FBMF Standard

미래방송미디어표준포럼표준 (국문표준)

FBMF-STD-004 제정일: 2017 년 06 월 15 일

IP기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 시스템을 위한 Common Encryption 규격

Common Encryption Specifications for IP-based Multi-CA/DRM Content Protection

FBMF

미래방송미디어표준포럼

Future Broadcast and Media Standards Forum

표준초안 검토 위원회	**방송콘텐츠보호기술WG**				
표준안 심의 위원회	**미래방송미디어표준포럼 운영위원회**				
	성명	**소 속**	**직위**	**위원회 및 직위**	**표준번호**
표준(과제) 제안	구한승	ETRI	책임연구원	방송콘텐츠보호기술WG의장	FBMF-STD-004
표준 초안 작성자	구한승	ETRI	연구원	방송콘텐츠보호기술WG의장	FBMF-STD-004
	이주한	한양대	-	-	
사무국 담당	김제우	KETI	수석연구원	미래방송미디어표준포럼 운영위원회 간사	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 FBMF 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 미래방송미디어표준포럼 의장
발행처 : 미래방송미디어표준포럼
135-703, 서울시 강남구 테헤란로 7길 22 본관 610호 (역삼동 한국과학기술회관)
Tel : 02-568-3556, Fax : 02-568-3557
발행일 : 2017.xx

서 문

1 표준의 목적

본 표준은 다운로드 방식 기반 멀티 CA/DRM (Conditional Access/Digital Rights Management) 솔루션 기술과 관련해 국제 표준인 ITU-T J. 1010및 ITU-T J.1011과 유럽 표준인 ETSI ISG ECI을 기반으로 하여 한국 상황에 맞는 IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템을 위한 Common Encryption 규격 정의를 목적으로 한다.

2 주요 내용 요약

본 표준은 CPE(Customer Premises Equipment)가 신뢰 환경에서 CA/DRM 클라이언트를 다운로드 하기 위한 교환 가능한 IMCP (IP-based Multi-CA/DRM Content Protection) 시스템의 Common Encryption (CENC) 규격을 명시한다. IMCP 시스템에서는 콘텐츠 보호 라이센스가 여러 공급 업체의 다양한 콘텐츠 암호 해독 모듈에 전달될 수 있도록 하는 CENC 기술을 사용한다. CENC 기술의 주요 이점은 콘텐츠를 암호화하는 공통 방법을 제공함으로써 콘텐츠 암호화를 키 획득과 분리하여 여러 DRM 시스템을 지원한다는 것이다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

본(이) 표준은 참조 표준 문서들을 기반으로 하여 한국 지상파 방송 현황에 맞춰서 IP기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 시스템을 위한 Common Encryption 규격을 정의하였다.

- ITU-T J.1010, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Use cases and requirements”, 2016.
- ITU-T J.1011, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Architecture, Definitions and Overview”, 2016.
- ETSI GS ECI 001-1, “ETSI GS ECI 001-1: Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview”, 2014.

- ETSI GS ECI 001-2, “ETSI GS ECI 001-2: Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements”, 2014.
- TG3-S31-087r13, “System Requirements for ATSC 3.0”, 2016.
- TG3-S36-086r10, “ATSC Candidate Standard: ATSC 3.0 Security and Service Protection”, 2017.
- ISO/IEC 23001-7, “MPEG systems technologies - Part 7: Common encryption in ISO base media file format files”, 2016.
- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항”, 2016
- FBMF-STD-002, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처”, 2017

3.2 인용 표준과 본 표준의 비교표

FBMF-STD-004	참조 표준	비고
5. IMCP 시스템 Common Encryption 규격	ATSC 3.0, TG3-S36-086r10	준용

Preface

1 Purpose

The purpose of this standard is to define the specifications of Common Encryption for the multi-device content protection system eligible for IP-based broadcasting environment in Korea (Rep. of) by referencing the international standards ITU-T J.1010, ITU-T J.1011 and the European standards ETSI ISG ECI.

2 Summary

This standard specifies the specifications of Common Encryption for exchangeable, embedded CA/DRM solutions, enabling CPE to download CA/DRM clients under a trusted environment. The IMCP system uses the Common Encryption technology which allows content protection licenses to be passed to various content decryption modules from multiple vendors. The key advantage of Common Encryption is that by providing a common way to encrypt content, it decouples the content encryption from the key acquisition and thus provides support for multiple DRM systems.

3 Relationship to Reference Standards

3.1 Relationship of Reference Standards

This standard specifies the specifications of Common Encryption for broadcasting service of Republic of Korea based on the reference standards.

- ITU-T J.1010, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Use cases and requirements”, 2016.
- ITU-T J.1011, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Architecture, Definitions and Overview”, 2016.
- ETSI GS ECI 001-1, “ETSI GS ECI 001-1: Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview”, 2014.
- ETSI GS ECI 001-2, “ETSI GS ECI 001-2: Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements”, 2014.

- TG3-S31-087r13, “System Requirements for ATSC 3.0”, 2016.
- TG3-S36-086r10, “ATSC Candidate Standard: ATSC 3.0 Security and Service Protection”, 2017.
- ISO/IEC 23001-7, “MPEG systems technologies - Part 7: Common encryption in ISO base media file format files”, 2016.
- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항”, 2016
- FBMF-STD-002, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처”, 2017

3.2 Differences between Reference Standards and this Standard

FBMF-STD-004	Reference Standard	Remarks
5. The Specifications of Common Encryption for IMCP system	ATSC 3.0, TG3-S36-086r10	modified

목 차

IP기반 방송 환경에서 멀티 CA/DRM 콘텐츠보호 시스템을 위한 Common Encryption 규격

Common Encryption Specifications for IP-based Multi-CA/DRM Content Protection

1 적용 범위

본 표준은 CPE(Customer Premises Equipment)가 신뢰 환경에서 CA/DRM 클라이언트를 다운로드 하기 위한 교환 가능한 IMCP (IP-based Multi-CA/DRM Content Protection) 시스템의 Common Encryption 규격을 명시한다. IMCP 시스템에서는 콘텐츠 보호 라이센스가 여러 공급 업체의 다양한 콘텐츠 암호 해독 모듈에 전달될 수 있도록 하는 Common Encryption (CENC) 기술을 사용한다.
본 표준은 IMCP 시스템상에서 콘텐츠 보호를 위해 DASH 콘텐츠 전달을 위한 콘텐츠 보호 의 방법을 정의한다.

