 연구원
방송콘텐츠연구팀 책임연구원, 팀장

최근 디지털 콘텐츠 산업에서의 저작권 보호 시스템에 대한 중요성이 강조되면서 상호 연동 가능한 DRM에 대한 연구가 활발히 진행되고 있다. MPEG-2/4 IPMPX는 이러한 요구조건을 만족시키기 위하여 시작된 대표적인 국제표준으로 현재 그 규격이 완성단계에 있다. 본 고에서는 기존의 폐쇄 프레임워크형 DRM 시스템 구조에서 탈피하여 개방 프레임워크형 기반의 DRM 플랫폼을 제시한 MPEG-2/4 IPMPX의 기술 내용과 구현사례에 대하여 살펴보고 앞으로 해결해야 할 문제점을 제시하였다. 또한 관련 기술동향에 대하여도 간단히 언급하였다.

I. 서론

아날로그 형태의 콘텐츠가 디지털화 되면서 저작권에 대한 심각한 문제가 대두되게 되었다. 이는 디지털 콘텐츠는 아날로그 콘텐츠와 달리 원본과 다름 없는 형태로 무한 복제와 재생이 가능하고, 대용량 매체와 인터넷이 범용화 되면서 디지털 콘텐츠가 순식간에 배포될 수 있기 때문이다. 이러한 환경은 디지털 콘텐츠 산업의 활성화를 가져올 수 있는 기반이 되지만, 현재의 디지털 콘텐츠 소비 문화는 양성적이라기 보다는 음성적인 면이 강하다고 할 수 있다. 즉 콘텐츠 플레이용 디바이스, 콘텐츠 저장용 디바이스, 콘텐츠 배포망 등이 저작권 보호에 대한 고려 없이 발전하면서 불법적인 콘텐츠 소비와 배포가 성행하게 되었다. 물론 디지털 콘텐츠에 대한 저작권 보호관리에 대한 노력이 아예 없었던 것은 아니었다. DRM(Digital Rights Management) 기술이라고 알려진 디지털 콘텐츠 저작권 보호관리 기술이 계속적으로 발전되고 있으며, 이 중 일부 기술들이 현재 유료 디지털 콘텐츠 서비스에 적용되어 사용되고 있다. 이러한 DRM 기술에는 다양한 암호화 알고리즘, 워터마킹 알고리즘, 인증 기술, 라이선스 생성 및 관리 기술, 콘텐츠 패키징 기술 등이 적용되고 있

으며 콘텐츠 생성 및 소비 시스템에 접목되어 적절한 저작권 보호 및 유통이 일어나도록 돕는다. 이러한 시스템을 일반적으로 DRM 시스템이라 한다.

기존의 DRM 시스템은 콘텐츠를 서비스하고자 하는 콘텐츠 제공자의 필요에 따라 자체적으로 개발되었다. 또한 DRM 시스템의 특성상 시스템에 대한 보안이 가장 중요하였으므로, 이에 대한 기술적인 공부가 어려운 것이 사실이었다. 따라서 특정 콘텐츠 제공자의 서비스를 받기 위해서는 해당 서비스업체에서 제공하는 고유한 플레이어(또는 DRM 시스템)를 사용자 단말에 설치해야 했다. 현재 다양한 콘텐츠 서비스 제공업체가 생겨나고 있으며 각 서비스 제공자들이 적용하는 DRM 시스템의 고유성 때문에 사용자들은 각각의 DRM 시스템이 적용된 여러 가지 플레이어를 사용자 단말에 설치해야 하는 번거로움이 있다. 단말 제조업체 측면에서 이러한 문제는 다양한 포맷의 콘텐츠를 소비할 수 있도록 하기 위한 하드웨어 및 소프트웨어적인 구조를 정하는 데 어려움을 주며 이에 따른 단말 제조 단가를 높게 만든다. 콘텐츠 서비스 제공업체 측면에서는 사용자 단말의 성능적·구조적 한계를 고려해야 하므로 원하는 DRM 기술을 마음대로 적용할 수 없는 문제가 생긴다. 결과적으로 이러한 DRM 시스템 사이의 호

환성 부재는 디지털 콘텐츠 산업을 활성화하는 데 있어서의 큰 장애물로 작용하게 된다.

MPEG(Motion Picture Experts Group) 국제 표준화 기구에서는 MPEG-2 및 MPEG-4 포맷의 콘텐츠에 대한 콘텐츠 보호 시스템 프레임워크를 정의하고 있으며, 이를 각각 MPEG-2 IPMPX(Intellectual Property Management and Protection Extension)와 MPEG-4 IPMPX라고 한다. MPEG-2/4 IPMPX에서는 각각의 DRM 기술들(인증, 암호화, 워터마킹 등)을 개별적인 툴(tool) 개념으로 보고 있으며 본 표준의 가장 큰 목적이 바로 다양한 보호 툴들을 하나의 단말에서 적용하여 사용할 수 있는 “Interoperable DRM Platform”을 정의하는 데 있다. 본 논문에서는 MPEG-2/4 IPMPX 표준 기술에 대하여 먼저 살펴보고 이와 관련된 연구 동향에 대하여 언급하도록 한다. 또한 MPEG-2/4 IPMPX를 산업에 적용하기 위하여 보완해야 할 점에 대하여 살펴보고 또한 이와 맥락을 같이하는 다른 국제 표준들에 대하여 간략히 소개한 후 이 글을 끝맺도록 한다.

II. MPEG IPMPX의 배경

MPEG IPMPX는 다양한 DRM 기술들이 단말에서 함께 적용될 수 있는 “훅(hook)”을 제공하는 개념에서 시작되었다. 이러한 “훅”을 통하여 DRM 시스템과 단말 사이에 통신이 일어나며 이를 통하여 DRM 시스템의 갱신, 안전한 통신 채널설정, 인증 등이 이루어질 수 있도록 하는 것이 기본 개념이었다[1]. MPEG IPMPX 개념은 가장 먼저 객체기반 디지털 콘텐츠 규격인 MPEG-4에 적용되었으며, 이어서 디지털 방송용 포맷인 MPEG-2 시스템에도 적용되게 되었다. 현재 새롭게 표준화가 진행되고 있는 MPEG-21에서도 역시 IPMP가 정의되고 있다. MPEG-2 IPMPX 규격은 “MPEG-2 System Amendment”와 “part 11”에 정의되어 있으며[2], MPEG-4 IPMPX 규격은 “MPEG-4 System Amendment”와 “part 13”에 정의되어 있다[3].

