NGBF Standard

차세대방송표준포럼표준(국문표준)

NGBF-STD-009 **제정일: 2016년 3월 30일**

지상파 UHDTV 방송 송수신 정합

- 파트 5. 콘텐츠보호

Transmission and Reception for Terrestrial UHDTV Broadcasting Service -

- Part 1. Content Protection

차세대방송표준포럼단체표준(국문표준)

NGBF-STD-009

제정일: 2016 년 3 월 30 일

지상파 UHDTV 방송 송수신 정합
- 파트 5. 콘텐츠보호

Transmission and Reception for Terrestrial UHDTV Broadcasting Service
- Part 5. Content Protection

서 문

1. 표준의 목적

본 표준은 지상파 UHDTV 방송 콘텐츠의 불법 녹화 및 유통 방지를 위한 지상파 UHDTV 방송 콘텐츠 암호화 방법, 보호 시그널링, 보호 시스템에 대한 송수신 정합 규격을 정의하며, 지상파 UHDTV 방송 콘텐츠 보호를 위해 보호 시스템을 운영하는 자와 보호된 UHDTV 방송 콘텐츠를 수신하여 정상적으로 처리하려는 수신기를 제작하는 자에게 필요한 기술 규격 제공을 목적으로 한다.

2. 주요 내용 요약

본 표준은 지상파 UHDTV 방송 송수신 시스템에 대한 규격 사항으로, 지상파 UHDTV 방송 콘텐츠 암호화 적용을 위한 공통 암호화 방식을 정의하며 보호된 방송 콘텐츠의 암호화 여부 및 방법을 표시하는 시그널링과 UHDCP 시스템의 메시지 전송 방법에 대해 기술한다. 또한 수신기에서 수신한 지상파 UHDTV 방송프로그램의 배포 조건 정보와 수신기 외부 출력 시 포함되어야 하는 포렌식 워터마킹 정보에 대해 기술한다. 그리고 송신 측에서 방송 콘텐츠 보호를 목적으로 하는 구성 시스템 간 연동 인터페이스 규격과 UHDCP 시스템을 교환하기 위한 다운로드 플랫폼 규격에 대해 기술한다.

3. 표준의 이력 정보

3.1. 표준의 이력

판수	제정·개정일	제정·개정 내역
제 1 판	2016.03.30.	제정 NGBF-STD-009

3.2. 주요 개정 사항

해당 없음

목 차

지상파 UHDTV 방송 송수신 정합 – 파트 5. 콘텐츠보호

1. 개요

본 표준은 지상파 UHDTV 방송 서비스를 제공하는데 필요한 송수신 정합 규격 중 콘텐츠보호 규격을 정의하기 위해 제정되었다.

2. 표준의 구성 및 범위

본 표준은 지상파 UHDTV 방송 콘텐츠의 불법 녹화 및 유통 방지를 위한 지상파 UHDTV 방송 콘텐츠 보호시스템(이하 보호시스템이라 명명) 표준을 포함한다. 본 표준은 6장 지상파 UHDTV 방송 콘텐츠 보호 요구사항을 만족하기 위한 기술 표준을 포함하고 있다.

본 표준은 7장에서 지상파 UHDTV 콘텐츠 공통 암호화 방법을, 8장에서 암호화 시그널링 표준을, UHDCP 시스템 메시지 전송 방법 및 UHDCP/DP 시그널링 표준을, 9장에서 UHDTV 콘텐츠 관리를 위한 Content Management Information 표준을, 10장에서 지상파 UHDTV 송신 시스템에서의 구성 시스템 간 연동 인터페이스 표준을, 11장에서 다운로드 플랫폼 표준을, 그리고 12장에서 지상파 UHDTV 수신기 외부 출력 시 포함되어야 하는 포렌식 워터마킹 정보 정의를 각각 기술한다.

3. 참조 표준(권고)

[1] ISO/IEC 23001-7 Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files (2nd Edition)

[2] ETSI TS 103 197 V1.5.1 (2008-10) Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt

[3] ISO/IEC 14496-12 Information technology – Coding of audio-visual objects – Part 12: ISO base media file format (4th Edition)

[4] 차세대방송표준포럼단체표준, "지상파 UHDTV 방송 송수신 정합 - 파트 2. 컴포넌트", NGBFK-16.xxxx/R1, 2016.

[5] 차세대방송표준포럼단체표준, "지상파 UHDTV 방송 송수신 정합 - 파트 3. 시스템즈", NGBFK-16.xxxx/R1, 2016.

[6] TTA 정보통신단체표준, IPTV 용 교환 가능한 CAS (iCAS), TTAK.08-0023/R2, 2011년 9월 28일

[7] NIST FIPS 800-38A Recommendation for Block Cipher Modes of Operation – Methods and Techniques

[8] ISO/IEC: ISO/IEC 23008-1:2015, "Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 1: MPEG media transport (MMT)," International Organization for Standardization, 2nd Edition, mm/dd/yy (publication expected 2016)

[9] W3C XML Signature Syntax and Processing Version 1.1, W3C Recommendation 11 April 2013

4. 용어 정의 및 약어

4.1 용어 정의

UHDCP 시스템: 보호된 방송 콘텐츠를 합당한 시청 요건을 갖춘 수신기만 정상적으로 접근할 수 있도록 키 관리 등의 접근 제어 메커니즘을 제공하는 시스템이다.

UHDCP 시스템 메시지: 접근 제어 목적을 위해 UHDCP 시스템이 생성하는 메시지이다.

UHDCP 시스템 식별자: 특정 UHDCP 시스템을 유일하게 식별하기 위한 값으로 UUID 형태를 갖는다.

UHDCP 클라이언트: UHDCP 시스템 메시지를 수신하여 이에 따라 보호된 방송 콘텐츠에 대한 접근 제어를 수행하는 수신기 모듈이다.

ISOBMFF Segment: ROUTE로 전달되는 DASH Segment 파일 또는 MMTP로 전달되는 MPU를 의미한다.

공통 암호화 방식: 암호화 및 키 맵핑 방식을 표준으로 정의한 것으로 서로 다른 UHDCP 시스템을 이용하여 동일한 파일을 복호화 하는 것이 가능하도록 하는 방식이다.

Key Rotation: 접근 제어 변경 또는 보안 목적으로 암호화 키를 변경하는 것을 의미한다.

Content Management Information: 수신기에서 수신한 지상파 UHDTV 방송프로그램의 배포 조건 정보를 나타낸다.

SimulCrypt: 서버에서 복수 UHDCP 시스템을 동시에 운영하기 위해 관련 방송 시스템 간 메시지 프로토콜 및 동기화 메커니즘을 정의하는 표준이다.

다운로드 플랫폼: 운영 중인 UHDCP 시스템을 다른 UHDCP 시스템으로 안전하게 변경하기 위한 시스템으로 수신기에 설치된 UHDCP 클라이언트 및 DP Manager를 변경할 수 있도록 안전한 이미지 다운로드, 설치, 운영 메커니즘을 제공한다.

DP Message: 다운로드 플랫폼에서 운영하는 UHDCP 시스템의 버전 정보, UHDCP 클라이언트 및 DP Manager 이미지의 전달 위치 정보, CA Token 및 CA Token

Revocation의 전달 위치 정보 등을 포함한 메시지이다.

DP Manager: DP Message를 수신하여 UHDCP 클라이언트 및 DP Manager 업데이트를 판단하고 업데이트 필요 시 이미지 다운로드, 설치, 운영을 수행하는 수신기 모듈이다.

CA Token: 수신기의 콘텐츠 시청 권한을 확인하기 위한 것으로 UHDCP 클라이언트 이미지 다운로드를 위한 증명 값으로 사용된다.

CA Token Revocation List: 폐기할 CA Token에 대한 식별자 리스트를 포함하는 메시지이다.

포렌식 워터마킹: 방송 콘텐츠에 대한 소유권자 정보 뿐만 아니라 수신자의 정보를 방송 콘텐츠에 삽입하는 기술이다.

4.2 약어

AES Advanced Encryption Standard

ATSC Advanced Television Systems Committee

CA Certificate Authority

CAS Conditional Access System

CENC Common Encryption

CMI Content Management Information

CPT Content Protection Table

CTR Counter

CTRL CA Token Revocation List

CW Control Word

DASH Dynamic Adaptive Streaming over HTTP

DP Download Platform

DPM Download Platform Message

DRM Digital Rights Management

DVB Digital Video Broadcasting

ECM Entitlement Control Message

ECMG ECM Genenator

EMM Entitlement Management Message

EMMG EMM Generator

HDCP High-bandwidth Digital Copy Protection

HTTP Hypertext Transfer Protocol

iCAS IPTV Interchangeable CAS

ISOBMFF ISO Base Media File Format

KID Key Identifier

LCT Layered Coding Transport

LLS Low Level Signaling

LS License Signaling

MMT MPEG Media Transport

MMTP MPEG Media Transport Protocol

MPD Media Presentation Description

MPU Media Processing Unit

NAL Network Abstraction Layer

PLP Physical Layer Pipe

ROUTE Real-time Object Delivery over Unidirectional Transport

SCS SimulCrypt Synchronizer

SLS Service Layer Signaling

SLT Service List Table

TOI Transport Object ID

TSI Transport Session ID

UHDCP UHD Content Protection

URL Uniform Resource Locator

USBD User Service Bundle Description

UUID Universally Unique Identifier

XML eXtensible Markup Language

5. 지상파 UHDTV 방송 콘텐츠 보호시스템 개요

본 5장은 표준의 이해를 돕기 위해 제공되며 표준에는 포함되지 않는다.