본 표준에서는 IMCP 시스템이 서로 다른 DRM 및 키 관리 시스템을 사용하여 동일한 파일의 암호 해독을 활성화하는데 사용할 수 있는 표준 암호화 및 키 매핑 방법을 명시한다. 본 표준에서 명시하는 암호화된 미디어 확장은 웹 애플리케이션이 콘텐츠 보호 시스템과 상호 작용할 수 있게 하는 API를 제공하여 암호화된 오디오와 비디오를 재생할 수 있도록 한다. IMCP 클라이언트는 표준화된 API와 CENC를 통해 같은 앱과 암호화된 파일을 하위 보호 시스템에 관계없이 어떤 브라우저에서나 사용할 수 있도록 디자인되었다.

2 참조 표준

다음 문서들이 본 표준의 참고 문서로 사용되었다.

2.1 국외 표준

- ITU-T J.1010, “Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Use cases and requirements”, 2016.
- ITU-T J.1011, “Embedded Common Interface (ECI) for exchangeable CA/DRM

solutions; Architecture, Definitions and Overview", 2016.

- ETSI GS ECI 001-1, "ETSI GS ECI 001-1: Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview", 2014.

- ETSI GS ECI 001-2, "ETSI GS ECI 001-2: Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements", 2014.

- TG3-S31-087r13, "System Requirements for ATSC 3.0", 2016.

- TG3-S36-086r10, "ATSC Candidate Standard: ATSC 3.0 Security and Service Protection", 2017.

- ISO/IEC 23001-7, "MPEG systems technologies - Part 7: Common encryption in ISO base media file format files", 2016.

2.1 국내 표준

- NGBF-STD-017, "IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항", 2016

- FBMF-STD-002, "IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처", 2017

3 용어 정의

3.1 IP기반 방송환경에서 멀티 CA/DRM 콘텐츠 보호 (IMCP, IP-based Multi-CA/DRM Content Protection)

CPE 내 소프트웨어 기반 변경 가능한 IMCP 클라이언트의 구현과 개발을 허용하고, IMCP를 준수하는 다른 CPE 장치와의 상호 호환성을 제공하는 아키텍처와 시스템.

3.2 IMCP서버 (IMCP Server)

IMCP 클라이언트에 콘텐츠 또는 기타 서비스를 제공하고 본 표준의 규범적 요구사항을 준수하는 모든 IP 연결 장치

3.3 IMCP 클라이언트 (IMCP Client)

IMCP와 호환되는 CA/DRM 클라이언트의 구현. 이것은 CPE에 있는 소프트웨어 모듈이고 콘텐츠 분배자나 운영자로부터 분배되는 콘텐츠에 대한 소비자 자격과 권리를 보호 받기 위한 모든 수단을 제공한다. 또한, IMCP 클라이언트는 소비자가 사용하는 권리나 자격 같은 조건을 받고 다양한 암호화된 메시지와 콘텐츠를 해석하기 위한 키를 받는다.

4 약어 및 규약

4.1 약어

본 표준은 다음 약어들을 사용한다.

AES	Advanced Encryption Standard
AVC	Advanced Video Coding
BLOB	Binary Large OBject
CDM	Content Decryption Module
CENC	MPEG Common Encryption
DRM	Digital Rights Management
EME	Encrypted Media Extensions
HEVC	High Efficiency Video Coding
IMCP	IP-based Multi-CA/DRM Content Protection
IP	Internet Protocol
ISO BMFF	ISO Base Media File Format
NAL	Network Abstraction Layer
OCSP	Online Certificate Status Protocol
RSA	Rivest, Shamir, and Adelman
UUID	Universally Unique Identifier

4.2 규약

본 표준은 다음의 규약을 따른다:

- “**반드시 ~ 해야한다.**” 또는 “**반드시 ~ 할 수 있어야 한다.**” 또는 “**절대 ~ 해서는 안된다.**”: 어떠한 경우에도 예외 없이 필수적인 항목 (영어의 SHALL에 해당)
- “**~ 해야한다.**” 또는 “**~할 수 있어야 한다.**”: 아주 명백한 사유가 있지 않는 한 “반드시 ~ 해야한다.”인 항목 (영어의 SHOULD에 해당)
- “~ 할 수도 있다.”: 추가적으로 허용될 수 있는 항목 (영어의 MAY에 해당)

5 IMCP시스템 Common Encryption 규격

5.1 시스템 개요

본 표준에 명시된 기술적인 개념은 CENC 호환 DRM 시스템 모두에서 적용될 수 있다. CPE는 IMCP 클라이언트들의 통합성과 인증을 보호하기 위한 필수 보안 기능을 갖춘 특별한 로더(loader)를 관리한다. 이 로더(loader)는 다른 IMCP 클라이언트를 인증하고 다운로드하기 위해 언제라도 호출되어 동작될 수 있다.
각 IMCP 클라이언트는 각자의 VM 인스턴스와 함께 분리된 소프트웨어 컨테이너 에 설치된다.