MPEG-2 IPMPX 규격과 MPEG-4 IPMPX 규격은 각각 2003년 3월과 2002년 10월에 FDIS로 승인된 상태이며, 2004년 3월부터 현재까지 두 시스템 규격에 따른 참조 소프트웨어에 대한 규격 테스트가 이루어지고 있다.

III. MPEG-2/4 IPMPX의 특징

MPEG-2/4 IPMPX의 가장 큰 목적은 앞서 서론에서도 언급했듯이 이기종의 DRM 시스템에 대한 상호운용성을 지원하는 시스템 플랫폼을 정의하는 것에 있다고 할 수 있다. MPEG-2/4 IPMPX에서 규정하고 있는 상호운용성에 대한 요구사항은 최종 사용자 입장에서의 요구사항과 단말 제조업자 입장에서의 요구사항으로 나뉜다. 최종 사용자 입장에서의 상호운용성이란 사용자가 소유하고 있는 단말의 종류에 상관없이 어떠한 콘텐츠 제공업자로부터 서비스된 콘텐츠라도 모두 소비될 수 있는 환경을 제공해야 함을 의미한다. 단말 제조업자 입장에서의 상호운용성이란 제조업자가 만든 단말이 어떠한 콘텐츠 시장에서도 적용되어 사용되어질 수 있어야 함을 의미한다. 즉 콘텐츠 제공업자가 자신이 서비스하는 콘텐츠에 적용한 DRM 기술에 대하여 단말은 그 구조상 수정되거나 추가되는 디바이스 없이 이를 모두 플레이 할 수 있는 플랫폼을 요구하고 있는 것이다. 이를 위하여 MPEG-2/4 IPMPX 표준에서는 다음의 몇 가지 사항을 규격으로 정의하고 있다.

1. 툴 리스트

기존의 DRM 기술에서 사용되어온 기본적인 기능 단위 모듈을 MPEG-2/4 IPMPX에서는 개개의 IPMP 툴로 간주한다. 즉 전체 DRM 시스템에 사용된 기능단위 모듈을 컴포넌트화하여 언제든지 필요하면 추가하고 반대로 필요치 않게 되면 제외시킬 수 있도록 한다. 이를 가능하게 하기 위해서는 각 IPMP 툴들을 식별할 수 있도록 하는 툴 ID가 필요하게 되는데, MPEG-2/4 IPMPX에서 IPMP 툴들이 시스템에 적용되어 사용되기 위해서는 먼저 공식적

인 툴 ID를 할당 받는 것을 기본 가정으로 하고 있다. 이러한 툴 ID 정보를 통하여 단말에서는 콘텐츠에 적용된 IPMP 툴들이 무엇인지 알고 필요한 IPMP 툴을 호출할 수가 있는 것이다. MPEG-2/4 IPMPX 규격에서는 이러한 정보를 툴 리스트(tool list)라는 구조로 정의하여 콘텐츠와 함께 배포되도록 정의하고 있다. 예를 들어 툴 ID가 01인 암호화 툴과 툴 ID가 02인 워터마킹 툴이 적용된 콘텐츠가 사용자 단말에 입력된다면, 단말은 제일 먼저 툴 리스트를 파악하여 이 콘텐츠를 플레이하기 위해 필요한 두 개의 IPMP 툴을 호출할 수 있는 것이다. 이러한 툴 리스트 구조 안에는 툴 ID 정보뿐만 아니라 특정 IPMP 툴이 단말에 존재하지 않을 경우 대체가 가능한 툴(alternative tool)을 기술할 수도 있고, 파라미터로 기능을 달리하는 툴(parametric tool)에 대한 정보를 기술할 수도 있다. 만일 적절한 툴이 단말에 존재하지 않을 경우 툴 스트림(stream)을 MPEG IPMPX 규격에서 정의하는 툴 컨테이너(container) 구조에 삽입하여 콘텐츠 스트림과 함께 전송할 수도 있다.

2. IPMP 디스크립터

IPMP 디스크립터(descriptor)는 보호가 필요한 오디오 스트림 또는 비디오 스트림에 대한 제어 구조를 정의한다. 즉 특정 IPMP 툴이 어떠한 제어점(control point)에 연결되어야 하며 해당 제어점에서의 우선순위는 어떤지를 기술하게 된다. 여기서 제어점이란 콘텐츠가 단말에 입력된 후 스크린이나 스피커를 통하여 최종 출력되기까지 거쳐야 하는 과정 중 다양한 IPMP 툴에 의하여 제어가 가능한 지점을 가리킨다. 하나 이상의 툴이 같은 제어점에서 동작할 수도 있기 때문에 우선순위를 기술하여 같은 제어점에서 적용될 툴의 순서를 정해 놓는다. MPEG-2/4 IPMPX 규격에서는 단말구조 상에 존재할 수 있는 여러 가지 제어점을 규정해 놓고 있다. 또한 툴을 작동시키기 위해서 필요한 초기화 정보 역시 IPMP 디스크립터 상에 기술된다. 따라서 툴 리스트를 통하여 호출된 툴은 IPMP 디스크립터에

기술된 정보에 의하여 적절한 제어점에 연결되며, 툴 초기화 정보에 의하여 작동될 준비를 마치게 된다.

3. 메시지 체계

다양한 IPMP 툴들이 하나의 단말에서 함께 동작하기 위해서는 툴과 툴 사이 또는 툴과 단말 사이에 의사소통이 필요하다. MPEG-2/4 IPMPX에서는 툴과 단말 사이에 주고 받는 모든 데이터들이 메시지를 통하여 이루어진다. 예를 들어, 단말이 툴 초기화 정보를 IPMP 디스크립터로부터 추출하여 특정 툴에 전달하거나 툴간에 상호인증을 수행할 때에도 메시지를 사용하며, 툴과 툴 사이 콘텐츠 스트림을 서로 주고 받을 때에도 메시지를 사용한다. MPEG-2/4 IPMPX가 이러한 메시지 구조를 갖는 이유는 다음과 같다. 첫째, 필요에 따라 시스템의 구조적인 수정 없이 추가적인 메시지를 생성하므로 새로운 애플리케이션에 적용할 수 있다. 둘째, 파라미터 형태의 정보 전달보다 메시지 형태의 정보 전달을 사용하게 되면 전달되는 정보에 대한 보안이 좀더 쉽기 때문이다. MPEG-2/4 IPMPX 규격은 필요에 따라 사용할 수 있는 다양한 메시지 구조와 타입을 정의해 놓고 있으며, 크게 비트 스트림 형태로 전달되는 IPMP 정보를 전달하기 위한 메시지들과 단말과 툴에서 생성된 정보를 전달하기 위한 메시지들로 나뉜다. 이러한 메시지 규격은 기본적으로 메시지를 보내는 엔티티의 ID와 메시지를 받는 엔티티의 ID를 기술하도록 되어 있다. 즉 보낸 메시지를 중간에서 받아서 적절한 목적지로 보내주는 역할이 필요한데 MPEG-2/4 IPMPX에서 이러한 역할을 하는 엔티티를 메시지 라우터(message router)라 지칭한다.