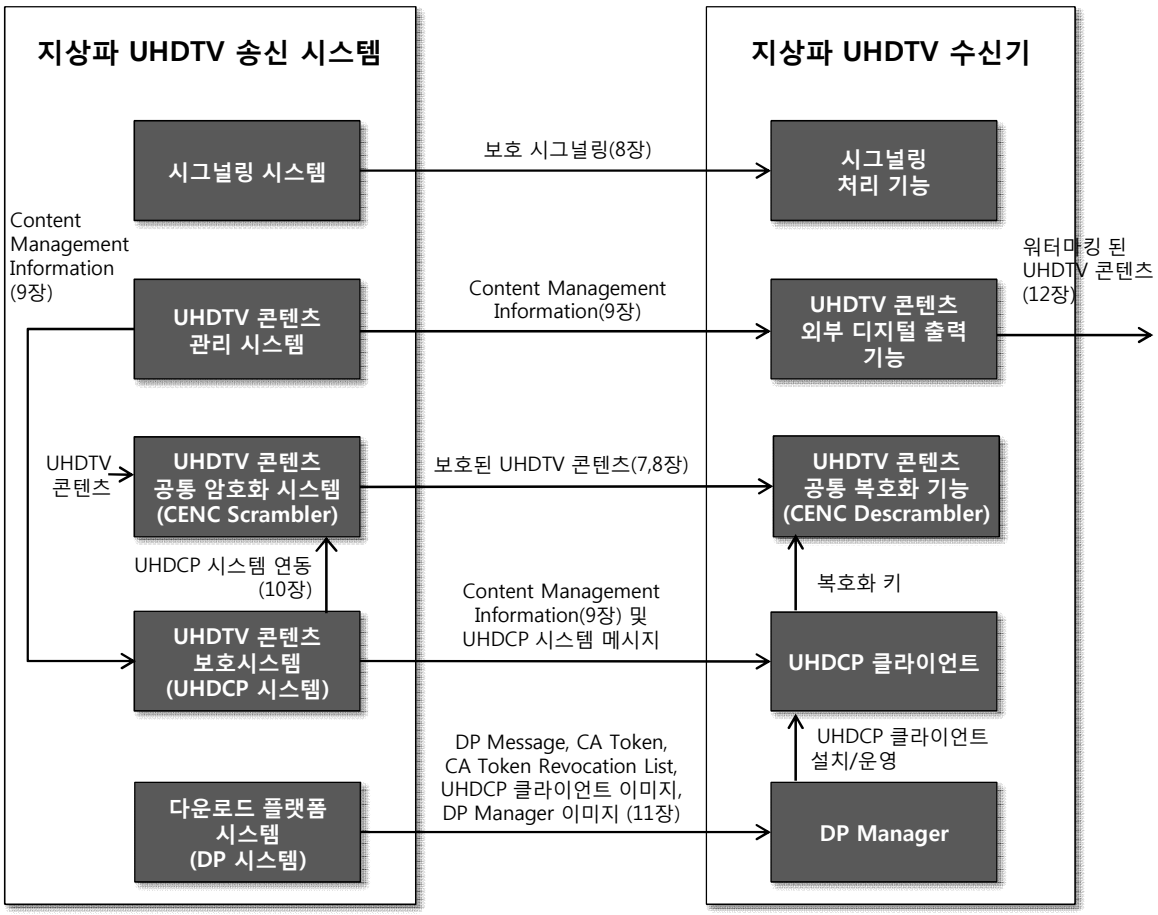

그림 5-1. 지상파 UHDTV 방송 콘텐츠 보호 표준 구성 요소

그림 5-1은 보호시스템의 서브 시스템인 지상파 UHDCP 송신 시스템 및 수신기에서의 각각의 표준 구성 요소를 나타낸다. 각 구성 요소에 대한 설명은 다음과 같다.

- **시그널링 시스템 및 시그널링 처리 기능**
  지상파 UHDTV 방송 콘텐츠 보호를 위해 운영하는 UHDCP 콘텐츠 보호시스템(UHDCP 시스템) 및 다운로드 플랫폼 시스템(DP 시스템)에 대한 시그널링 정보(예를 들어 각 시스템 식별자, 각 시스템의 데이터 전달 위치 정보 등)를 전달 및 처리하는 기능을 각각 담당한다.

- **UHDTV 콘텐츠 관리 시스템 및 UHDTV 콘텐츠 외부 디지털 출력 기능**
  지상파 UHDTV 방송 콘텐츠의 디지털 외부 출력 시 콘텐츠 복사 제어를 위한

Content Management Information 생성 및 전달, 그리고 이 정보에 따른 수신기에서의 외부 디지털 출력 제어를 담당한다. 외부 디지털 출력 시 본 표준에서 정의한 포렌식 워터마킹 정보가 UHDTV 방송 콘텐츠에 포함된다.

- **UHDTV 콘텐츠 공통 암호화 시스템(CENC Scrambler) 및 UHDTV 콘텐츠 공통 복호화 기능(CENC Descrambler)**

  불법 유통을 목적으로 지상파 UHDTV 방송 콘텐츠에 접근하는 것을 원천적으로 차단하기 위해 UHDCP 시스템 독립적인 공통 암호화 방식으로 지상파 UHDTV 방송 콘텐츠를 암호화 하고 역으로 수신기에서의 복호화 기능을 담당한다. 보호된 지상파 UHDTV 콘텐츠에는 암호화 된 콘텐츠 뿐만 아니라 암호화 여부, 암호화 알고리즘 식별자, 암호화 키 식별자 등과 같은 콘텐츠 암호화 시그널링 정보가 포함된다.

- **UHDTV 콘텐츠 보호시스템(UHDCP 시스템) 및 UHDCP 클라이언트**

  UHDTV 방송 콘텐츠를 암호화 하기 위한 다양한 보안 키 관리(발급, 갱신, 폐지 등) 등을 수행하는 시스템과 이에 대응하는 수신기에서의 클라이언트 기능이다. 송신 시스템에는 하나 이상의 UHDCP 시스템을 운영할 수 있으며 CENC Scrambler와의 연동을 위해 표준 인터페이스를 이용한다. 본 표준에서는 UHDCP 시스템에 대한 표준을 포함하지 않는다.

- **다운로드 플랫폼 시스템(DP 시스템) 및 DP Manager**

  수신기에서 동작하는 UHDCP 클라이언트 이미지 및 DP Manager 이미지에 대한 다운로드, 설치, 운영을 위한 시스템으로, 본 표준에서는 현재 운영하고 있는 UHDCP 시스템 및 DP 시스템에 대한 정보를 포함하는 DP Message, CA Token, CA Token Revocation List, UHDCP 클라이언트 이미지, DP Manager 이미지에 대한 포맷 및 전송 프로토콜에 대한 표준을 포함한다.

6. 지상파 UHDTV 방송 콘텐츠 보호 요구사항

본 장에서는 지상파 UHDTV 방송 콘텐츠 보호를 위한 서비스 및 시스템 요구사항에 대해 기술한다.

6.1 서비스 요구사항

(의미) 콘텐츠 보호란 지상파 방송사에서 제공하는 방송 콘텐츠를 합당한 시청 요건을 갖춘 수신 단말에만 정상적인 서비스가 되도록 하는 기능을 말한다.

6.2 시스템 요구사항

6.2.1 콘텐츠 스크램블링

순번	요구사항
1.1	높은 수준의 콘텐츠 기밀성(Confidentiality)을 제공하기 위해 보안성이 높은 표준화된 암호화 알고리즘을 이용하여 콘텐츠를 암호화 해야 한다.
1.2	방송 시그널링을 통해 해당 채널에 대한 보호 여부를 표시해야 하며 특정 콘텐츠 전송 단위에서의 스크램블링 여부, 키 식별자를 표시할 수 있어야 한다.

6.2.2 콘텐츠 보호 관리

순번	요구사항
2.1	각 방송사는 하나 이상의 콘텐츠 보호 관리 시스템을 동시에 운영할 수 있어야 한다.
2.2	콘텐츠 보호 관리 시스템은 유일하게 식별 가능해야 한다.
2.3	방송 시그널링에 해당 채널에서 사용하는 콘텐츠 보호 관리 시스템에 대한 식별자가 포함되어야 한다.
2.4	UHD 방송 서비스 운영 중에 콘텐츠 보호 관리 시스템을 다른 시스템으로 안전하게 변경할 수 있어야 하며 이를 위한 다운로드 플랫폼을 제공해야 한다.

2.5	다운로드 플랫폼은 TV 수신기 모델 별, 특정 수신기 별로 콘텐츠 보호 관리 시스템 클라이언트의 안전한 다운로드 및 설치, 운영 기능을 제공해야 한다.
2.6	콘텐츠 보호 관리 시스템이 변경되더라도 기존 수신기에 대한 하위 호환성이 보장되어야 한다.

6.2.3 콘텐츠 사용 제어

순번	요구사항
3.1	UHD 방송 콘텐츠의 녹화/재생/이동/복사를 허용하기 위한 이용 제어 정보가 UHD 방송 콘텐츠와 함께 전송되어야 하며 정보에 대한 무결성을 보장해야 한다.
3.2	채널 별, 콘텐츠 별로 이용 제어 권한을 설정할 수 있어야 한다.
3.3	수신기는 저장된 UHD 콘텐츠 재생 시 이용 제어 정보에 따라 재생 제어를 해야 한다.
3.4	사적 이용을 위해 2차 단말기로 UHD 콘텐츠 이동/복사 시 이용 제어 정보에 따라 콘텐츠의 이동/복사를 제어해야 한다.
3.5	디지털 외부 출력 보호를 위해 HDCP(High-bandwidth Digital Copy Protection) 2.2 이상이 지원되어야 한다.

6.2.4 포렌식 워터마크 삽입

순번	요구사항
4.1	UHD 콘텐츠 외부 디지털 출력 시 포렌식 워터마크가 삽입되어 출력되어야 한다.

7. 지상파 UHDTV 콘텐츠 공통 암호화 방식

본 장에서는 지상파 UHDTV 콘텐츠 보호를 위한 공통 암호화 방식에 대해 기술한다.

지상파 UHDTV 시스템에서는 미디어 콘텐츠의 전송 컨테이너 형식을 ISOBMFF (ISO Base Media File Format)[3]를 기반으로 하고 있기 때문에 본 표준에서는 ISOBMFF Segment[1] 수준에서의 보호를 위한 공통 암호화 방식에 대해 다룬다. ISOBMFF Segment가 아닌 다른 전송 컨테이너 형식 또는 전송 레벨에 대한 보호는 본 표준에서 다루지 않는다.

기본적으로 ISOBMFF Segment에 대한 공통 암호화 방식은 표준 [1]을 기반으로 한다. 본 표준에서는 이 표준을 CENC 표준이라고 부른다.

7.1 CENC 적용 규칙

본 절에서는 지상파 UHDTV 콘텐츠 보호를 위해 CENC 적용 시 준수해야 하는 몇 가지 규칙에 대해 기술한다.

7.1.1 Protection Scheme

ISOBMFF Segment는 CENC 표준[1] 10장에서 정의하는 'cenc' Protection Scheme (AES 128 bits Counter Mode)을 이용하여 보호해야 한다. 이에 따라 CENC 표준[1] 5장에서 설명하는 바와 같이 Protection Scheme 시그널링을 위해 ISOBMFF Segment의 Scheme Type Box ('schm')의 scheme_type 필드는 'cenc'로 지정되어야 한다. CENC 표준[1] 11장에서 정의하는 'cbc1' Protection Scheme은 이용하지 않는다.

그리고 CENC 표준[1] 10.6.2절에서 명시한 바와 같이 NAL 구조의 비디오 샘플 암호화 시 부샘플 암호화(Subsample Encryption) 이용해야 한다.