IMCP 컨테이너는 CA/DRM 기능 전용이다. CPE와의 인터페이스는 다양한 CA/DRM 기능들에 필요한 요청과 데이터 교환을 가능하게 한다. 이러한 요청과 데이터 교환은 IMCP 클라이언트와 호스트, 같은 호스트에 있는 두 개의 IMCP 클라이언트, 또는 서로 다른 호스트에 있는 두 개의 IMCP 클라이언트 사이에서 이루어 진다.
IMCP클라이언트들은 multicrypt 모드에서 동작하는 CENC 호환 DRM 시스템들의 서버 쪽이 각자의 최신 표준에 호환이 되면, 그 플랫폼 안에 구성될 수 있다.

5.2 공통 암호화 (Common Encryption)

IMCP 시스템은 방송용 송출용 미디어 컨테이너로 MPEG-defined ISO Base Media File Format (ISO BMFF)을 사용한다. MPEG Common Encryption (CENC)는 ISO BMFF와 함께 사용하기에 적합한 디지털 저작권 관리 시스템이다. DRM 암호화가 필요한 모든 미디어는 반드시 MPEG Common Encryption (CENC)를 사용해야 한다.
CENC의 주요 이점은 콘텐츠를 암호화하는 공통 방법을 제공함으로써 콘텐츠 암호화를 키 획득과 분리하여 여러 DRM 시스템을 지원한다는 것이다.

CENC 메커니즘은 미디어 샘플 또는 그 일부만 암호화하고 파일 및 트랙 구조 박스와 같은 ISOBMFF 메타 데이터는 암호화되지 않도록 하여 플레이어가 파일을 올바르게 인식하고 읽고 필요한 모든 라이센스를 획득 할 수 있게 한다. CENC는 AVC 및 HEVC와 같은 NAL 기반 비디오 인코딩 포맷의 암호화를 지원하므로 하위 샘플의 비디오 데이터만 암호화되고 NAL 헤더는 암호화되지 않는 하위 샘플 암호화 기능을 제공한다. 이러한 유연성은 비디오의 무료 미리 보기를 제공하고, 비디오 편집 및 처리를 가능하게 하며, 오디오와 같은 일부 서비스 구성 요소에 대한 무료 액세스를 제공하는데 사용될 수 있다. ISOBMFF "mdat" 박스에 있는 샘플 내의 암호화된 바이트 범위에 대한 오프셋(offset)을 제공함으로써 플레이어는 파일을 쉽게 처리하고 해독 및 재생을 위해 암호화된 청크(chunk)를 해독기로 전달할 수 있다.

암호 해독이 작동하려면 CENC가 ISOBMFF에 다음 정보를 제공해야 한다:

- Key Identifier (KID): 키 ID는 트랙의 암호화 된 모든 샘플과 연관되어야 한

다. 하나의 키가 전체 트랙에 사용되는 경우.

- Initialization Vector (IV): 암호화 함수를 초기화하는데 사용되는 난수값으로 모든 샘플에 대한 해독 키를 구성할 수 있으려면 먼저 IV를 알아야 한다.
- 라이센스 취득 정보: 라이센스 취득에 대한 정보는 각 DRM 시스템에 따라 다르다. 플레이어는 암호화된 스트림에 대한 액세스를 제공하는 DRM 시스템 중 적어도 하나를 지원해야 한다.

키 ID는 다음과 같이 제공될 수 있다:

- 전체 트랙에 하나의 키가 적용된 경우에는 트랙 암호화 박스 “tenc”의 default_KID
- 샘플 그룹 서술자(descriptor)박스 "sgpd"를 사용하여 샘플 그룹화 구조에서 제공되는 동일한 암호화 키를 공유하는 샘플 세트의 키

모든 샘플에 대한 IV는 암호화된 청크(chunk)의 위치에 대한 정보와 함께 "mdat" 박스 또는 "senc" 박스에 샘플 보조 정보의 일부로 포함되어 제공된다.
라이센스 취득 정보는 각 DRM 시스템이 SystemID로 식별되는 보호 시스템 특정 헤더 박스 "pssh"의 일부로 포함되어 제공된다. "pssh" 박스는 지원되는 키 ID와 지원되는 키 ID로 식별되는 키를 얻는 방법을 설명하는 불투명한 시스템 특정 정보의 목록도 함께 제공한다.

그림 1은 암호화된 트랙의 구조를 나타낸다.

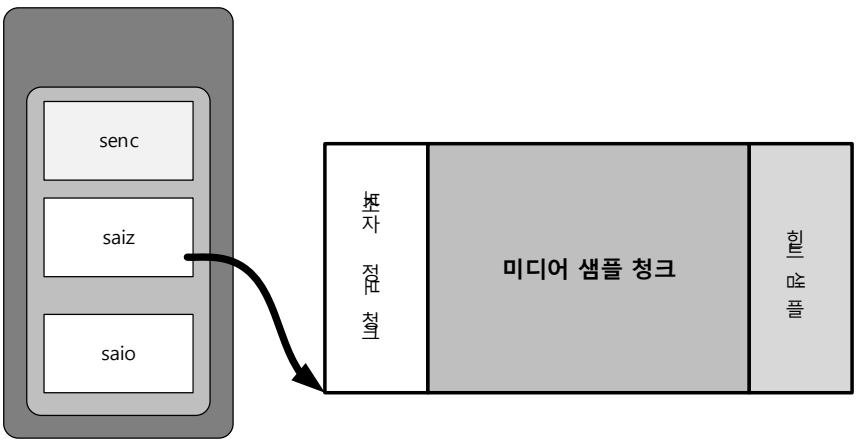

그림 1 CENC 관련 정보의 저장소

5.3 암호화된 미디어 확장 (Encrypted Media Extensions)