4. 인증 체계

폐쇄 프레임워크 기반인 기존의 DRM 시스템에서는 시스템 자체에 대한 보안을 중요시 하였기 때문에 시스템 내부 컴포넌트 사이의 인증이 중요하지 않았다. 다만 단말 DRM 시스템과 서버 DRM 시스템과 같이 서로 떨어져 있는 컴포넌트 간에만 신뢰

할 수 있는 채널을 설정하기 위한 인증과정이 필요했다. 그러나 MPEG-2/4 IPMPX는 개방 프레임 워크 기반으로, 플러그-인 형태의 IPMP 툴 각각이 보안이 필요한 중요한 정보를 파싱(parsing)하거나 보호되지 않은 형태의 미디어 데이터를 처리하기 때문에 실제적인 툴의 동작에 앞서 해당 툴이 신뢰할 수 있는 툴인지를 판가름하는 툴에 대한 인증과정이 중요해진다. 일반적으로 인증과정은 서로의 전자 인증서를 교환하여 유효성을 확인하는 방식으로 이루어지며, 상대방에 대한 확인이 끝난 후에는 통신을 위한 보안레벨(integrity protected communication, full secure, authenticated communication)을 결정하게 된다. 이러한 보안레벨은 일반적으로 콘텐츠 제공자에 의하여 미리 미디어 비트스트림 안에 정의된 정보에 의하여 결정된다. 예를 들어, 하나의 미디어 스트림이 하나 이상의 IPMP 툴에 의하여 보호가 되어 우선순위가 가장 높은 툴이 우선순위가 낮은 툴을 작동시키는 경우에, 우선순위가 높은 툴은 IPMP_initMutualAuthentication 메시지를 사용하여 통신이 필요한 엔티티를 서로에게 알리고 상호간에 사용할 보안레벨을 결정하게 된다. 다음으로 IPMP_MutualAuthentication 메시지를 사용하여 안전한 채널을 설정하게 된다. 상호인증을 통하여 안전한 통신 채널이 만들어졌다면, IPMP_Secure Container 메시지를 이용하여 정보를 안전한 형태로 패키징하여 보내게 된다.

5. 툴 다운로드

만일 콘텐츠에 적용된 IPMP 툴이 단말에 존재하지 않을 경우 두 가지 방법으로 필요한 툴을 습득할 수 있는데, 첫번째 방법은 툴 컨테이너 구조를 사용하여 콘텐츠와 함께 툴을 전달하는 방법이 있고, 두번째 방법은 툴 리스트에 기술된 툴 ID를 사용하여 리모트 서버(또는 이웃하는 IPMP 디바이스)에 해당 툴을 요청하여 다운로드 받는 방식이 있다. 단말에 있는 IPMP 툴을 호출하거나 로컬 툴 검색 실패 이벤트가 일어났을 경우 툴을 리모트 서버로부터 다운로드 하는 역할을 하는 개념적인 엔티티를 MPEG-

2/4 IPMPX에서는 툴 매니저(tool manager)라고 지칭한다. 이러한 툴 다운로드 기능은 기존의 툴을 새로운 버전으로 갱신시키거나 다른 툴로 교체하는 경우에도 사용될 수 있기 때문에 IPMP 툴에 대한 안전성을 향상시켜 주는 중요한 기능 중 하나이다.

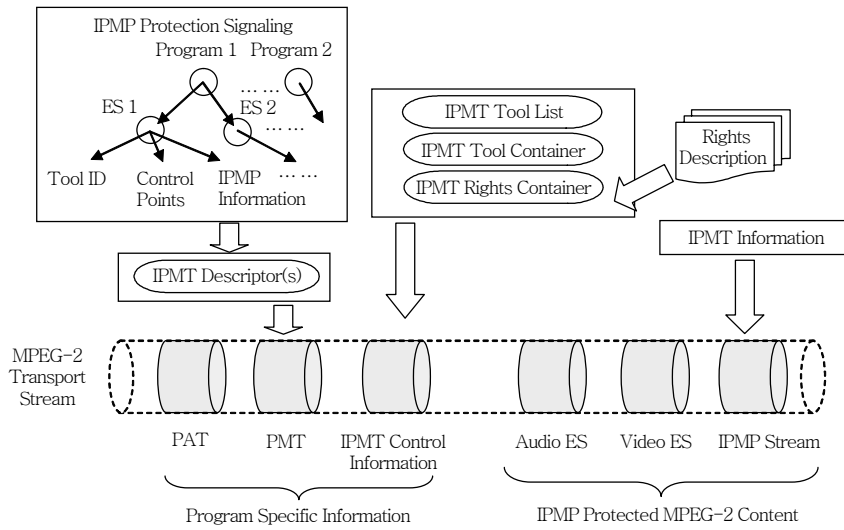
이상으로 MPEG-2/4 IPMPX가 기존의 DRM 시스템과 다른 몇 가지 주요한 특징에 대하여 살펴본다. 다음 장에서는 앞에서 살펴본 각각의 특징적인 요소들이 MPEG-2 시스템 및 MPEG-4 시스템 규격 안에서 어떻게 적용되는가를 좀더 구체적으로 살펴보도록 한다.