[1] 본 표준에서는 설명의 용이성을 위해 ROUTE로 전달되는 DASH Segment 파일과 MMTP로 전달되는 MPU를 통칭하여 ISOBMFF Segment라고 부른다.

7.1.2 상호 교환 가능한 서로 다른 미디어 표현에 대한 암호화

DASH의 경우 Adaptation Set 내 모든 Representation들은 동일한 암호화 키와 권한 정보(Rights 또는 License)에 의해 보호되도록 해야 한다. 이에 따라 Adaptation Set에 속하는 모든 Representation들에 대해, 각 Representations에 해당하는 Track Encryption Box ('tenc')의 default_KID는 모두 같은 값을 가져야 한다. 그리고 MPD 내에서 <ContentProtection> Descriptor는 Representation 수준이 아닌 Adaptation Set 수준에 포함되어야 한다.

이러한 제약 사항은 네트워크 대역폭 변경에 의한 Adaptive Streaming 기능 또는 다른 목적의 서비스를 제공하기 위해, 수신기가 현재 수신하고 있는 Representation에서 같은 Adaptation Set에 포함된 다른 Representation으로 변경하여 서비스를 제공하려는 경우에 권한 정보 재확인(또는 획득) 및 복호화 키 재계산 등으로 인한 서비스 제공 단절 가능성을 방지하기 위해 사용된다. 만일 하나의 Adaptation Set 내에서 서로 다른 품질의 Representation에 대해 서로 다른 권한 정보에 의해 제어되도록 하고자 한다면 이 Representation들을 서로 다른 Adaptation Set에 포함되도록 구성하고 이 Adaptation Set에 대해 <ContentProtection> Descriptor를 포함시켜야 한다.

MMT 프로토콜에서도 상기와 같이 서로 다른 Asset 간의 서비스 제공 변경을 허용하는 경우 같은 암호화 키와 권한 정보에 의해 보호될 수 있도록 해야 한다.

7.1.3 샘플 암호화 키 및 초기화 벡터

하나의 ISOBMFF Segment 내 특정 Track의 모든 샘플은 동일한 암호화 키를 이용하여 암호화 해야 한다.

초기화 벡터의 이용은 문서 [7] Appendix B. Generation of Counter Blocks를 참조하여야 한다.

7.1.4 Key Rotation

실시간 방송 지상파 UHDTV 콘텐츠의 경우 접근 제어 변경 또는 보안 목적 상 샘플

암호화 키는 주기적으로 변경(Key Rotation)해야 한다. 본 규격에서는 특정한 암호화 키 변경 주기(Crypto Period)에 대해서 명시하지 않는다. 7.1.3절 관점에서 하나의 ISOBMFF Segment 내에서는 Key Rotation을 하지 않아야 한다.

8. 지상파 UHDTV 콘텐츠 보호 시그널링

본 장에서는 7장에서 설명한 공통 암호화 기술을 이용하여 지상파 UHDTV 방송 콘텐츠 보호 시 콘텐츠 암호화 시그널링과 콘텐츠 보호 관리 시스템(UHDCP 시스템) 및 다운로드 플랫폼 시스템(DP 시스템) 시그널링 방식에 대해 기술한다.

지상파 UHDTV 콘텐츠 보호 시그널링은 크게 1) 콘텐츠 암호화 시그널링과 2) UHDCP/DP 시스템 시그널링으로 구성된다. 콘텐츠 암호화 시그널링은 서비스 보호 여부, ISOBMFF Segment 암호화 시 사용되는 암호화 알고리즘 표시, 서비스 스트림 암호화 여부, 각 Sample의 암호화 여부, 암호화 부분 표시, 암호화 키 식별자 및 초기화 벡터(Initialization Vector)에 대한 시그널링을 다룬다. UHDCP/DP 시스템 시그널링은 UHDCP 시스템과 DP 시스템의 데이터 전달 방식 및 이 데이터 전달 위치에 대한 시그널링에 대해 다룬다.

8.1 콘텐츠 암호화 시그널링

UHDTV 방송 콘텐츠 암호화 시 전달해야 하는 콘텐츠 암호화 시그널링 항목 및 이의 방법은 표 8-1과 같다.

표 8-1. 콘텐츠 암호화 시그널링

시그널링 항목	시그널링 방법
서비스 보호 여부	■ LLS SLT에서 보호되는 서비스의 @protected를 이용한다.
서비스 보호를 위해 적용한 암호화 알고리즘 표시	■ ISOBMFF Segment 암호화 알고리즘 식별자 정보는 SLS MPD <ContentProtection> Descriptor 또는 ISOBMFF Segment의 Scheme Type Box ('schm')를 통해 시그널링 한다. ■ 미디어 전송 프로토콜(ROUTE 또는 MMTP)이 MPD를 사용하는 경우, 암호화를 적용하는 Adaptation Set 하위에 아래 예와 같이 하나의 <ContentProtection> descriptor가 반드시 포함되어야 한다.

시그널링 항목	시그널링 방법
	<ContentProtection schemeIdUri="urn:mpeg:dash:mp4protection:2011" value="cenc" cenc:default_KID="34e5db32-8625-47cd-ba06-68fca0655a72" /> ■ @cenc:default_KID는 선택사항이다. ■ CENC 표준[1]의 5장 Scheme Signaling에서 기술한 바와 같이 ISOBMFF Segment의 Protection Scheme Information Box ('sinf") 하위 Scheme Type Box ('schm')의 scheme_type 필드는 "cenc"로 표시하고 scheme_version 필드로 CENC 표준[1] 버전(0x0001 0000)을 표시한다. ■ MPD <ContentProtection> Descriptor와 ISOBMFF Segment에서의 암호화 알고리즘 표시 값은 반드시 동일해야 한다. ■ 상기 MPD <ContentProtection> Descriptor에서 @cenc:default_KID가 명시된다면 이 값은 CENC 표준[1] 9.2절에서 정의하는 Track Encryption Box ('tenc')의 default_KID 값과 동일하게 지정해야 한다.
서비스 스트림(Track) 암호화 여부 표시	■ 서비스 스트림(Track)에 암호화 적용 시 Sample Description Box에 있는 four-character-code(예: 'mp4v', 'mp4a', 'hvc1')는 암호화를 적용하였음을 표시하는 four-character-code(예: 'encv', 'enca')로 변경되어야 한다. 그리고 원본 sample entry type은 Original Format Box ('frma')에 저장되어야 한다. 이에 대한 세부적인 내용은 ISOBMFF 표준[3] 8.12절을 참고한다. ■ Sample Description Box의 four-character-code가 암호화 적용을 의미하는 경우 이에 해당하는 ISOBMFF Segment의 Sample Group Description Box에는 CENC 표준[1] 7장에 기술되어 있는 Sample Encryption Information Group Entry가 반드시 포함되어야

시그널링 항목	시그널링 방법
	한다.
ISOBMFF Segment 내 특정 Sample의 암호화 여부 및 암호화 부분 표시	■ CENC 표준[1] 7장에 기술되어 있는 IsEncrypted 필드를 이용하여 각 Sample의 암호화 여부를 표시한다. 세부적인 내용은 CENC 표준[1] 7장을 참고한다. ■ 참고로, 하나의 ISOBMFF Segment에 있는 Sample들 중 일부 Sample들은 암호화하고 일부 Sample들은 암호화 하지 않을 수 있다. ■ CENC 표준[1] 10장에서 Sample 암호화 시 Full Sample Encryption 또는 Subsample Encryption을 이용할 수 있다. 각 Sample의 암호화된 부분, 암호화 되지 않은 부분에 대한 표시 방법은 CENC 표준[1] 8장을 참고한다.
각 Sample 암호화 키 식별자(KID)	■ CENC 표준[1] 7장에 기술되어 있는 KID 필드를 이용하여 각 Sample의 암호화 키를 식별한다. 세부적인 내용은 CENC 표준[1] 7장을 참고한다.
각 Sample 암호화 시 사용하는 Initialization Vector	■ 각 Sample 암호화 시 사용하는 Initialization Vector는 CENC 표준[1] 8장에 기술되어 있는 InitializationVector 필드를 이용한다. ■ 각 Initialization Vector의 크기 정보는 CENC 표준[1] 7장에 기술되어 있는 IV_Size 필드를 이용한다.

8.2 UHDCP/DP 시스템 시그널링

본 절에서는 UHDCP/DP 시스템 시그널링 관련하여 UHDCP/DP 시스템 식별자 표시 방법, UHDCP/DP 시스템의 데이터 전달 방식 및 이 데이터 전달 위치에 대한 시그널링에 대해 다룬다.

8.2.1 UHDCP 시스템 식별자 표시 방법

UHDCP 시스템 식별자는 CENC 표준[1]에 따라 UUID 체계를 갖는다. 서비스 보호 시 적용한 UHDCP 시스템 식별자 정보 시그널링 방식은 다음과 같다.

- UHDCP 시스템 식별자 정보는 SLS를 통해 전달되는 MPD Adaptation Set 하위 <ContentProtection> Descriptor 또는 ISOBMFF Segment의 Movie Box ('moov') 또는 Movie Fragment Box ('moof') 하위 Protection System Specific Header Box ('pssh')를 통해 시그널링 한다.

  ✓ 각 서비스 범위에서 복수의 UHDCP 시스템이 적용될 수 있기 때문에 MPD Adaptation Set 하위에 복수의 <ContentProtection> Descriptor가 존재할 수 있다. 그리고 Movie Box 또는 Movie Fragment Box 하위에도 각 UHDCP 시스템 별로 다른 복수의 Protection System Specific Header Box가 존재할 수 있다.

- 미디어 전송 프로토콜(ROUTE 또는 MMTP)이 MPD를 사용하는 경우, MPD Adaptation Set 하위에는 각 UHDCP 시스템 별로 아래 예와 같이 <ContentProtection> descriptor가 반드시 포함되어야 한다.

```
<ContentProtection
    schemeIdUri="urn:uuid:d0ee2730-09b5-459f-8452-200e52b37567"
    value="Acme 2.0">
        <cenc:pssh>
            YmFzZTY0IGVuY29kZWQgY29udGVudHMgb2YgkXB
            zc2iSIGJveCB3aXRoIHRoaXMgU3lzdGVtSUQ=
        </cenc:pssh>
</ContentProtection>
```

  ✓ 상기 예는 하나의 UHDCP 시스템에 대한 시그널링 만을 포함하고 있으나 서비스 보호를 위해 적용한 UHDCP 시스템이 복수인 경우 상기 <ContentProtection> Descriptor는 복수 개 존재할 수 있다.

  ✓ @cenc:pssh는 선택 사항이다.

- CENC 표준[1] 9.1절에서 정의하는 Protection System Specific Header Box ('pssh')

는 ISOBMFF Segment의 Movie Box ('moov') 또는 Movie Fragment Box ('moof') 하위에 존재할 수 있다.