W3C Encrypted Media Extensions (EME)는 웹 애플리케이션이 CDM (Content Decryption Module)라고 하는 장치 상주 DRM 시스템 에이전트와 키 소스의 암호 해독 키 교환을 용이하게 하고 암호화된 오디오 및 비디오 미디어 콘텐츠의 재생을 지원하기

위한 JavaScript API를 지정한다. EME는 MPEG-CENC (Common Encryption) 보호 콘텐츠로 MPEG-DASH를 사용하여 HTML5에서 사용하는 가변 비트율 스트리밍을 가능하게 하는 HTML5 Media Source Extensions 규격을 기반으로 한다. EME 아키텍처는 그림 2에 묘사되어 있다. 그림 2는 콘텐츠 해독 및 재생을 가능하게 하기 위해 암호화된 콘텐츠의 검색과 라이센스 및 주요 자료 수집에 관련된 기능 엔터티(entity)간의 EME 동작처리흐름 나타내고 있다.

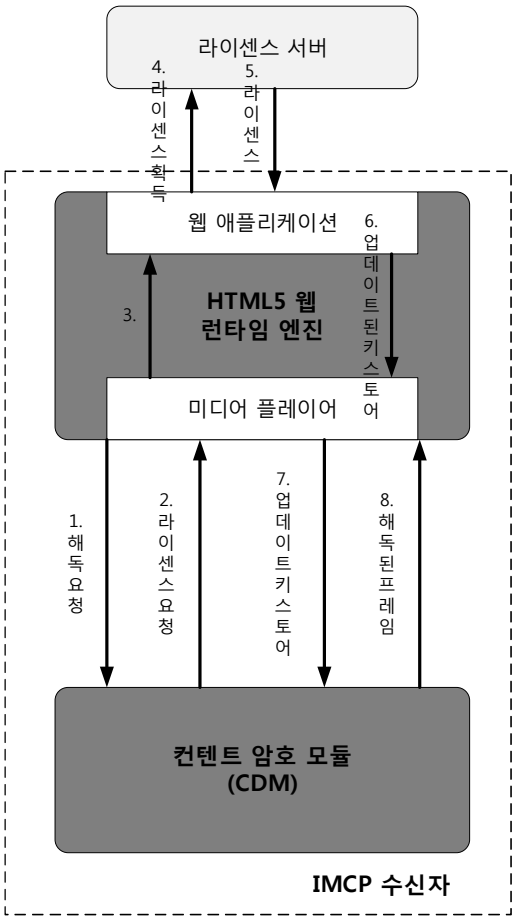

그림 2 암호화된 미디어 확장 동작 흐름

EME의 주요 개체는 MediaKeySession와 MediaKeys이다. 웹 애플리케이션은 MediaKeys 객체에서 createSession ()을 호출하여 라이센스 및 해당 키의 수명을 나타내는 MediaKeySession 객체를 만든다. 애플리케이션은 암호화된 이벤트 처리기에서 얻은 미디어 데이터를 CDM에 전달하여 라이센스 요청을 시작한다. 차례로 선택한 DRM 시스템의 CDM은 데이터 blob (라이센스 요청)을 생성하고 이를 애플리케이션에 다시 전달한 다음 해당 요청을 라이센스 서버로 보낸다. 그런 다음 MediaKeySession의 update () 메서드를 사용하여 서버에서 반환된 라이센스가 애플리케이션에서 CDM으로 전달된다. CDM 그리고/또는 브라우저는 키 세션에 저장된 키를 사용하여 미디어 샘플이 있을 때 이를 해독한다. CDM은 웹 브라우저에 내장되거나 암호가 해독된 프레임을 디코더에 전달할 때 필요한 보안 수준에 따라 신뢰할 수 있는 환경에서 실행될 수 있다.

5.4 CENC와 EME를 위한 DASH 클라이언트 프로세스

5.4.1 개요

본 절에서는 CENC 보호 미디어에 접속할 때 IMCP 수신자의 동작을 설명한다.
DASH 형식의 스트리밍 서비스 콘텐츠를 보호하기 위해 DASH는 다수의 DRM 시스템에 대한 CENC 프레임워크를 지원한다. DASH는 고유한 방식의 특정 시그널링 정보를 보호 시스템에 포함한다.

시그널링 정보는 두 가지 방식으로 전달된다:

a) MPD 내 미리 저장되어 있는 위치에 전달되는 방식,
b) 인밴드(Inband)로 DASH 콘텐츠를 수반하는 방식.

두 방식은 ISO/IEC 23001-7에 정의된 사용 방식과 호환되고, movie 프래그먼트(fragment)를 fragment를 위한 ISO BMFF 형식의 메타데이터 박스가 지정된다. 세부사항은 DASH-IF IOP 표준에 명시된 관련 내용을 따른다.

5.4.2 DASH에서의 기본 CENC 동작

본 절은 DASH 형식의 DRM 시스템에 의해 보호되고 전달되는 스트리밍 콘텐츠가 어떻게 해독되고 재생되는지에 관한 기본 메커니즘을 설명한다. 본 절에서는 라이센스 및 키 획득과 후속 콘텐츠 해독 및 재생을 위해 수신기 및 수신기와 라이센스 서버 사이에 필요한 상호 작용을 설명한다.