IV. MPEG-2 시스템과 IPMPX

MPEG-2 시스템 표준은 현재 디지털 방송과 DVD 저장 포맷 등에서 사용되고 있으며, ATM 망, 컴퓨터 네트워크, 나아가서는 정보 고속도로 등에서 연결되어 동영상 데이터가 전달되는 것을 목적으로 한 것이기 때문에 향후 이를 이용한 다양한 응용이 시도될 것으로 보인다. MPEG-2 IPMPX 표준은 현재와 가까운 미래에 디지털 콘텐츠 산업의 가장 큰 부분을 담당하게 될 MPEG-2 콘텐츠를 보호하고 유통시키기 위한 flexible, renewable, interoperable 플랫폼을 만들기 위하여 시작되었다. MPEG-2 IPMPX 표준은 MPEG-2 시스템 표준이 완료된 이후에 시작되었기 때문에, 기존의 MPEG-2 시스템과 호환을 유지하면서 어떻게 IPMPX 기능을 추가할 것인가가 관건이었다. 본 장에서는 MPEG-2 IPMPX 표준에서 정의하고 있는 콘텐츠 구조와 이를 소비하기 위한 단말의 구조에 대하여 살펴보기로 한다.

1. 콘텐츠 구조

MPEG-2 전송 스트림의 구조는 크게 PSI(Program Specific Information) 부분과 미디어스트림 부분으로 구성되어 있다[4]. 미디어스트림 부분에는 압축된 오디오 및 비디오 스트림을 담고 있고, PSI 부분에는 미디어스트림에 대한 프로그램 정보



(그림 1) MPEG-2 TS 구조와 IPMPX 정보의 위치

<표 1> PSI 섹션 PID

Structure Name	Stream Type	Reserved PID #
Program Association Table	ITU-T Rec. H.222.0 ISO/IEC 13818-1	0x00
Program Map Table	ITU-T Rec. H.222.0 ISO/IEC 13818-1	Assigned in the PAT
Network Information Table	Private	Assigned in the PAT
Conditional Access Table	ITU-T Rec. H.222.0 ISO/IEC 13818-1	0x01
Transport Stream Description Table	ITU-T Rec. H.222.0 ISO/IEC 13818-1	0x02
IPMP Control Information Table	ITU-T Rec. H.222.0 ISO/IEC 13818-1	0x03

와 사용자 인증 정보가 MPEG-2 시스템 규격에서 정의하고 있는 여러 가지 테이블(PAT, PMT, CAT 등)에 나뉘어 삽입되어 있다. 특별히 PMT(Program Mapping Table)는 콘텐츠를 구성하는 미디어 스트림에 대한 정보를 포함하기 때문에 MPEG-2 IPMPX에서는 IPMP 디스크립터를 PMT 안에 기술하도록 정의하고 있다. 또한 IPMP Control Information Table(이하 IPMP CIT)이라는 새로운 테이블을 정의하고 여기에 앞장에서 언급한 툴 리스트, 툴 컨테이너 그리고 라이트 컨테이너(rights container)를 삽입하도록 정의하고 있다. 여기서 라이트 컨테이너는 콘텐츠에 대한 사용규격이나 정책을 포함한다. 마지막으로 미디어스트림과 같이 하나의 독립된 스트림으로 전달되는 IPMP 스트림은 IPMP 툴로 전달될 수 있는 모든 종류의 IPMP 데이터를 전달할 수 있다. 예를 들어서 주기적으로 변경

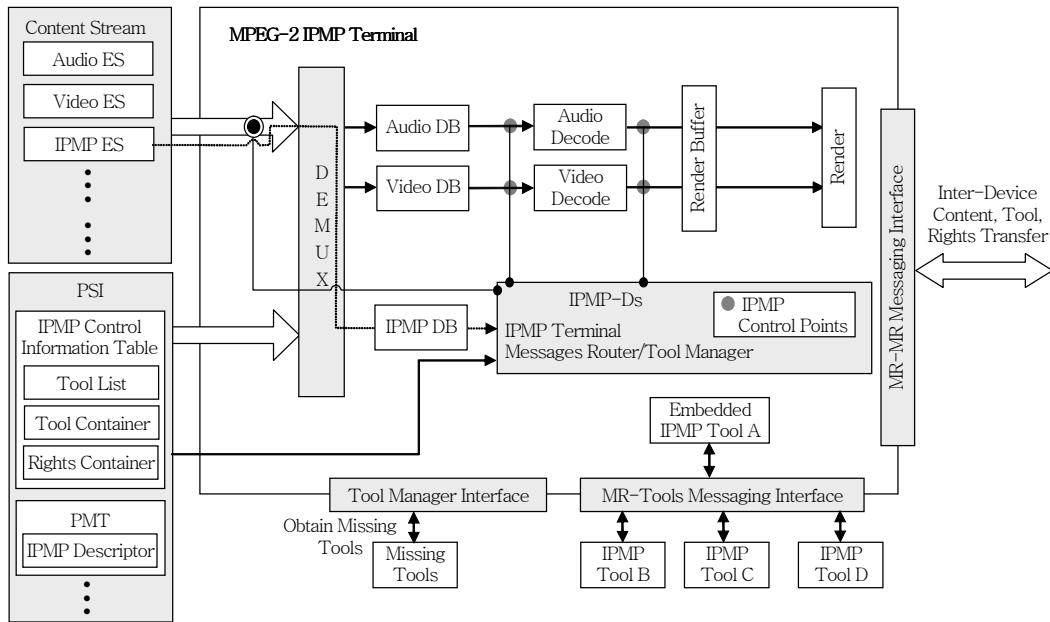
이 필요한 복호화툴 키 정보나 워터마킹툴 키정보를 전달하는 데 사용될 수 있다. (그림 1)은 IPMPX 관련 정보가 MPEG-2 전송 스트림에 삽입되는 위치를 나타낸다.

<표 1>은 MPEG-2 IPMPX 표준화를 통하여 새롭게 추가된 IPMP CIT를 포함하는 PSI를 구성하고 있는 테이블들과 이들의 PID를 보여준다. IPMP CIT는 PID 3번으로 정의되어 있다.

2. 단말 구조

(그림 2)는 MPEG-2 시스템과 IPMPX 관련 모듈의 상호작용을 보여준다.