- ✓ 동일한 UHDCP 시스템에 대해 Movie Box에 'pssh'가 존재하고 이에 해당하는 MPD <ContentProtection> Descriptor 하위에 <cenc:pssh>가 존재하는 경우 'pssh'와 <cenc:pssh> 값은 동일해야 한다.
- ✓ MPD <ContentProtection> Descriptor 하위에 <cenc:pssh>가 존재하지 않지만 Movie Box 또는 Movie Fragment Box 하위에 'pssh'가 존재하는 경우는 허용한다.
- ✓ MPD <ContentProtection> Descriptor 하위에 <cenc:pssh>가 존재하지만 Movie Box 또는 Movie Fragment Box 하위에 'pssh'가 존재하지 않는 경우는 허용하지 않는다.
- ✓ Movie Box에 있는 'pssh'와 Movie Fragment Box에 있는 'pssh'의 내용은 다를 수 있다.
- ✓ Movie Box 또는 Movie Fragment Box에 있는 'pssh'의 내용이 시간이 지남에 따라 자주 변경 되는 경우 이 'pssh'의 내용이 MPD <ContentProtection> Descriptor 하위의 <cenc:pssh>로 삽입하지 않을 것을 권고한다.

8.2.2 DP 시스템 식별자 표시 방법

DP 시스템을 유일하게 식별하기 위한 식별자는 UUID 체계를 갖는다.

8.2.3 UHDCP/DP 시스템 시그널링

제한 수신 시스템(Conditional Access System) 형식의 UHDCP 시스템이 생성하는 데이터는 크게 ECM과 EMM으로 나뉜다. 일반적으로 ECM은 암호화 된 Control Word(콘텐츠 암호화 키)와 보호된 해당 서비스의 접근 제어 정보를 포함하고 EMM은 보호된 서비스에 접근을 허용하기 위한 권한 정보를 포함한다. 실시간 방송 서비스의 경우 일반적으로 ISOBMFF Segments의 암호화 키가 주기적으로 변경(Key Rotation)되기 때문에 ECM

또한 주기적으로 변경될 수 있다.

디지털 저작권 관리(Digital Rights Management) 형식의 UHDCP 시스템은 일반적으로 라이선스 메커니즘을 통해 보호된 서비스에 대한 접근 제어를 수행한다. 각 디지털 저작권 관리 기술마다 라이선스 구성 및 전달 방법은 다르나 일반적으로 라이선스에는 서비스 접근을 허용하기 위한 권한 정보와 암호화 콘텐츠를 복호화 하기 위한 키가 포함되고 암호화 된 콘텐츠에는 라이선스 발급을 위한 라이선스 발급 정보(예를 들어 라이선스 서버 URL, 암호화 콘텐츠 식별자 등)가 포함된다.

각 UHDCP 시스템이 전달하는 ECM 또는 라이선스 발급 정보의 전달 방식 및 이의 전달 위치 시그널링에 대한 설명은 다음과 같다.

- 제한 수신 시스템 방식의 ECM은 ISOBMFF Segment의 Movie Fragment Box ('moof') 하위 Protection System Specific Header Box ('pssh')의 Data 필드를 통해 전달한다. ECM은 'pssh' 자체가 아니라 'pssh'의 Data 필드에 해당함을 주의해야 한다. Protection System Specific Header Box에 대한 설명은 CENC 표준[1] 9장을 참조한다.

- 디지털 저작권 관리 방식에서 라이선스 발급 정보를 암호화 된 ISOBMFF Segment에 넣고자 하는 경우 이 라이선스 발급 정보는 ISOBMFF Segment의 Movie Box('moov') 또는 Movie Fragment Box('moof') 하위 Protection System Specific Header Box('pssh')의 Data 필드를 통해 전달한다. 라이선스 발급 정보는 'pssh' 자체가 아니라 'pssh'의 Data 필드에 해당함을 주의해야 한다. Protection System Specific Header Box에 대한 설명은 CENC 표준[1] 9장을 참조한다.

- 상기 Protection System Specific Header Box의 SystemID 필드에는 해당 UHDCP 시스템 식별자를 지정한다.

- ISOBMFF Segment에 포함된 ECM에는 동일 ISOBMFF Segment 내 Sample들을 암호화 위해 사용한 모든 암호화 키들을 반드시 포함하고 있어야 한다. 그러나 이 ECM에 다음 Crypto Period에서 사용할 암호화 키들을 포함하는 것에 대해 제한하지 않는다.

UHDCP 시스템이 전달하는 EMM/라이선스와 DP 시스템이 전달하는 데이터(예를 들

어 CA Token, CA Token Revocation List, UHDCP 클라이언트 이미지, DP Manager 이미지 등)의 전달 방식 및 전달 위치 시그널링에 대한 설명은 다음과 같다.

- UHDCP 시스템이 전달하는 EMM/라이선스는 단방향 방송망으로 전달하는 경우 ROUTE 또는 MMTP 방식으로 전달한다.
  - ✓ ROUTE 방식으로 EMM/라이선스를 전달하는 경우 각 UHDCP 시스템의 EMM/라이선스는 서로 다른 LCT Session으로 구성하여 전달한다.
  - ✓ MMTP 방식으로 EMM/라이선스를 전달하는 경우 표준 [8] 9.3.13절에 있는 라이선스 시그널링 메시지 LS_message()를 통해 전달한다. 여기서 라이선스는 DRM 방식의 라이선스 또는 CAS 방식의 EMM을 의미한다.
- DP 시스템이 전달하는 데이터는 단방향 방송망으로 전달하는 경우 ROUTE 방식으로 전달한다. 각 DP 시스템의 데이터는 서로 다른 LCT Session으로 구성하여 전달한다.
- 각 UHDCP/DP 시스템 데이터가 전달되는 ROUTE 또는 MMTP에 대한 시그널링 정보는 표 8-2의 Content Protection Table (CPT)에 포함되어 전달된다.
- CPT는 LLS를 통해 전달하며 LLS_table_id는 0x81이다.
  - ✓ 일반적으로 UHDCP/DP 시스템 데이터는 특정 서비스 채널 수신 상태와 상관 없이 수신기의 해당 클라이언트 모듈로 전달되어 처리되어야 하므로 LLS 수준에서 전달 위치를 시그널링 한다.
- CPT는 XML 문서로 표현되며 이의 XML Namespace는 다음과 같다. CPT의 XML 스키마 정의는 부속서 A를 참고한다.

http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Delivery/CPT/1.0/

표 8-2. CPT XML Format

Element or Attribute Name	Use	Data Type	Description
CPT	1		CPT Root Element
@bsid	1	unsignedShort	Broadcast Stream 식별자

Element or Attribute Name	Use	Data Type	Description
CP	1..n		각 UHDCP/DP 시스템 별로 존재한다.
@operatorId	1	unsignedByte	UHDCP/DP 시스템 운영 식별자(0~127 값 범위)
@cpUuid	1	string	UHDCP/DP 시스템을 식별하기 위한 UUID 값
BroadcastDelivery	0..n		UHDCP/DP 시스템 데이터를 단방향 방송망으로 전달하는 경우 존재한다.
@dataType	1	unsignedByte	UHDCP/DP 시스템이 전달하는 데이터 타입으로 표 8-3을 참조한다. 표 8-3의 System-defined values는 각 UHDCP/DP 시스템 별로 임의로 정의할 수 있으며 이 값은 cpUuid 값 내에서 유일한 데이터 타입 값으로 사용할 수 있다.
@dataSeqNum	0..1	unsignedByte	@dataType으로 식별되는 UHDCP/DP 데이터에 대한 버전이다. 단방향 방송망 환경 수신기에서 dataSeqNum가 증가되면 해당 데이터를 갱신한다. dataSeqNum는 @dataType으로 식별되는 데이터가 변경될 경우 1씩 증가하며, 최고값 후에는 0으로 돌아간다. 본 속성은 데이터 타입 별로 존재할 수도 있고 존재하지 않을 수도 있다.
@cpProtocol	1	unsignedByte	UHDCP/DP 시스템이 전달하는 데이터 전송 프로토콜을 나타내며 값은 표 8-4를 참고한다.
@plpId	1	unsignedByte	UHDCP/DP 시스템 데이터를 전송하는 PLP에 대한 식별자
@dIpAddr	1	string	UHDCP/DP 시스템 데이터를 전송하는 패킷의 목적지 주소 dotted-IPv4 문자열
@dPort	1	unsignedShort	UHDCP/DP 시스템 데이터를 전송하는 패킷의 목적지 포트 번호
@sIpAddr	1	string	UHDCP/DP 시스템 데이터를 전송하는 패킷의 원본 주소 dotted-IPv4 문자열

Element or Attribute Name	Use	Data Type	Description
@tsi	0..1	unsignedInt	UHDCP/DP 시스템 데이터를 ROUTE로 전송하는 경우 LCT Session의 TSI (TSI 값으로 0은 사용되지 않아야 한다.)
@bw	0..1	unsignedInt	Maximum Bandwidth를 의미하며 ROUTE로 전송하는 경우에만 존재한다.
SrcFlow	0..1		ROUTE로 전송하는 경우에만 존재하며 SrcFlow에 대해서는 표준 [5]의 ROUTE SrcFlow 부분을 참조한다.
InetUrl	0..1	anyURI	UHDCP/DP 시스템 데이터를 요청하기 위한 URL이며 이 URL로 데이터 요청 시 서버에게 해당 UHDCP/DP 시스템의 UUID를 알려주기 위해 Query String에 'cpUuid=<UHDCP_DP_UUID>'를 반드시 포함시켜야 한다. 본 항목은 UHDCP/DP 시스템이 전송하는 데이터가 브로드밴드 방식으로 전송 가능한 경우 존재한다.
@dataType	1	unsignedShort	UHDCP/DP 시스템이 전달하는 데이터 타입으로 표 8-3을 참조한다. 표 8-3의 System-defined values는 각 UHDCP/DP 시스템 별로 임의로 정의할 수 있으며 이 값은 cpUuid 값 내에서 유일한 데이터 타입 값으로 사용한다.

표 8-3. dataType 의 코드표

dataType	Meaning
0x00	Reserved
0x01	DP Message
0x02	UHDCP EMM 또는 라이선스
0x03 ~ 0x7F	Reserved
0x80~FF	System-defined values

표 8-4. CPT.CP.BroadcastDelivery@cpProtocol 의 코드표

cpProtocol	Meaning
0	Reserved
1	ROUTE
2	MMTP
other values	Reserved for future use

9. UHDTV 콘텐츠 관리 정보

본 장에서는 지상파 UHDTV 방송프로그램 관리를 위한 CMI 신호의 의미와 문법을 정의한다.