본 절에서는 두 가지 대체 방법을 메시지와 엔터티(entity) 상호 간의 처리 흐름을 통해 설명한다. 첫 번째 (5.4.2.1 절 참조)에서, CDM에 의한 DRM 라이센스 및 콘텐츠 키의 획득은 스트리밍 전달 프로그램의 시작될 때 발생한다. 두 번째 방법 (5.4.2.2 절 참조)에서, CDM에 의한 DRM 라이센스 및 콘텐츠 키의 획득은 프로그램 전달 중에 발생한다. DRM 보호 콘텐츠 재생 시 시작 지연은 주로 광대역 네트워크에 대한 특정 서비스 요구사항 및 실제 라이센스 취득 지연에 영향을 받지만, DRM 보호 콘텐츠 재생 시 시작 지연을 줄이는데 있어 방송 프로그램의 시작 전에 라이센스 및 키 획득을 부트스트래핑(bootstrapping)하는 첫 번째 방법이 두 번째 방법보다 더 적합할 수 있다.

5.4.2.1 프로그램 전달 전의 라이센스 취득 방식

그림 3은 MPD의 ContentProtection 서술자(descriptor)가 CDM에 라이센스 서버의 URL 및 기본 KID와 같은 제휴 메타 데이터를 제공하는데 사용되는 방법을 설명하는 메시지 처리 흐름의 한 예이다. 이는 CDM이 미디어 전달에 앞서 DRM 라이센스 및 관련 키 자료를 요청하고 획득하도록 한다. 암호화된 미디어 콘텐츠가 나중에 방송되면 수신기는 콘텐츠를 즉시 렌더링하기 위해 필요한 해독 키를 갖는다.

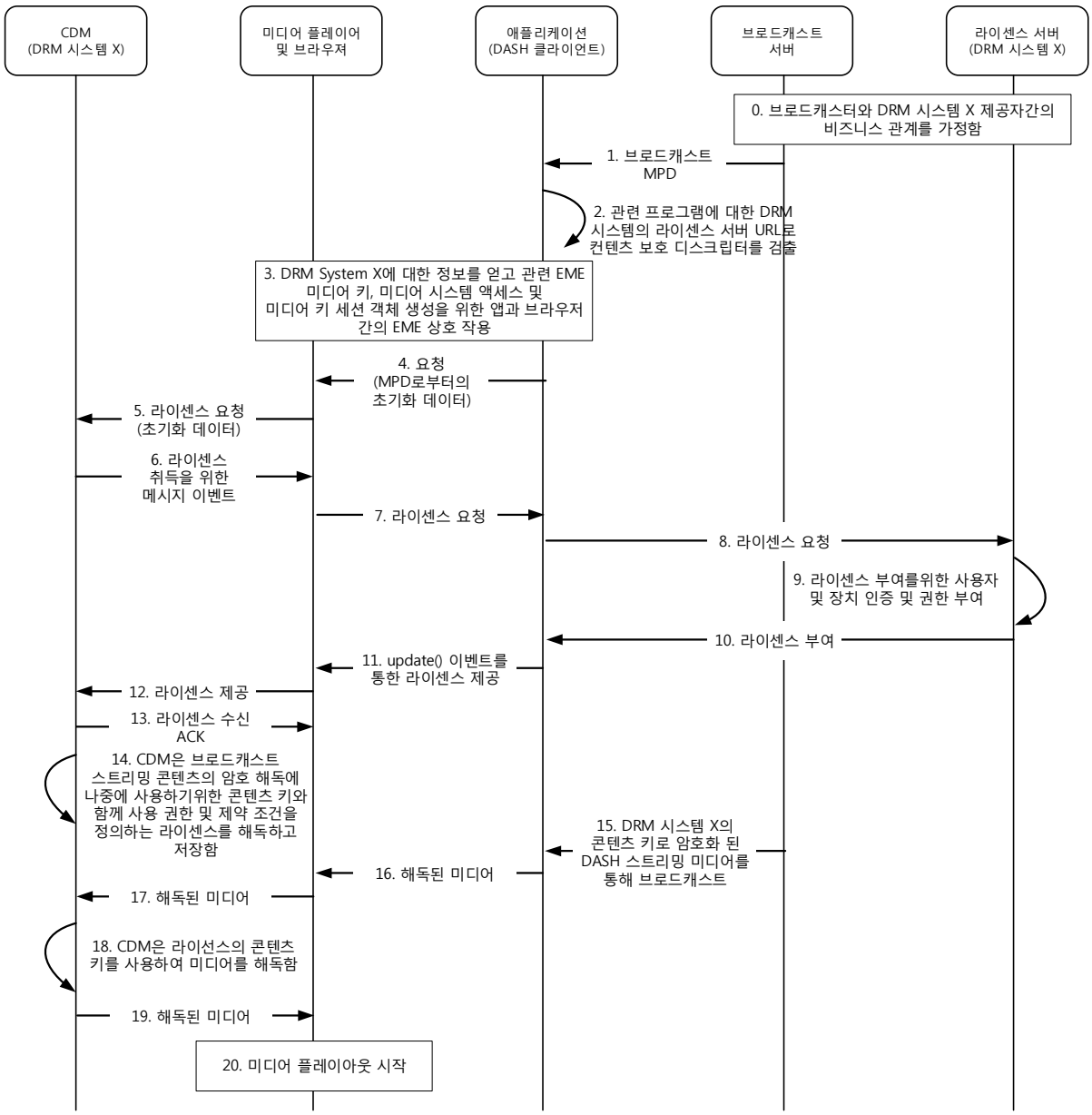

그림 3 DASH에서 프로그램 시작 전에 DRM 라이센스 및 키 획득 과정

5.4.2.2 프로그램 전달 동안의 라이선스 취득 방식

그림 4는 DASH Segments에 저장된 보호 시스템 관련 메타 데이터, 특히 'moov' 또는 'moof' 박스의 'pssh' 박스를 사용하여 라이센스 서버의 URL 및 CDM에 대한 기본 KID와 같은 제휴 메타 데이터를 제공하는 방법을 설명하는 메시지 처리 흐름의 예이다. CDM이 DRM 라이센스 및 관련 키 자료를 요청하고 획득하는데 걸리는 시간 동안에는 프로그램을 렌더링할 수 없다. 이 방법과 관련된 start-up 지연이 더 크기 때문에 5.4.1.1 절의 대체 방법이 방송 사업자에 의해 채택될 것을 제안한다.