먼저 MPEG-2 단말 시스템의 기본적인 처리과정을 보면 다음과 같다. MPEG-2 TS가 단말에 입력되면 역다중화기(DEMUX)를 통하여 PSI 정보 및



(그림 2) MPEG-2 IPMPX 구조도

오디오/비디오 스트림으로 분리되게 되고, 오디오와 비디오 스트림은 각각의 해당 디코더를 통하여 비압축 스트림으로 변형된다. 마지막으로 비압축된 오디오/비디오 스트림은 렌더링(rendering) 모듈을 통해 스피커와 스크린을 통하여 출력되게 된다. IPMPX는 이러한 MPEG-2 단말 시스템의 기본적인 콘텐츠 처리흐름 과정 가운데 다양한 제어점(그림에서 회색 원으로 표시)을 마련하고 있으며, 이러한 제어점을 통하여 IPMP 툴이 연결되고 미디어데이터에 대한 적절한 처리 또는 제어가 일어난다. 일반적으로 역다중화기 전에서의 제어점은 채널 가입자 인증을 위하여 사용되고, 디코더 전단에서의 제어점은 복호화 툴들에 의하여 제어되며, 렌더링 전단에서의 제어점은 워터마킹 툴이나 핑거프린팅 툴에 의하여 제어된다. <표 2>는 MPEG-2 IPMPX에서 정의하고 있는 제어점을 나타낸다.

IPMPX의 중추적인 역할을 담당하는 IPMP 터미널은 개념적인 엔터테인먼트 메시지 라우터와 툴 매니저로 구성된다. 메시지 라우터는 단말과 툴 사이의 메시지 전달을 담당하며, 툴 매니저는 툴 리스트에 기술된 필요한 툴들을 호출하거나 만일 필요한 툴이 단말에 없을 경우, 또는 기존의 툴을 새로 갱신할 필

<표 2> MPEG-2 IPMPX 제어점

번호	제어 위치
0x00	No control point
0x01	역다중화기 전
0x02	디코더 전
0x03	디코더 후
0x04	ISO reserved
0xDE	User private
0xFF	Forbidden

요가 있을 경우, 리모트 서버로부터 툴을 다운로드 하는 역할을 한다.

여기까지 MPEG-2 IPMPX 표준에서 정의하고 있는 콘텐츠 구조와 이를 소비하기 위한 단말의 구조를 간단히 살펴보았다. MPEG-2 IPMPX의 장점은 기존의 CA 시스템에 비하여 다양한 보호 툴들이 적용 가능하며, 결과적으로 단순한 방송 시청에 대한 제어뿐만 아니라 저장된 콘텐츠에 대한 유통, 홈 네트워크에서의 이웃하는 디바이스 간 콘텐츠 전송과 같은 앞으로 디지털 방송환경에서 제공 가능한 다양한 서비스 시나리오에서의 콘텐츠 보호 및 제어가 가능하다는 점이다.

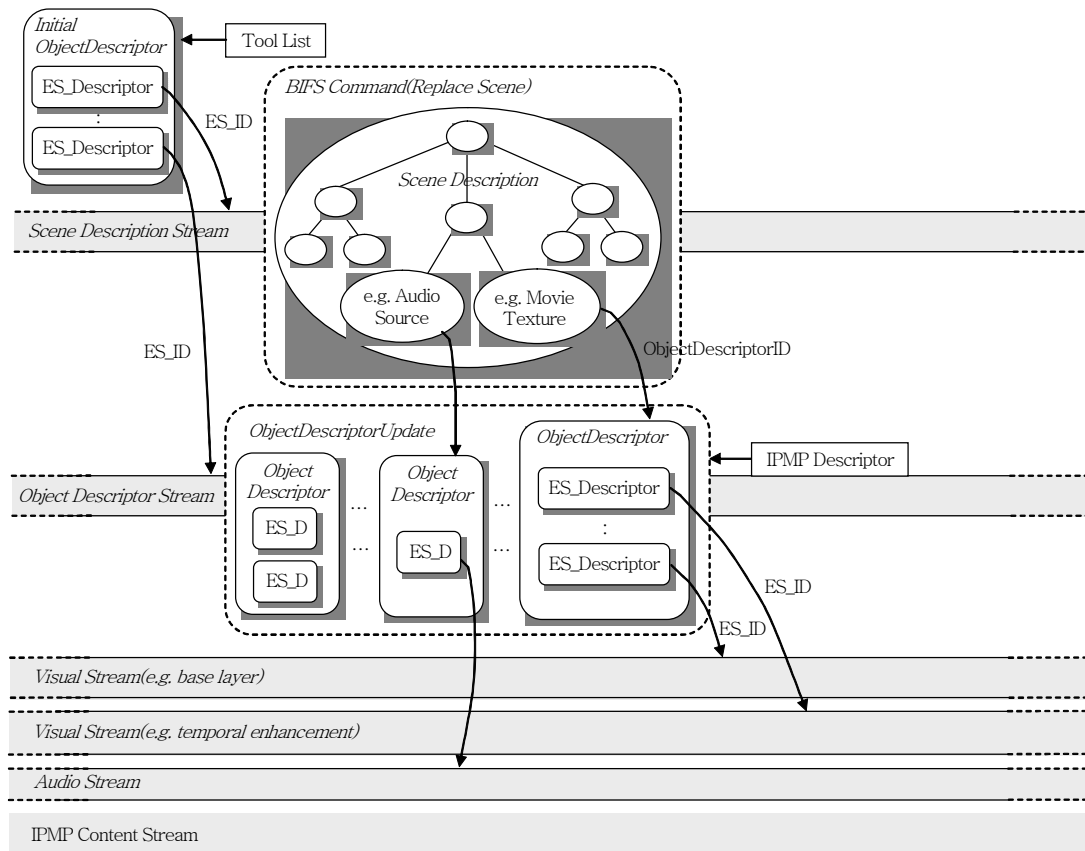
V. MPEG-4 시스템과 IPMPX

MPEG-4 IPMPX는 MPEG-2 IPMPX에 대한 표준화가 시작되기 전에 이미 표준화가 시작되었으며 결국 MPEG-2 IPMPX 표준의 근간이 되었다. 따라서 MPEG-4 IPMPX 개념과 MPEG-2 IPMPX의 개념은 매우 유사하며 실제적으로 두 표준에서 정의하고 있는 IPMP 정보와 IPMP 메시지들은 중복되는 부분이 많다. 다만 MPEG-4 IPMPX는 보호하고자 하는 대상이 MPEG-4 시스템 포맷의 콘텐츠이고 MPEG-2 IPMPX의 경우는 MPEG-2 TS 포맷의 콘텐츠이기 때문에 각각의 IPMP 정보가 삽입되는 위치와 단말에서의 시스템 디코더 차이로 인한 IPMP 정보의 추출방법이 다를 뿐이다. 본 장에서는 MPEG-4 IPMPX 표준에서 정의하고 있는 콘텐츠 구조와 이를 소비하기 위한 단말의 구조에 대

하여 살펴보기로 한다.