9.1 지상파 UHDTV 방송프로그램 보호 신호 규격

9.1.1 CMI 문법과 의미

본 절에서는 CMI의 문법(syntax)과 의미(semantics)를 정의한다. CMI 전송 경로에 따라 Binary format과 XML format을 정의한다. CMI는 UHDCP 시스템 및 ATSC 3.0 Delivery System을 통해 전달 가능하며, UHDCP 시스템을 통해 전달되는 정보를 우선한다.

9.1.1.1 전송 경로: UHDCP System

UHDCP 시스템을 통해 CMI를 전송할 수 있고, 이 경우를 위해 Binary Format을 정의한다.

표 9-1. Content Management Information (Binary Format)

Syntax	Bits	비고
content_management_information(){		
version	8	CMI Version 정보
redistribution_control_code	2	배포 제어 정보
redistribution_area	1	배포 범위 ('0'=한국, '1'=제한없음)
reserved	5	
if (redistribution_control_code==01){		
redistribution_condition()		제한적 배포 조건(표 9-2 참조)
}		
cmi_signature (optional)	320	CMI 정보에 대한 Signature
}		

표 9-2. Redistribution Condition

Syntax	Bits	비고
redistribution_condition(){		
holdback_time	3	배포 허용 시점
allowed_max_resolution	2	배포 허용 최대 해상도
allowed_copy	2	최대 허용 복사 횟수
reserved	1	
}		

각 필드의 의미는 아래에 함께 설명한다.

9.1.1.2 전송 경로: ATSC 3.0 Delivery System

CMI는 SLS USBD 안의 ContentManagementInfo XML 엘리먼트 또는 Service Announcement의 Content Fragment 안의 PrivateExt 엘리먼트 하위 ContentManagementInfo XML 엘리먼트를 통해 전송될 수 있고, 세부 XML 스키마는 9.1.1.2.1, 9.1.1.2.2절을 참고한다

9.1.1.2.1 SLS USBD를 통한 CMI 전송

ROUTE와 MMT에서 전송되는 CMI는 각 ROUTE와 MMT SLS의 USBD를 통해 전달된다. CMI에 대한 XML 엘리먼트 정의는 표 9-3과 같으며 이 XML 엘리먼트는 USBD userServiceDescription의 PrivateExt 엘리먼트 하위 ContentManagement XML 엘리먼트로 존재한다. CMI의 XML 스키마 정의는 부속서 B를 참고한다.

표 9-3. SLS USBD 의 ContentManagementInfo XML 엘리먼트 정의

Element or Attribute Name		Use	Description
ContentManagementInfo		O	
	@version	M	프로그램 보호신호의 버전 정보 본 규격에서는 0x02로 지정한다.
	RedistributionControlCode	M	방송프로그램 배포 제어 정보.

	@code	M	방송프로그램 배포 제어 정보 값 본 값이 '3'일 경우 방송프로그램은 모든 단말에서 인식이 가능한 형태로 자유로운 배포가 가능하며, '1'일 경우 9.1.1.3절의 제한적 배포 조건의 범위 내에서 배포 할 수 있다. '0'과 '2'는 사용하지 않는다.
	RedistributionCondition	CM	RedistributionControlCode@code 속성 값이 '1'일 경우에만 전송되며, 자세한 문법(syntax)는 9.1.1.3절을 따른다.
@redistributionArea		M	방송프로그램의 배포범위를 의미 지역정보를 포함하는 저장매체를 통하여 배포할 경우 한국으로 명시해야 한다. 지역정보를 포함하는 재배포 혹은 재전송 시(IP 실시간 재전송 등)에는 배포지역이 한국임을 명시하거나 한국으로 제한하여야 한다.
Signature		O	CMI의 무결성을 검증하기 위한 Signature로, 무결성이 보장되지 않을 경우 프로그램은 위조된 프로그램으로 간주한다. Signature는 XML Signature Syntax and Processing Version 1.1 표준[9] 기반의 XML Signature이다.

(M: Mandatory, O: Optional, CM: Conditional-Mandatory)

9.1.1.2.2 Content Fragment를 통한 CMI 전송

개별 프로그램 단위로 CMI가 전송될 수 있다. Content Fragment를 통해 전달되는 CMI는 표준 [4]의 Service Announcement의 Content Fragment 안에 PrivateExt XML 엘리먼트의 하위 ContentManagementInfo XML 엘리먼트로 전달되며, 문법(Syntax)은 표 9-4와 같다. 각 XML 엘리먼트/속성에 대한 설명은 표 9-3을 참조한다.

Content Fragment를 통해 전달되는 ContentManagementInfo XML 엘리먼트를 정의하는 XML 스키마의 XML Namespace는 다음과 같다. 이 XML 스키마 정의는 부속서 B를 참고한다.

http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Protection/CMI/1.0/

USBD에 포함된 ContentManagementInfo XML 엘리먼트와 Content Fragment에 포

함된 ContentManagementInfo XML 엘리먼트의 내용이 다른 경우 Content Fragment에 있는 내용이 우선한다.

표 9-4. Content Fragment 의 ContentManagementInfo XML 엘리먼트

ContentManagementInfo
version
RedistributionControlCode
code
RedistributionCondition
holdbackTime
allowedMaxResolution
allowedCopy
redistributionArea
Signature

9.1.1.3 재배포 조건(Redistribution Condition) 엘리먼트 확장

제한적 재배포 조건(Redistribution Condition)은 9.1.1절의 CMI 문법과 의미에서 RedistributionControlCode@code == 1에 적용하여야 하는 RedistributionCondition에 해당하는 것으로써, UHDTV 수신기가 해당 방송프로그램을 타 UHDTV 수신기에서 사용할 수 있도록 배포하는 것이 허락되지만, 단말에서 지원 가능한 필드에 대해서는 RedistributionCondition 신호를 해석하여 제한적 배포 조건을 적용할 수 있어야 한다.

Element or Attribute		Usage	Datatype	Description
RedistributionCondition		0..1		
	@holdbackTime	1	unsignedByte	배포 허용 시점
	@allowedMaxResolution	1	unsignedByte	배포 허용 최대 해상도
	@allowedCopy	1	unsignedByte	최대 허용 복사 횟수

- **holdbackTime**: 방송프로그램 배포 허용 시간
  - ✓ 방송프로그램의 방영 후, 지정된 시간(방영시간 + time)이 지난 후에 배포를 허용한다.

값	시간

0	24 시간
1	48 시간
2	1 주일 (24 x 7)
3	4 주일 (24 x 28)
4~6	reserved
7	제한없음

- **allowedMaxResolution**: 방송프로그램 배포 허용 최대 해상도

  ✓ 방송프로그램에 대해서 허용 최대 해상도보다 같거나 작은 범위의 화면 해상도 출력만 허용한다.

값	해상도
0	SD (720 x 480) 이하
1	FHD (1920 x 1080) 이하
2	reserved
3	제한없음

- **allowedCopy**: 방송프로그램 최대 허용 복사 횟수

  ✓ 방송프로그램의 타 디바이스로의 콘텐츠 복사는 지정된 횟수만 허용한다.

값	횟수
0	복사 불가
1	9회
2	reserved
3	제한없음

10. 송신 시스템 연동 인터페이스

본 장에서는 CENC Scrambler와 UHDCP 시스템 간의 연동 인터페이스에 대해 기술한다.

기본적으로 CENC Scrambler와 UHDCP 시스템 간 연동 인터페이스는 DVB SimulCrypt 규격[2]을 따른다.

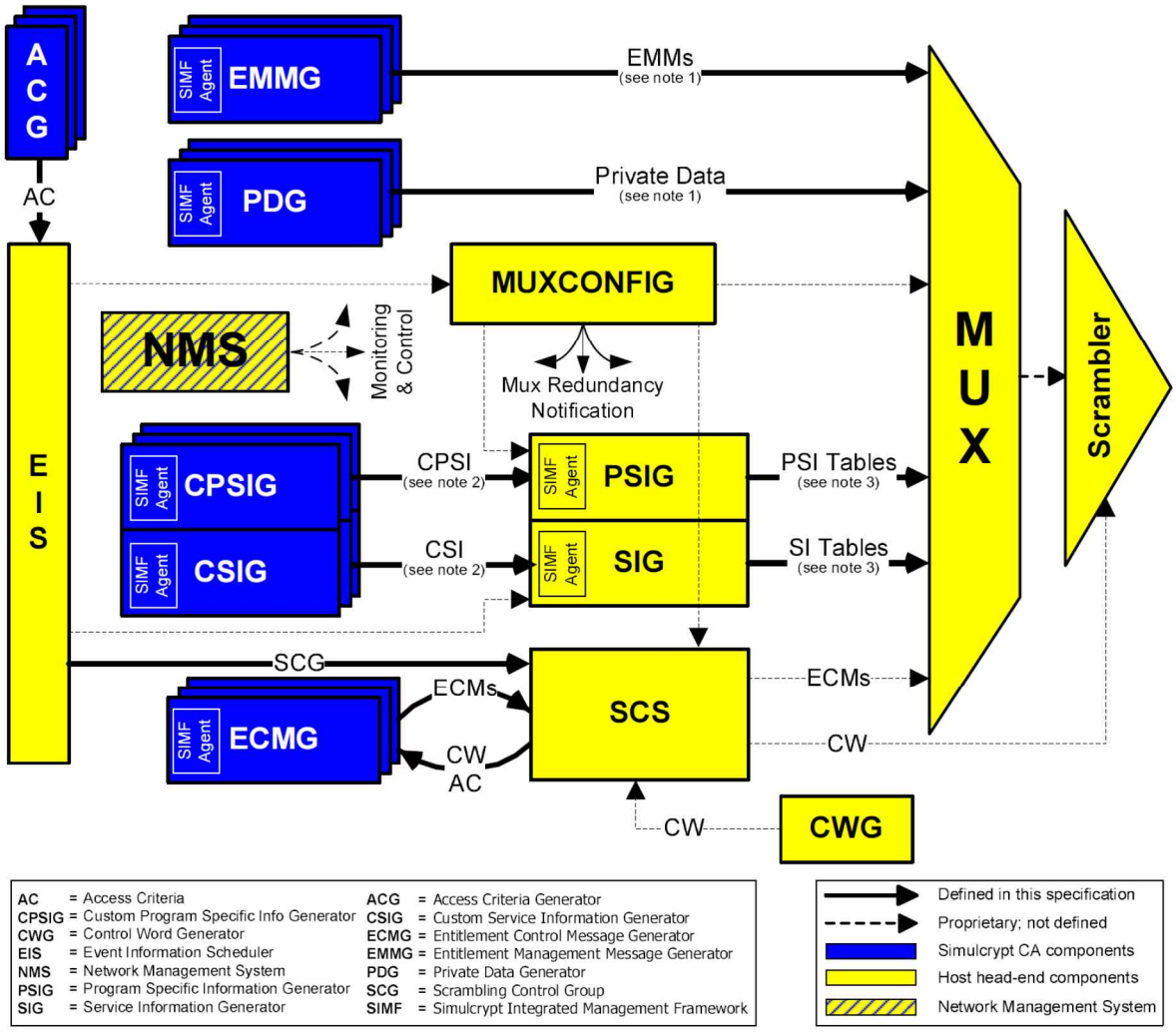

그림 10-1. DVB SimulCrypt System Architecture (DVB SimulCrypt 규격[2] 발췌)

본 표준에서는 DVB SimulCrypt 규격[2]의 System Architecture 상에서 SCS (SimulCrypt Synchronizer), CWG (Control Word Generator), SCR (Scrambler) 기능을 제공

하는 장비를 CENC Scrambler라고 부른다. MUX (Multiplexer) 기능은 CENC Scrambler가 제공하거나 다른 방송 장비에서 제공할 수 있다. UHDCP 시스템은 ECMG (ECM Generator), EMMG (EMM Generator) 기능을 제공한다.