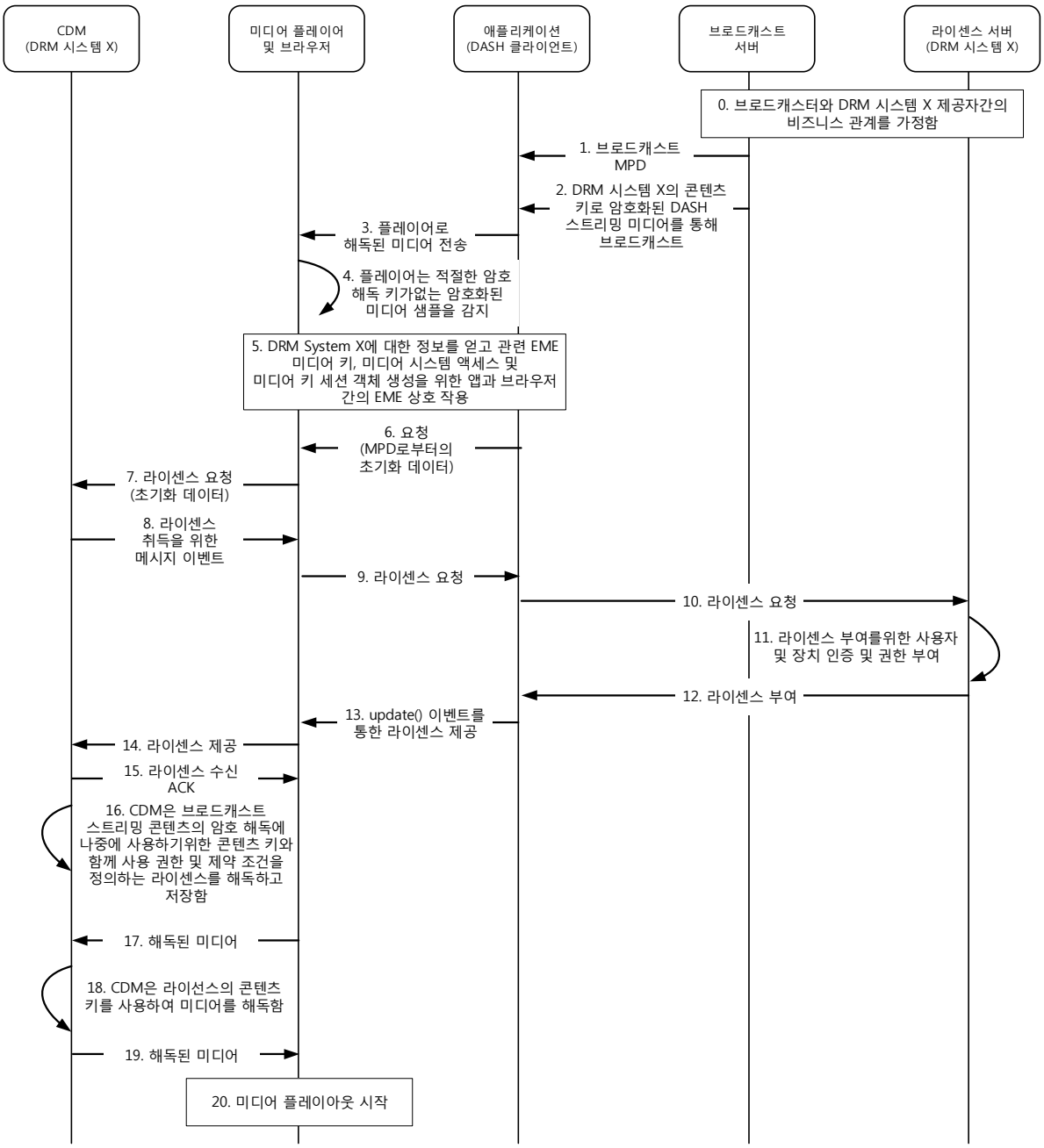

그림 4 DASH에서 프로그램 전달 동안의 DRM 라이센스 및 키 획득 과정

5.4.3 DRM과 CENC를 위한 프레임워크 솔루션

ISO-BM 23001-7은 ISO BMFF와 함께 Common Encryption에 대한 규범적 표준을 나타내며, DASH에 의해 수반되는 스트리밍 미디어의 DRM 보호에 사용되는 다음의 기술 요소를 포함하고 있다.

- AES-128 CTR 모드를 사용하는 NAL 구조 비디오 및 기타 미디어의 CENC
- 다수의 DRM 시스템에 의한 개별 표현의 암호 해독 지원
- 시간 경과에 따른 콘텐츠 암호화 키의 변경을 가능하게 하는 키 순환

- MPD에서 default_KID 및 'pssh' 매개 변수의 신호를 활성화하는 ContentProtection 서술자(descriptor)의 확장

DASH에서 사용할 수 있는 주요 DRM 관련 신호 구성 요소 및 도구는 다음과 같다:

1) 일반 암호화 또는 특정 DRM 방식의 사용 시그널링에 대한 URI를 포함하는 MPD의 ContentProtection 서술자(descriptor)가 사용된다.