1. 콘텐츠 구조

MPEG-4 콘텐츠는 오디오/비디오 미디어 스트림, 장면을 구성하는 객체(object)의 표시방법과 특성을 지정하고 시간/공간상에 배치하기 위한 정보를 담고 있는 scene description 스트림, 그리고 화면을 구성하고 있는 각각의 객체 미디어에 대한 정보를 담고 있는 object description 스트림으로 구성되어 있다[5],[6]. Scene description 정보와 object description 정보는 각각 IOD(Initial Object Descriptor)와 OD(Object Descriptor) 구조 안에 정의되어 있다. 또한 각 객체를 구성하는 엘리먼트 스트림은 ESD(Element Stream Descriptor)에 기술되도록 정의하고 있다. 따라서 MPEG-4 IPMPX 규격에서는



(그림 3) MPEG-4 콘텐츠 구조와 IPMPX 정보의 위치

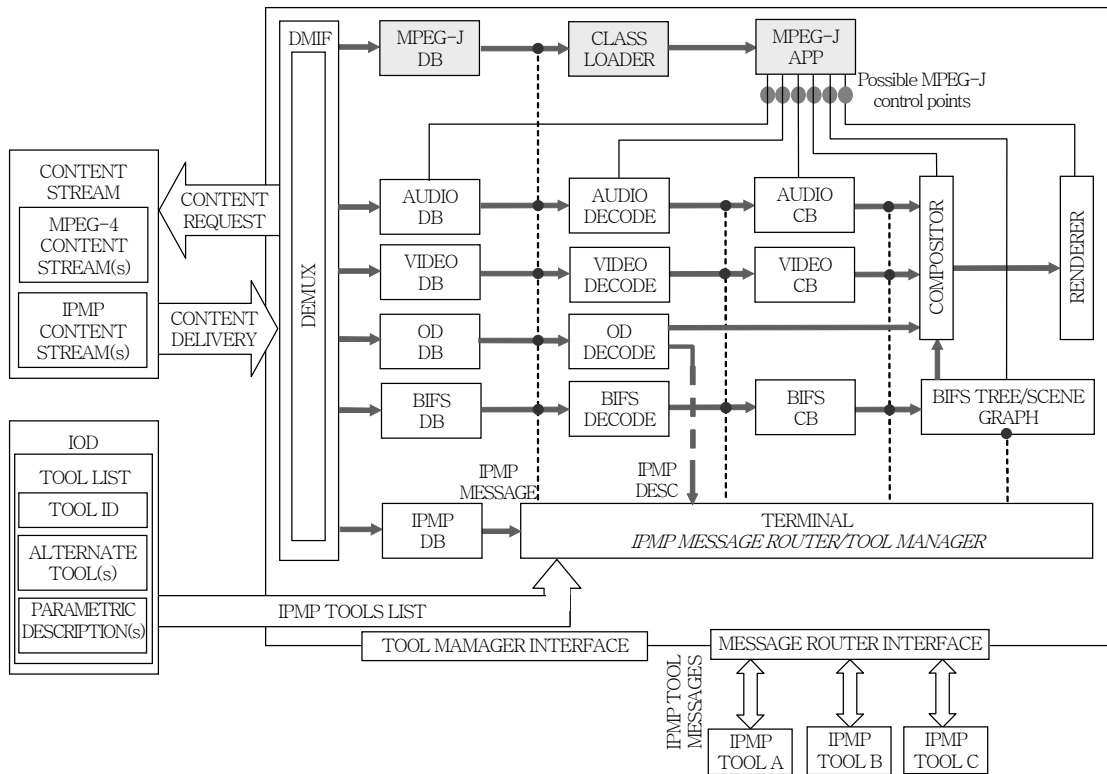
툴 리스트는 IOD에, IPMP 디스크립터는 IOD, OD 또는 ESD 안에 기술하도록 정의하고 있다. 즉 툴의 적용 범위에 따라 장면전체의 제어를 위한 툴이라면 IOD에 기술되며, 하나의 객체에 영향을 주는 툴이라면 OD에, 마지막으로 각 ES별 제어를 위한 툴이라면 ESD에 기술되는 것이다. 또한 IOD 안에는 IPMP 툴을 콘텐츠와 함께 전송하기 위하여 IPMP 툴 스트림이라는 새로운 스트림타입을 정의하고 있다. 전송되는 툴의 포맷, 패키지 정보와 IPMP 툴 ID는 IPMP 툴 스트림을 디코딩하기 위한 정보를 담고 있는 Decoder ConfigDescriptor 안에 기술되어 있으며, 이때 IPMP 툴 매니저는 IPMP 툴 스트림을 위한 디코더 역할을 한다. 이 외에도 MPEG-4 IPMPX 표준에서는 MPEG-2 IPMPX 표준에서와 같이 주기적으로 변경될 수 있는 IPMP 데이터를 IPMP 콘텐츠 스트림이라고 하는 독립적인 스트림 형태로 콘텐츠와 함께 단말에 전달하도록 정의하고

있다. (그림 3)은 MPEG-4 콘텐츠의 구조와 IPMPX 정보의 위치를 나타낸다.

2. 단말 구조

(그림 4)는 MPEG-4 시스템에 적용되는 IPMPX의 구조를 보여준다.

MPEG-4 콘텐츠가 단말에서 소비되는 과정은 MPEG-2 콘텐츠의 경우와 유사하다. 먼저 콘텐츠 스트림과 IOD가 단말에 입력되면, 역다중화기를 거쳐 각 ES별로 나누어지게 된다. 여기서 오디오와 비디오 스트림은 각각 오디오 비디오 디코더를 통하여 비압축 스트림으로 변형되어 장면합성을 위한 컴포지터(compositor)로 전달된다. 또한 장면정보(BIFS) 및 장면을 구성하는 객체정보(OD)가 각각의 디코더를 통하여 컴포지터로 입력되어 다양한 오디오 비디오 스트림이 합성된 하나의 장면을 연출하게 된다. IPMPX가 MPEG-4 단말에서 작동하는 방식도



(그림 4) MPEG-4 IPMPX 단말 구조

MPEG-2 IPMPX와 거의 유사하다. MPEG-2 IPMPX에서 개념적 엔티티로 존재하는 메시지 라우터와 툴 매니저가 MPEG-4 IPMPX 터미널에도 존재하며 그 역할이 동일하다. 또한 MPEG-2 IPMPX에서 정의하고 있는 툴과 터미널 사이 또는 툴과 툴 사이에 사용되는 메시지들도 기능과 이름까지도 거의 유사하다. 다만, MPEG-4 콘텐츠를 구성하는 ES의 종류가 다양하기 때문에 MPEG-4 IPMPX에서는 MPEG-2 IPMPX 보다 다양한 제어점이 존재하며 각 제어점의 특징을 잘 이용한다면 보다 다양한 컨트롤이 가능해진다.