본 표준에서는 UHD 콘텐츠 보호를 위해 7장에서 설명한 CENC 적용 시 DVB SimulCrypt 규격[2]의 ECMG ⇔ SCS Interface와 EMMG ⇔ MUX Interface에서 수정 또는 확장되어야 하는 부분에 대해서 기술한다.

10.1 ECMG ⇔ SCS Interface

UHDCP ECMG와 SCS 간 연동 인터페이스는 기본적으로 DVB SimulCrypt 규격[2] 5장 ECMG ⇔ SCS Interface를 따른다. 본 절에서는 CENC 적용으로 인해 수정/추가되어야 하는 ECMG ⇔ SCS Interface의 Parameters 및 Messages에 대해 기술한다.

10.1.1 Parameters

CENC 표준[1]에서는 UHDCP 시스템 식별자 체계가 DVB CA_System_id(16 bits) 체계가 아닌 UUID 체계이므로 기존 Super_CAS_id Parameter와 동일한 목적으로 사용하는 다른 Parameter인 Super_System_id를 표 10-1과 같이 추가 정의한다.

CENC 표준[1]은 ISOBMFF Segments의 Sample들을 암호화 하기 위해 AES 128 bits 암호화 알고리즘을 이용하므로 Key 값은 16 bytes 크기를 갖는다. 또한 이 Key의 식별자(KID)를 UUID 체계로 사용할 것을 강력하게 권고하고 있으며 KID는 16 bytes 크기로 표현하게 되어 있다. ECMG ⇔ SCS Interface에서 암호화 키 및 키 식별자를 표시하기 위한 Parameter는 CP_CW_Combination이므로 표 10-1과 같이 이 Parameter를 정의한다.

CENC 표준[1]은 DASH MPD <ContentProtection> Descriptor 요소에 default_KID와 pssh를 XML 형태로 넣을 수 있도록 정의하고 있다. CENC Scrambler가 상기한 MPD <ContentProtection> Descriptor를 처리할 수 있는 경우 ECMG가 MPD <ContentProtection> Descriptor 요소에 들어갈 default_KID와 pssh의 Data를 SCS로 전달할 수 있도록 하기 위해 표 10-1과 같이 MPD_kid_pssh_Combination Parameter를 추가 정의한다.

CENC 표준[1]은 Track Encryption Box 'tenc'에 default_KID를 넣을 수 있고 Movie Box 'moov'에 pssh를 넣을 수 있도록 정의하고 있다. 이를 지원하기 위해 표 10-1과 같이 Default_kid_pssh_Combination Parameter를 추가 정의한다.

표 10-1. parameter_type values for use with CENC

Parameter_type Value	Parameter Type	Type/Units	Length (bytes)
0x0014	CP_CW_Combination	----	
	CP	uimsbf	2
	KID	uimsbf	16
	CW	uimsbf	16
0x8001	Super_System_id	uimsbf	18
0x8002	MPD_kid_pssh_Combination	----	
	default_KID	uimsbf	16
	pssh_data	user defined	Variable
0x8003	Default_kid_pssh_Combination	----	
	default_KID	uimsbf	16
	pssh_data	user defined	Variable

- **CP_CW_Combination**: 이 Parameter는 Crypto Period, Key ID, CW 필드의 연속(concatenation)으로 구성된다. Key ID는 CENC 표준[1]에서의 KID에 해당하며 CW는 KID로 식별되는 키 값을 나타낸다.

- **Super_System_id**: 이 Parameter는 CENC 표준에서의 Content Protection System을 구분하기 UUID 16 bytes와 Subsystem_ID 2 bytes로 구성된다. SCS는 Subsystem_ID를 통해 Content Protection System의 특정한 ECMG를 식별할 수 있다. Subsystem_ID 값에 대한 지정은 시스템 사용자에 의해 지정될 수 있는 사적인 값이다.

- **MPD_kid_pssh_Combination**: 이 Parameter는 MPD ContentProtection Descriptor에 들어갈 수 있는 default_KID와 pssh_data를 포함한다. pssh_data는 CENC 표준[1]에서 정의하는 'pssh' Box의 Data(Content Protection System specific data)를

말한다. SCS는 pssh_data를 이용하여 최종적인 'pssh' Box를 생성해야 한다. 만일 전달하려는 default_KID와 pssh_data가 Crypto Period 이전에 전달한 default_KID와 pssh_data에서 변함이 없다면 동일한 default_KID와 pssh_data를 전달하거나 이 Parameter를 사용하지 않아야 한다. 그러나 더 이상 default_KID 또는 pssh_data를 전달하지 않기를 원한다면 다음과 같이 처리해야 한다.

- ✓ default_KID를 전달하지 않는다면 default_KID는 0x00 값으로 채운다. pssh_data를 전달하지 않는다면 pssh_data 필드는 존재하지 않아야 하며 이 경우 이 Parameter의 길이(parameter_length)는 default_KID 필드의 길이 만을 나타내는 값 16(10진수)이 될 것이다.

- **Default_kid_pssh_Combination**: Track Encryption Box 'tenc'에 들어갈 수 있는 default_KID와 Movie Box 'moov'에 들어갈 수 있는 'pssh' Box의 pssh_data를 나타낸다. default_KID와 pssh_data 사용 설명은 상기 MPD_kid_pssh_Combination Parameter의 해당 부분과 동일하다.

ECM_response 메시지에 포함되는 ECM_datagram은 Movie Fragment ('moof')에 포함되어 전달되는 'pssh' Box의 Data를 나타낸다. 만일 Movie Fragment ('moof')를 통해 'pssh' Box를 전달하지 않기 위해서는 ECM_datagram Parameter의 길이를 0(zero)로 하여 전송하도록 한다.

ECM을 전달하는 Container가 MPEG-2 section format 또는 MPEG-2 transport stream packet format이 아니기 때문에 section_TSpkt_flag Parameter 값은 0x02 값으로 지정해야 한다.

10.1.2 Channel specific Messages

UHDCP ECMG와 SCS 간 Channel 연결을 위한 메시지는 DVB SimulCrypt 규격[2] ECMG ⇔ SCS Interface 5.4절을 따른다. 다만, Channel_setup message를 표 10-2와 같이 수정한다.

표 10-2. Channel_setup Message for use with CENC

Parameter	Number of instances in message
ECM_channel_id	1
Super_System_id	1

10.1.3 Stream specific Messages

UHDCP ECMG와 SCS 간 Stream 연결을 위한 메시지는 DVB SimulCrypt 규격[2] ECMG ⇔ SCS Interface의 5.5절을 따른다. 다만, ECM_response message를 표 10-3과 같이 수정한다.

표 10-3. ECM_response Message for use with CENC

Parameter	Number of instances in message
ECM_channel_id	1
ECM_stream_id	1
CP_number	1
ECM_datagram	1
MPD_kid_pssh_Combination	0 to 1
Default_kid_pssh_Combination	0 to 1

10.2 EMMG ⇔ MUX Interface

UHDCP EMMG와 MUX 간 연동 인터페이스는 기본적으로 DVB SimulCrypt 규격[2] 6장 EMMG ⇔ MUX Interface를 따른다. 본 절에서는 CENC 적용으로 인해 수정/추가되어야 하는 EMMG ⇔ MUX Interface의 Parameters 및 Messages에 대해 기술한다.

10.2.1 Parameters

CENC 표준[1]에서는 UHDCP 시스템 식별자 체계가 DVB CA_System_id(16 bits) 체계가 아닌 UUID 체계이므로 기존 client_id Parameter와 동일한 목적으로 사용하는 다른 Parameter인 UUID_Client_id를

표 10-4와 같이 추가 정의한다.

표 10-4. parameter_type values for use with CENC

Parameter_type Value	Parameter Type	Type/Units	Length (bytes)
0x8001	UUID_client_id	uimsbf	18

- **UUID_client_id**: 이 Parameter의 첫 16 bytes는 CENC 표준[1]에서의 Content Protection System을 구분하기 UUID 16 bytes를 지정하기 위해 사용한다. 하위 2 bytes는 Content Protection System의 특정 EMMG를 식별하기 위해 사용할 수 있다.

EMM을 전달하는 Container가 MPEG-2 section format 또는 MPEG-2 transport stream packet format이 아니기 때문에 section_TSpkt_flag Parameter 값은 0x02 값으로 지정해야 한다.

10.2.2 Channel/Stream specific Messages

UHDCP EMMG와 MUX 간 Channel 및 Stream 연결을 위한 메시지는 DVB SimulCrypt[2] 규격 EMMG ⇔ MUX Interface의 6.2.4절 및 6.2.5절을 따른다. 다만, 모든 Channel/Stream specific Messages에서 client_id Parameter는 사용하지 않아야 하고 10.2.1절에서 추가 정의한 UUID_client_id Parameter를 사용해야 한다.

11. 다운로드 플랫폼

본 장에서는 다운로드 플랫폼에 대해 설명한다.

다운로드 플랫폼은 UHDCP 클라이언트 이미지를 서버에서 수신기로 안전하게 다운로드, 설치, 운영할 수 있는 시스템이다. 다운로드 플랫폼 서버는 지상파 UHDTV 방송 콘텐츠 보호를 위해 운영하는 UHDCP 클라이언트에 대한 버전 관리를 수행하며 필요한 경우 수신기에 설치되어 있는 UHDCP 클라이언트에 대한 업데이트 또는 신규 UHDCP 클라이언트 설치를 수행한다. 다운로드 플랫폼 서버는 현재 운영하고 있는 UHDCP 클라이언트에 대한 정보를 수신기에 제공하기 위해 11.1절에서 설명할 DP Message를 단방향 방송망 또는 양방향 네트워크를 통해 전달한다. DP Message가 전달되는 위치 정보는 8.2.3절에서 설명한 CPT에 포함되어 있다. DP Message에는 현재 운영하는 UHDCP 클라이언트에 해당하는 UHDCP 시스템 식별자, 버전 정보 뿐만 아니라 11.2절에서 설명할 CA Token, CA Token Revocation List, UHDCP 클라이언트 이미지, DP Manager 이미지가 다운로드 되는 단방향/양방향 전달 위치 정보를 포함하여 전달한다.