2) 암호화 매개 변수 및 default_KID를 지정하는 초기화 세그먼트의 무비 박스('moov')에서 보호 체계 정보의 일부로 전달되는 'tenc' 박스의 매개 변수이다. default_KID 정보는 MPD에서 대역 외 (out-of-band)로 수행될 수 도 있다.

3) 적용 가능한 경우, 초기화 벡터와 하위 샘플 암호화 범위의 형태로 Common Encryption 샘플 보조 정보의 시그널링에 ISO / IEC 23001-7에서 정의된 'senc' 박스를 사용하거나 SampleAuxiliaryInformationSizesBox ('saiz')와 SampleAuxiliaryInformationOffsetsBox ('saio')를 통한다.

4) 보호 시스템에 특정한 형식으로 각 DRM 시스템에 대한 'pssh' 라이센스 취득 데이터 또는 키. 'pssh'는 ISO / IEC 23001-7에 정의된 보호 시스템 특정 헤더 박스를 나타내며 초기화 세그먼트 또는 미디어 세그먼트에 저장될 수 있다. 또한 MPD의 cenc:pssh 요소에 있을 수도 있다. MPD에 cenc:pssh 정보가 있으면 MPD 크기가 증가하지만 내용을 수정하지 않고도 더 빠른 파싱(parsing), 초기 액세스 및 DRM 시스템 추가가 가능할 수 있다.

5) 연속 라이브 콘텐츠에 액세스할 수 있는 권한을 시간 경과에 따라 수정할 수 있도록 하는 키 순환.

VoD (주문형 비디오) 콘텐츠에 대한 암호화 메타 데이터 지원과 관련된 박스 구조의 그래픽 표현이 그림 5에 나와 있다.

그림 5 단일 키로 VoD 콘텐츠를 보호하기위한 CENC 관련 메타 데이터 구조

실시간 스트리밍 콘텐츠에 대한 암호화 메타 데이터 지원과 관련된 박스 구조의 그래픽 표현이 그림 6에 나와 있다.

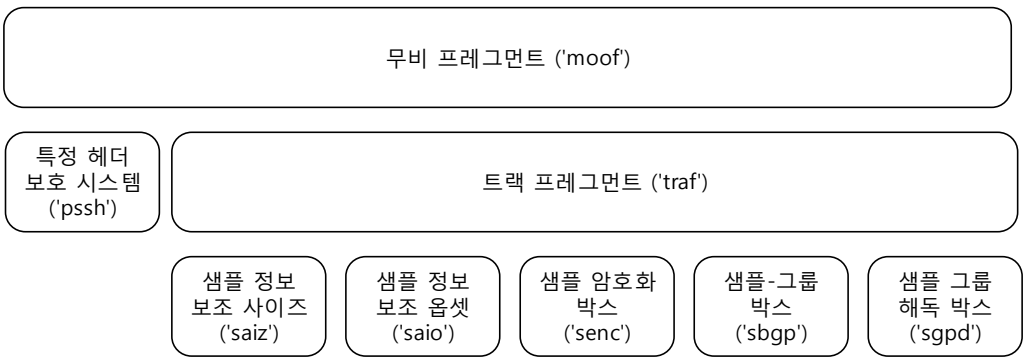

그림 6 실시간 스트리밍 콘텐츠 보호를 위한 CENC 관련 메타 데이터 구조

5.4.4. 암호화를 위한 MPD 지원과 DRM 시그널링

MPD는 DRM 클라이언트가 콘텐츠를 재생할 수 있는지 여부를 결정할 수 있게 하는데

사용되는 콘텐츠 암호화 및 키 관리 방법에 대한 신호를 포함한다. 그 정보는 ContentProtection 서술자(descriptor)에 포함되며, 적어도 단일 인스턴스가 암호화 된 내용을 설명하는 각 AdaptationSet 요소에 있어야 한다.

5.4.4.1 mp4 보호 방식을 위한 콘텐츠 보호 서술자(descriptor)의 사용

MPEG-DASH에 명시된 바와 같이 @schemeIdUri 값이 "urn:mpeg:dash:mp4protection:2011" 인 ContentProtection 서술자(descriptor)는 내용이 @value 속성과 같은 스키마로 암호화 되었음을 나타낸다. 콘텐츠 보호 체계의 파일 구조는 MPEG-DASH 5.8.5.2절에 명시되어 있으며 @value는 CENC 방식임을 의미하는 'cenc'이다. "urn:mpeg:cenc:2013" 확장 네임 스페이스 내에 정의된 대로 @cenc:default_KID 와 함께 ContentProtection 서술자(descriptor)의 @schemeIdUri 값은 수신자가 DRM Adaptation Set을 해독하는데 사용되는 라이센스를 얻거나 이전에 획득한 라이센스를 식별하기에 충분할 수 있다.

@cenc : default_KID가 각 Adaptation Set에 대해 존재하면 플레이어는 default_KID를 서로 비교하고 저장된 라이센스의 default_KID와 비교하여 각 Adaptation Set에 대해 새 라이센스를 얻어야 하는지에 대한 여부를 결정할 수 있다. 플레이어는 단순히 이 KID 문자열을 비교하고 각 DRM 시스템에 특정한 라이센스 정보를 해석하지 않고도 필요한 고유 라이센스를 결정할 수 있다.

5.4.4.2 uuid 방식을 위한 콘텐츠 보호 서술자(descriptor)의 사용

MPD 내의 UUID ContentProtection 서술자(descriptor)는 라이센스 취득을 위한 특정 DRM 체계의 이용 가능성을 나타낼 수 있다.

다음은 그 예이다:

```
<ContentProtection
schemeIdUri="urn:uuid:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
value="DRMNAME version"/>
```

schemeIdUri 는 특정 DRM 시스템에 대해 등록된 시스템 ID와 동일한 UUID 문자열을 갖는 UUID URN을 사용한다. 이는 MPEG DASH 5.8.5.2 절에 명시되어있다. 알려진 DRM 시스템 ID 목록은 DASH ID 저장소에서 찾을 수 있다.