VI. 개발사례

유럽 연합 프로그램인 IST(Information Society Technology) 주관으로 2003년 3월에 시작되어 2004년 2월까지 수행되었던 MOSES(MPEG Open Security for Embedded Systems) 프로젝트는 다양한 플랫폼에서 서비스되고 있는 디지털 콘텐츠를 안전하고 신뢰성 있게 창작하고, 전달하고, 소비하기 위한 디지털 콘텐츠의 보호, 저작권 관리기술 개발을 그 목표로 하고 있다[7]. MOSES 프로젝트를 통하여 구현된 시스템은 뮤직 콘텐츠 유통 시나리오와 디지털 방송 시나리오를 기반으로 하고 있으며, 각각 MPEG-4 IPMPX와 MPEG-2 IPMPX 표준을 기반기술로 하고 있다. 본 프로젝트에서 구현된 MPEG-2/4 IPMPX 모듈들은 현재 MPEG-2 IPMPX와 MPEG-4 IPMPX의 참조 소프트웨어로 인정되어 MPEG CVS 서버를 통하여 공개되고 있으며, 이를 적용한 OpenSDRM 시스템은 MPEG-4 IPMPX 기술이 실제 콘텐츠 유통 서비스에도 접목이 가능함을 보여주고 있다(www.music-4you.com).

VII. 해결과제

상호 연동가능한 DRM 플랫폼으로 기존의 DRM 시스템에 비하여 큰 장점을 가지고 있는 MPEG-2/4 IPMPX도 아직 해결해야 할 기술적인 과제가 많다. 첫째, MPEG-2 IPMPX의 경우 이미 MPEG-

2 시스템이 표준화 된 후, 산업화에서 활용되고 있는 시점에서 표준이 시작되었으므로, 기존에 제품으로 만들어진 MPEG-2 시스템 디코더는 MPEG-2 IPMPX에서 제안하고 있는 다양한 제어점들을 지원하기 어렵다. 예를 들어 MPEG-2 IPMPX에서는 역다중화기와 미디어 디코더 사이에 암호화 툴들이 적용될 수 있는 제어점을 마련해 놓고 있으나, 현재 상용화되고 있는 칩셋은 역다중화기와 미디어 디코더가 하나의 칩으로 구현되고 있다. 따라서 이를 지원할 수 있는 하드웨어 플랫폼에 대한 개발이 시급하다. 둘째, MPEG-2/4 IPMPX는 다양한 보호툴들의 적용을 지원하고 있다. 일반적으로 이러한 툴들이 처리해야 하는 미디어 데이터량이 적지 않고 계산량이 많기 때문에 이를 실시간으로 처리하기 위해서는 높은 성능의 단말을 필요로 하게 된다. 그러나 단말마다 OS 환경이 다르고 CPU 성능도 다르기 때문에 서로 다른 단말에 따른 툴 적용 문제를 어떻게 해결해야 할 것인가가 풀어야 할 숙제 중의 하나이다. 셋째, MPEG-2/4 IPMPX가 다른 DRM 시스템과 같이 소프트웨어적인 측면이 강하기 때문에, 해킹에 대한 우려가 높다. 그러나 예전에 소프트웨어 모듈이 가지고 있었던 보안적 취약점이 DRM 기술의 진보로 말미암아 상당 부분 해결되었으며 더욱 보완되고 있으므로, 이를 바로 MPEG-2/4 IPMPX에 적용할 수 있으리라 본다.

VIII. 관련 표준화

상호연동 가능한 DRM 플랫폼은 다만 MPEG-2/4 영역에서만 다루어지고 있는 내용이 아니라, 다양한 콘텐츠 저장매체를 기반으로 하는 콘텐츠 소비자나 특정 콘텐츠 서비스에서도 중점적으로 고려되고 있다. 본 장에서는 MPEG-2/4 IPMPX와 같이 상호연동 가능 DRM 플랫폼을 목적으로 하는 표준화 동향에 대하여 살펴보도록 한다.

1. DVB CPCM

DVB(Digital Video Broadcasting)은 약 300여 개의 방송, 네트워크, 제조, 및 법률관련 업체들이

모여 디지털 방송과 관련된 국제 표준을 만들고 있는 단체이다[8]. PVR과 같은 디지털 저장 매체에 저장되는 콘텐츠에 대한 보호가 필요함에 따라, DVB commercial module에서는 DVB CA(Conditional Access)의 제어범위를 넘어서는 도메인에서의 콘텐츠의 보호와 관리를 위한 공통 프레임워크를 제공해야 할 필요성을 느끼게 되었고, DVB CPCM(Content Protection and Copy Management)에 관한 요구사항을 제출했다. DVB CPCM의 보호 범위는 콘텐츠가 자유롭게 이동하거나 복사될 수 있는 디지털 홈 네트워크 환경과 개인 비디오 녹화기(PVR)를 포함한다. DVB CPT(Copy Protection Technologies)를 담당하고 있는 서브그룹에서는 제출된 요구사항에 대하여 2001년 7월에 공개적으로 외부로부터 해결 제안(call for proposals)을 받아들이기 시작하였으며 총 24개의 proposal들이 제안되었다[8]-[10]. 이들을 기반으로 PC, 셋톱박스, TV, PVR, disk recorder 등을 고려한 기능 모델을 구체화 시켰으나, 제안된 기술 중 표준으로 적합한 기술을 채택하기 위하여 2002년 6월에 기술 요구사항(technical requirements)을 정의할 것을 결정하였다. 2004년 현재 기술 요구사항에 대한 정립과 함께 기술 규격(technical specification)에 대한 초안이 작성중에 있다. 기술 초안에서 중점적으로 다루게 될 표준화 항목으로는 system description, signalling formats and interoperability, security, system interfaces, CPCM toolbox, 그리고 시나리오 예제들이 추가될 것이다.