다운로드 플랫폼 서버는 DP Message 뿐만 아니라 CA Token, CA Token Revocation List, UHDCP 클라이언트 이미지, DP Manager 이미지를 단방향 방송망 또는 양방향 네트워크를 통해 전달한다. CA Token은 수신기의 콘텐츠 시청 권한을 확인하기 위한 것으로 향후 UHDCP 클라이언트 이미지 다운로드를 위한 증명 값으로 사용된다. CA Token Revocation List는 폐기할 CA Token에 대한 식별자 리스트를 포함하고 있다. UHDCP 클라이언트 이미지와 DP Manager 이미지는 수신기에서 동작할 UHDCP 클라이언트와 DP Manager에 대한 소프트웨어 이미지이다.

수신기에는 상기한 DP Message, CA Token, CA Token Revocation List, UHDCP 클라이언트 이미지를 처리하는 DP Manager가 존재한다. DP Manager는 DP Message를 수신하여 운영해야 하는 UHDCP 클라이언트가 현재 수신기에 설치되어 동작하고 있는지, UHDCP 클라이언트 이미지 업데이트 또는 신규 UHDCP 클라이언트 다운로드 및 설치가 필요한지를 판단한다. UHDCP 클라이언트 이미지 다운로드 및 설치가 필요한 경우 DP Message에 있는 UHDCP 클라이언트 이미지 다운로드 전달 위치를 참조하여 UHDCP 클라이언트 이미지 다운로드 및 설치를 수행한다. DP Manager는 CA Token 다운로드 또는 CA Token 업데이트를 수행하며 수신기에 있는 CA Token이 CA Token Revocation List에 포함되어 있는 경우 해당 CA Token에 대한 폐기를 수행한다. 그리고 수신기에는 DP

Manager 업데이트를 관리하는 DPM Loader가 존재한다.

11.1 DP Message

DP Message는 DP 시스템에서 운영하는 UHDCP 시스템에 대한 정보(현재 운용 중인 UHDCP 시스템 식별자 및 버전, UHDCP 클라이언트 및 DP Manager 이미지의 단방향/양방향 전달 위치 정보, CA Token 버전 및 단방향/양방향 전달 위치 정보, CA Token Revocation List 버전 및 단방향/양방향 전달 위치 정보 등)을 포함한다. DP 서버는 DP Message를 주기적으로 전송하며 수신기는 UHDCP 클라이언트 운영 및 업데이트 동작을 위해 DP Message를 수신 및 처리해야 한다.

본 표준에서 정의하는 DP Message는 11.1.1.1절에서 정의하는 XML 형태로 구성된다. DP Message는 단방향 방송망 또는 양방향 네트워크를 통해 전달될 수 있다. 11.1.1.2절에서 세부적으로 설명하겠지만, DP Message는 단방향 방송망으로 전달되는 경우 ROUTE를 통해 전달되고, 양방향 네트워크의 경우 HTTP(S) 요청/응답으로 전달된다. DP Message가 전달되는 ROUTE 채널에 대한 위치 정보와 양방향 네트워크 HTTP(S) URL 정보는 CPT (Content Protection Table)을 통해 제공된다.

11.1.1 DP Message 정의 및 전달 방식

DP Message는 DP 서버에서 수신기에 있는 DP Manager (DPM Loader)로 전달하는 메시지로 DP 시스템에서 운영하는 DP 시스템 정보와 UHDCP 시스템 정보를 포함한다. DP 시스템 운영 정보로는 해당 DP 시스템이 관리하는 대상 서비스 리스트 정보, 대상 수신기 리스트 정보, 대상 수신기 별 DP Manager 및 UHDCP 클라이언트 이미지 버전 정보, DP Manager 이미지 전달 위치 정보, UHDCP 클라이언트 이미지 전달 위치 정보, CA Token 버전 및 단방향/양방향 전달 위치 정보, CA Token Revocation List 버전 및 단방향/양방향 전달 위치 정보 등이 포함된다. 세부적인 DP Message 구조 및 설명은 표 11-1을 참고한다.

DP Message는 DP 시스템을 운영하는 시스템 별로 생성하여 전달할 수 있으며 XML 구조로 되어 있다.

수신기는 기본적으로 DPM Loader 및 DP Manager가 설치되어 있어야 하며 수신기에는 운영하는 DP Manager의 DP 시스템 식별자(UUID 형태)와 Operator ID 값이 미리 저장되어 있어야 한다.

11.1.1.1 DP Message 정의

DP Message는 표 11-1과 같이 XML 구조로 정의된다. 본 규격에서는 DP Manager 및 UHDCP 클라이언트 이미지, CA Token, CA Token Revocation List 등을 총칭하여 DP 데이터라고 부른다. DP Message는 각 DP 데이터의 버전 및 단방향/양방향 전달 위치 정보를 포함한다. DP Message의 XML Namespace는 다음과 같다. DP Message의 XML 스키마 정의는 부속서 C를 참고한다.

http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Protection/DPM/1.0/

표 11-1. DP Message XML Format

Element or Attribute Name	Use	Data Type	Description
DPM	1		DP Message Root Element
@operatorId	1	unsignedByte	DP 운영 시스템 식별자(0~127 값 범위)
@version	1	unsignedShort	DP Message 정보 버전 하위 정보 중 일부라도 변경이 있으면 값 1을 증가시키며 최대 값 이후 다시 0으로 재설정한다.
DpInfo	1		DP 운영 정보
ServiceList	1		서비스 식별 정보 리스트
Service	1..n		DP 운영 대상이 되는 서비스 식별 정보
@globalServiceID	1	anyURI	SLS <userServiceDescription> 하위 @globalServiceID에 해당
@serviceId	1	unsignedShort	SLS <userServiceDescription> 하위 @serviceId에 해당
DeviceList	1		Device 정보 리스트
Device	1..n		DP 운영 대상이 되는 Device 정보

Element or Attribute Name	Use	Data Type	Description
@modelType	1	string	Device 모델 식별자로 hexadecimal 형태로 표시
Dpm	0..1		Device에서 현재 운영되는 DP Manager 정보
@sysUuid	1	string	DP 시스템 식별자 (UUID 체계)
@version	1	string	현재 사용하는 DP 시스템 버전
@refUri	0..1	anyURI	해당 DP Manager 이미지 전달 위치 정보에 대한 참조 식별자(DeliveryInfo@id)
Dpc	0..n		Device에서 현재 운영되는 UHDCP 클라이언트 정보
@sysUuid	1	string	현재 사용하는 UHDCP 클라이언트의 시스템 식별자 (UUID 체계)
@version	1	string	현재 사용하는 UHDCP 클라이언트 버전
@refUri	0..1	anyURI	해당 UHDCP 클라이언트 이미지 전달 위치 정보에 대한 참조 식별자 (DeliveryInfo@id)
Cat	0..n		각 수신기 별 CA Token 버전 및 전달 위치 정보 제공
@version	1	string	현재 CA Token 버전
@refUri	0..1	anyURI	해당 CA Token 전달 위치 정보에 대한 참조 식별자(DeliveryInfo@id)
Ctrl	0..1		CA Token Revocation List 버전 및 전달 위치 정보 제공
@version	1	string	현재 CA Token Revocation List 버전
@refUri	0..1	anyURI	해당 CA Token Revocation List 전달 위치 정보에 대한 참조 식별자 (DeliveryInfo@id)
DeliveryInfo	0..n		DP 데이터의 전달 위치 정보
@id	1	anyURI	DP 데이터의 전달 위치 정보 식별자
@type	1	string	전달하는 DP 데이터가 DP Manager 이미지인 경우 “dpm”, UHDCP 클라이언트 이미지인 경우 “dpc”, CA Token인 경우 “cat”, CA Token Revocation List인 경우 “ctrl”로 지정 (인식하지 못하는 type은 무

Element or Attribute Name	Use	Data Type	Description
시한다.)			
@sysUuid	0..1	string	@type="dpm"인 경우 DP 시스템, @type="dpc"인 경우 UHDCP 클라이언트에 해당하는 UHDCP 시스템 식별자를 나타낸다. @refUri로 참조하는 Device.Dpm@sysUuid 또는 Device.Dpc@sysUuid 값과 동일해야 한다. @type="cat", @type="ctrl"인 경우 본 속성은 존재하지 않는다.
BroadcastDelivery	0..1		DP 데이터가 단방향 방송망으로 전달되는 경우 존재한다. 본 항목과 InetUrl 항목 중 하나는 최소한 존재해야 한다.
@plpId	0..1	unsignedByte	DP 데이터를 전달하는 PLP에 대한 식별자 DP Message와 동일한 PLP로 전달되는 경우 생략 가능하며 기본적으로 DP Message가 전달되는 PLP ID를 이용한다.
@dIpAddr	0..1	string	DP 데이터를 전달하는 패킷의 목적지 주소 dotted-IPv4 문자열 DP Message와 동일한 목적지 IP Address로 전달되는 경우 생략 가능하며 기본적으로 DP Message가 전달되는 목적지 IP Address를 이용한다.
@dPort	0..1	unsignedShort	DP 데이터를 전달하는 패킷의 목적지 포트 번호 DP Message와 동일한 포트 번호로 전달되는 경우 생략 가능하며 기본적으로 DP Message가 전달되는 포트 번호를 이용한다.
@sIpAddr	0..1	string	DP 데이터를 전달하는 패킷의 원본 주소 dotted-IPv4 문자열 DP Message와 동일한 원본 IP Address로

Element or Attribute Name	Use	Data Type	Description
			전달되는 경우 생략 가능하며 기본적으로 DP Message가 전달되는 원본 IP Address를 이용한다.
@tsi	0..1	unsignedInt	DP 데이터를 전달하는 LCT Session의 TSI (TSI는 값 0은 사용되지 않아야 함) DP Message와 동일한 LCT Session로 전달되는 경우 생략 가능하며 기본적으로 DP Message가 전달되는 LCT Session를 이용한다.
@bw	0..1	unsignedInt	Maximum Bandwidth
@Content-Location	0..1	anyURI	DP 데이터 파일 식별자(또는 파일 이름)
SrcFlow	0..1		DP Message가 전달되는 SrcFlow와 동일한 경우 생략 가능하다. 규격 [5]의 ROUTE SrcFlow를 참조한다.
InetUrl	0..1	anyURI	DP 데이터를 요청하기 위한 URL 이 URL로 DP 데이터 요청 시 서버에게 해당 DP 시스템 또는 UHDCP 시스템의 UUID, 요청하는 DP 데이터 버전을 알려주기 위해 HTTP(S) Request의 Query String에 'sysUuid=<*DeliveryInfo@sysUuid*>', 'version=<*DeliveryInfo@version*>'를 포함시켜야 한다. @type="dpm" 또는 @type="dpc"인 경우 sysUuid와 version은 반드시 포함시켜야 하며 @type="cat", @type="ctrl"인 경우 sysUuid는 포함하지 않고 version은 반드시 포함시켜야 한다. @type="dpc"와 @type="ctrl"인 경우 CA Token Format에 있는 SW Download Server Info와 CTRL Server Info와 동일한 값으로 URL이 지정되어야 하며 만일 다른 값을 갖는 경우 본 DP Message에 있

Element or Attribute Name	Use	Data Type	Description
			는 값이 우선한다.
Signature	1	ds:Signature	DP Message의 메시지 인증 및 무결성을 위해 XML Signature Syntax and Processing Version 1.1 표준[9] 기반의 XML Signature를 포함한다.