5.4.4.3 MPD의 보호 시스템 특정 헤더 박스

'pssh' 박스는 등록된 시스템 ID와 함께 사용하기 위해 각 DRM 시스템에 의해 정의되며 무비 박스 ('moov')에 명목상 저장되며 무비 프래그먼트(fragment) 박스 ('moof')에 추가될 수 있다.

같은 박스는 ISO / IEC 23001-7에 정의된 "urn:mpeg:cenc: 2013" 네임 스페이스의 확장 요소 cenc:pssh를 사용하여 UUID 방식에 대한 ContentProtection 서술자 (descriptor) 내의 MPD에 저장할 수 있다. MPC에서 동일한 "urn:mpeg:cenc: 2013" 확장 네임 스페이스에 정의된 대로 cenc:pssh 요소와 cenc:default_KID 특성을 전달하는 것은 라이브 콘텐츠에 대한 초기화 세그먼트의 이용 시 키 식별과 라이센스 평가 및 라이센스 검색을 지원하는데 유용하다. 이를 통해 광대역 네트워크를 통해 IMCP 수신자가 프로그램 시작 전에 라이센스 요청을 취득할 수 있다. 또한 시간이 지남에 따라 라이센스 요청이 확산되면 'pssh'의 라이센스 획득 정보가 포함된 초기화 세그먼트에서 시작할 때 많은 시청자가 동시에 라이센스 요청을 함으로써 라이센스 서버가 과부하 되는 현상을 방지 할 수 있다. 각 Adaptation Set에 대한 mp4protection ContentProtection 서술자(descriptor)에 표시된 cenc:default_KID를 사용하면 수신자의 DRM 클라이언트가 다음을 결정할 수 있다:

- 프로그램에 대한 관련된 해독 키는 구매 또는 가입 없이 시청자가 이용할 수 있으며,
- 키가 이미 다운로드 된 경우
- 선택된 각 Adaptation Set 요소의 default_KID에 기반하여 클라이언트가 프로그램의 @availabilityStartTime 전에 다운로드해야 하는 라이선스.

5.5 방송 전용 장치를 위한 DRM 라이선스 및 키 전송 (DRM License and Key Delivery for Broadcast-Only Devices)

본 표준에서 CENC 및 EME 메커니즘을 기반으로 하는 DRM으로 보호된 서비스 및 콘텐츠는 광대역 지원 장치에서만 사용할 수 있다. 다시 말해, 수신기는 DRM으로 보호되는 서비스 및 프로그램을 표시하기 위해 콘텐츠 해독을 가능하게 하는 DRM 라이센스 및 키를 얻기 위해 광대역 네트워크에 액세스할 수 있어야 한다.

본 표준은 브로드밴드 네트워크에 대한 액세스 권한이 없는 방송 전용 장치가 DRM 기술을 사용하여 콘텐츠가 보호된 프로그램에 액세스 할 수 있는 기술에 대해서는 설명하지 않는다.

본 표준의 향후 개정판에서는 브로드밴드 네트워크에 대한 액세스 권한이 없는 방송 전용 장치가 DRM 보호 콘텐츠에 액세스할 수 있도록 지원할 수도 있다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

‘해당 사항 없음’

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

‘해당 사항 없음’

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 관련 국내 표준

본 표준의 연계(family) 표준은 다음과 같다:

- NGBF-STD-017, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 유스케이스 및 요구사항”, 2016
- FBMF-STD-002, “IP 기반 방송 환경에서 멀티 CA/DRM 콘텐츠 보호 시스템 아키텍처”, 2017

상기 표준은 본 표준에서 다루고 있는 IMCP 시스템의 유스케이스와 요구사항 및 아키텍처를 정의하고 있다.

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] IEEE: “Use of the International Systems of Units (SI): The Modern Metric System,” Doc. SI 10, Institute of Electrical and Electronics Engineers, New York, N.Y.

[2] ISO/IEC: ISO/IEC 23001-7 Second edition 2015-04-01, “Information technology —MPEG systems technologies —Part 17: Common encryption in ISO base media file format files.”

[3] ISO/IEC: ISO/IEC 14496-12 Fourth edition 2012-07-15 Corrected version 2012-09-15, “Information technology — Coding of audio-visual objects — Part 12: ISO base media file format.”

[4] W3C: “Encrypted Media Extensions,” W3C Editor’s Draft 03 September 2015, World Wide Web Consortium, https://w3c.github.io/encrypted-media/.

[5] ATSC: “ATSC Mobile DTV Standard, Part 6 - Service Protection,” A/153 Part 6:2011, Advanced Television Systems Committee, Washington, D.C., 23 May 2011.

[6] W3C: “Media Source Extensions”, W3C Editor’s Draft 14 July 2015, World Wide Web Consortium, https://w3c.github.io/media-source/.

[7] ISO/IEC: “ISO/IEC 23009-1:2014, Information technology —Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats,” International Organization for Standardization, Geneva, 2nd Edition, 15 May 2014.

[8] DASH: “Guidelines for Implementation: DASH-IF Interoperability Points”, Version 4.0, DASH Industry Forum, Beaverton, OR, 12 December 2016.

[9] DASH: “Guidelines for Implementation: DASH-IF Interoperability Points for ATSC 3.0”, Version 1.0, DASH Industry Forum, Beaverton, OR, 31 January 2017.

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

‘해당 사항 없음’

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2017.06.15	제정 FBMF-STD-004	-	UHDTV분과위원회
오류정정				
오류정정				
제2판				