2. DMP

DMP(Digital Media Project)는 비영리 단체에 의하여 2003년 12월에 시작된 국제 표준화 프로젝트로, 다양한 형태로 존재하는 디지털 미디어들을 다양한 디바이스에서 효율적이며 합법적으로 소비할 수 있는 통합 환경을 제공하는 데 그 목적이 있다. 현재 ETRI(한국), British Telecom(영국), MPEG LA(미국), Telecom Italia(이태리) 등 다양한 국가로부터 약 14개 기관에서 참여하고 있으며,

크게 recommended action 파트와 technical specification 파트로 나누어 프로젝트를 수행하고 있다[11]. 특히 DMP에서는 현재 디지털 콘텐츠 산업이 활성화되지 못하는 가장 큰 이유가 기존에 아날로그 콘텐츠 환경에서 저작권자들이 소유했던 이득과 권리가 디지털 환경으로 넘어오면서 보호되지 않기 때문이라고 보면서, 기존의 저작권자들이 그동안 아날로그 콘텐츠에 대하여 행사했던 권리들(Traditional Rights and Usage: TRU)을 정리하는 것을 첫번째 과제로 보고 있다. 현재까지 약 70여 개의 TRU들이 정의되었으며, 이들을 기반으로 앞으로 정의할 시스템 규격을 위한 요구사항을 정의하고 있다[12].

3. ISMACryp

ISMA(Internet Streaming Media Alliance)는 인터넷을 통한 스트리밍 미디어 서비스를 활성화하기 위하여 미디어 엔코더, 서버, 플레이어에 대한 표준을 정의하고 있다. 특히 ISMACryp 규격은 다양한 벤더에 의하여 제공되는 스트리밍 서비스를 제공할 수 있도록 interoperable DRM에 대한 규격을 정의하고 있다[13]. 스트리밍 미디어의 보호를 위하여 ISMA 미디어와 프로토콜에 대한 암호화 및 인증을 실시하고, 이를 위하여 기본적인 암호화 및 인증 알고리즘이 제공되어야 한다. ISMA 단말은 ISMA 자체 포맷 콘텐츠만을 지원하는 단말과 MPEG-4 시스템 형태의 콘텐츠까지 지원하는 단말로 나누어 정의하고 있으며, 이에 따라 MPEG-4 시스템 형태의 콘텐츠를 지원하는 단말은 MPEG-4 IPMPX와의 호환성도 제공할 것을 정의하고 있다. ISAM DRM 구조는 크게 mastering, key license MGT, sender, ISMA receiver의 4가지 엔티티로 구성된다. Mastering 엔티티는 콘텐츠를 보호된 형태(ISMACryp)로 만들며, 준비된 콘텐츠를 sender에게 보내 준다. 또한 해당 콘텐츠에 대한 라이선스 정보를 key license MGT로 보내 준다. ISMA 단말이 sender에게 콘텐츠를 요청하면 sender는 ISMACryp 형태의 콘텐츠를 전달하고 이를 풀기 위한

키를 key license MGT에게 요청하는 구조로 되어 있다. 엔티티들 간의 통신은 반드시 인증을 통하여 안전하게 이루어진다. 본 규격은 2003년 12월에 1차 버전이 완성되었으며 현재 ISMA 홈페이지(www.isma.tv)를 통하여 등록하면 무료로 다운로드 받을 수 있다.

IX. 결론

본 논문에서는 최근 표준화가 완료중인 MPEG-2/4 IPMPX의 목적과 특징에 대하여 소개하고 관련 개발사례와 MPEG-2/4 IPMPX에서 앞으로 해결해야 할 과제들에 관하여 살펴보았다. 또한 interoperable DRM을 목적으로 하는 다른 표준화 동향에 대하여도 간단히 살펴보았다. 유비쿼터스 시대를 앞둔 현재, 콘텐츠가 다양한 디바이스로 이동하면서도 저작권에 대한 보호가 일관성을 유지하기 위해서는 DRM 시스템에 대한 호환성 유지가 대단히 중요하다. MPEG-2/4 IPMPX 개념은 기존의 DRM 시스템이 갖고 있었던 호환성 문제를 풀기 위한 중요한 힌트를 준다고 할 수 있다. 바로 IPMP 틀 개념과 인터페이스 메시지라고 할 수 있는데, 이러한 개념은 전체 DRM 시스템 안에서 세부 컴포넌트별로 제어를 할 수 있도록 하며, 컴포넌트별 갱신을 가능하게 한다. 또한 컴포넌트들 간에 융통성 있는 인터페이스를 가능하게 하여 특정 애플리케이션 환경에서도 IPMPX 시스템을 쉽게 적용할 수 있도록 한다.

마지막으로, 앞으로 interoperable DRM이 더욱 발전하기 위해서는 DRM 환경에서 사용되는 term들을 명확히 정의하고 이들이 공통적으로 사용할 language가 정의되어야 할 것으로 보인다.

참고 문헌

- [1] IPMP 101(m7885)
- [2] ISO/IEC 13818-1 2000 Study of FPDAM 2
- [3] ISO/IEC 14496-1 2001 FDAM 3
- [4] ISO/IEC 13818-1, MPEG2 system
- [5] ISO/IEC 14496-1, Information Technology - Coding of Audio-Visual Objects - Part 1: Systems, 2001.
- [6] ISO/IEC 14496-2, Information Technology - Coding of Audio-Visual Objects - Part 2: Visual, 2001.
- [7] MOSES, Part C- RTD Proposals: Description of Contribution to EC Policies, Economic Development, Management and Participants, Oct. 2001.
- [8] DVB-CPT 002r1, *Draft DVB CPCM Specification*, Dec. 2001.
- [9] DVB-CPT 187r14, *DVB CPCM Functional Model Definitions and Applications*, Ver. 3, 2003. 8. 15.
- [10] DVB-CPT 017r5, *Draft Technical Requirements*, Feb. 2003.
- [11] DMP-0022, *The Digital Media Manifesto*, Feb. 2004.
- [12] DMP-0046, *Traditional Rights and Usages of Media Users*, 2004. 4. 20.
- [13] ISMA, Encryption and Authentication Specification, Ver. 1.0, Feb. 2004.