11.1.1.2 DP Message 전달 방식

본 절에서는 DP Message 전달과 관련하여 DP 서버에서 수신기 Host 모듈로 전달하는 방식과 수신기가 DP Message를 수신하는 방식에 대해 설명한다.

DP Message는 단방향 방송망을 통한 ROUTE 또는 양방향 네트워크를 통한 HTTP(S) 요청/응답 방식으로 DP 서버에서 수신기 Host로 전달된다. DP Message가 전달되는 ROUTE 채널 정보 또는 HTTP(S) URL 정보는 8.2.3절에서 정의한 CPT를 통해 전달된다. 이 때 전달되는 Data Type (CPT.BroadcastDelivery@dataType 또는 CPT.InetUrl@dataType)은 DP Message로 지정되어야 한다.

DP Message를 ROUTE로 전달하는 경우 DP Message를 전달하기 위한 ROUTE 객체 TOI 값은 다음과 같이 설정해야 한다. DP Message를 전달하기 위한 TOI 구성 필드에 대한 설명은 11.1.2절을 참고한다.

- **T** (1 bit): 0b0 (DP 시스템)
- **System ID** (7 bits): DP Message의 DPM@operatorId 값
- **Message Type** (8 bits): 0x01 (DP Message)
- **Version** (16 bits): DP Message 버전 값

DP Manager는 수신기 Host에 있는 ROUTE 수신기가 DP Message를 수신할 수 있도록 TOI 필터링 비트 마스킹을 다음과 같이 설정해야 한다. DP Message 수신을 위한 TOI 필터링 비트 마스킹 방법에 대한 설명은 11.1.2절을 참고한다.

- **T** (1 bit): 0b0 (DP 시스템)

- **System ID** (7 bits): DP Message의 DPM@operatorId 값
- **Message Type** (8 bits): 0x01 (DP Message)
- **Version** (16 bits): Don't care bits

ROUTE 수신기는 CPT를 통해 파악된 특정 DP 시스템의 DP Message가 전달되는 LCT Session을 열고 상기 TOI 필터링 비트 마스킹을 적용하여 DP Message를 수신하여 DP Manager에게 전달할 수 있어야 한다.

CPT를 통해 DP Message가 양방향 네트워크를 통해 제공될 수 있도록 DP Message URL 정보가 제공되는 경우 Host는 이 URL을 통해 DP Message를 HTTP(S) 요청/응답 형식으로 수신할 수 있다. Host는 DP Message에 대한 HTTP(S) 요청 시 서버에게 DP 시스템의 식별자와 DP 운영 시스템 식별자를 알려 주기 위해 HTTP(S) Request의 Query String에 'sysUuid=<Dpm@sysUuid>'와 'operatorId=<DPM@operatorId>'를 반드시 포함해야 한다.

11.1.2 보호시스템 데이터 필터링 기법

ROUTE로 전달되는 DP 데이터 또는 UHDCP 데이터(예를 들어 EMM, 라이선스 파일 등) 중 반복적으로 전달되는 데이터를 수신기가 이미 수신하여 처리하였다면 성능 측면에서 불필요하게 재수신 및 재처리 하는 것은 비효율적일 수 있다. 또한 DP 시스템, UHDCP 시스템 측면에서 필요한 데이터만 수신할 수 있도록 요청하는 기법이 필요하다. 이와 관련하여 본 절에서는 ROUTE 사용 시 보호시스템에서 사용하는 데이터 필터링 기법에 대해 설명한다.

DP Manager 및 UHDCP 클라이언트는 수신기 Host에 있는 ROUTE 수신기에게 필터링 할 ROUTE 객체의 TOI 필터링 비트 마스킹 또는 수신할 파일 이름(Content-Location)에 대한 필터링 규칙을 설정하여 ROUTE 수신기가 이 필터링 규칙을 통과하는 ROUTE 객체만 수신한 후 DP Manager 또는 UHDCP 클라이언트에게 전달하도록 할 수 있다. ROUTE 수신기는 설정된 필터링 규칙에 따라 해당하는 ROUTE 객체만 수신할 수 있다. 만일 필터링 규칙이 설정되어 있지 않다면 모든 ROUTE 객체를 수신하여 DP Manager 또는 UHDCP 클라이언트에게 전달한다. TOI 필터링 비트 마스킹 기반의 필터링 규칙을

적용하는 경우 ROUTE 수신기는 필요하지 않은 TOI 값을 갖는 패킷을 처리/저장하지 않아도 되므로 보다 효율적인 운영이 가능할 것이다.

본 표준에서는 DP Manager 또는 UHDCP 클라이언트가 ROUTE 수신기에게 필터링 규칙을 지정/삭제/업데이트 하는 인터페이스에 대해서는 규격화 하지 않는다.

TOI 필터링 비트 마스킹을 통한 필터링 방식을 위해 ROUTE 객체의 LCT TOI 필드를 그림 11-1과 같이 구분한다.

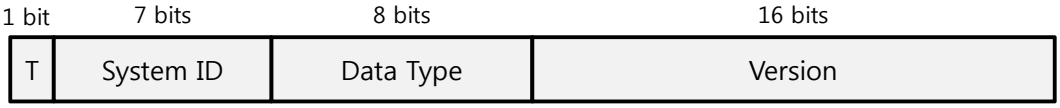

그림 11-1. TOI 필드 할당

- **T** (System Type; 1 bit): DP 시스템(값 0) 또는 UHDCP 시스템(값 1)을 식별한다.
- **System ID** (7 bits): 운영하는 DP 시스템 또는 UHDCP 시스템의 식별자 값을 지정한다.
  - ✓ System Type이 DP 시스템인 경우 OperatorId (DP Message의 DPM@operatorId) 값이 포함된다.
  - ✓ UHDCP 시스템의 경우는 UHDCP 시스템 식별자를 지정할 수 있다. UUID 형태의 UHDCP 시스템 식별자는 TOI 필드의 크기 제한 상 사용할 수 없으므로 UHDCP 서버와 UHDCP 클라이언트 간 미리 조정된 값을 이용한다.
- **Data Type** (8 bits): DP 시스템 또는 UHDCP 시스템에서 정의한 데이터 타입을 지정한다. Data Type 값은 표 11-2와 같다.
- **Version** (16 bits): 데이터의 버전을 나타낸다. 데이터 객체의 내용이 변경된 경우 1씩 증가되어야 하며 최대 값 이후 다시 0으로 재설정해야 한다.

표 11-2. Data Type 코드표

Data Type	Meaning
0x00	Reserved
0x01	DP Message
0x02	UHDCP EMM
0x03	CA Token
0x04	CA Token Revocation List
0x05	UHDCP 클라이언트 이미지
0x06	DP Manager 이미지
0x07~0x7F	Reserved
0x80~FF	System-defined values

각 DP 서버, UHDCP 서버는 상기 TOI 필터링 비트 마스킹 기법에 따라 ROUTE 객체의 TOI 값을 설정하여 ROUTE 채널로 데이터를 전송 해야 한다. DP Manager 또는 UHDCP 클라이언트는 자신이 수신하고자 하는 데이터 형식이 있는 경우 필요한 TOI 구성 필드에 대한 TOI 필터링 비트 마스킹을 설정하여 필요한 데이터만 수신할 수 있다.

11.2 CA Token 및 UHDCP/CP 이미지 다운로드

UHDCP 클라이언트를 다운로드하는 방식은 TTA 표준 "IPTV용 교환 가능한 CAS(iCAS)" 표준[6] 중 3.5.3절 CA Token 전송 프로토콜(CA Token Request 및 CA Token Response)과 3.6.2절 CAS S/W 전송 프로토콜(CAS S/W Request, CAS S/W Response 및 CAS S/W Ack), 3.5.2절 CA Token Revocation List (CTRL)을 따르며, 전송되는 메시지는 전자 봉투 방식을 사용해서 보호한다.

브로드밴드 환경에서는 iCAS 표준[6] 기반의 메시지 전송 프로토콜을 그대로 준수하고, 방송망 환경에서 iCAS 표준[6]의 확장 규격으로 본 표준을 사용한다. 본 표준에 포함되지 않은 상세 규격들은 iCAS 표준[6]을 따르고, 본 표준에서는 수정이 필요한 부분만 기술한다.

11.2.1 CA Token

11.2.1.1 CA Token Response Message

	(msb)							(lsb)
bit / byte	7	6	5	4	3	2	1	0
0	Version (1byte)							
1	Type (1byte)							
2	Command (2bytes)							
3								
4	Length (4bytes)							
5								
6								
7								
8	Result (1byte)							
9	Reason (3bytes)							
10								
11								
12	Encryption Algorithm (1byte)							
13	PUB_C Encrypted Data Length (=y) (3bytes)							
14								
15								
12	*E{PUB_C, (CEK Type || CEK) } (y bytes)*							
…								
O1	CEK Encrypted Data Length (=y) (4bytes)							
O1+1								
O1+2								
O1+3								
O2	*E{CEK, Nc || CA Token} (z bytes)*							
…								

그림 11-2. CA Token Response Message (iCAS 표준[6] 발췌)

그림 11-2는 iCAS 표준[6] 3.5.3절 내의 전자 봉투 방식의 CA Token Response Message에 해당한다. 메시지 포맷은 그대로 사용하되, 방송망 환경 적용을 위해 아래와 같이 일부 필드 내용을 수정한다.

- **Version** (1 byte): 현재 Message의 version을 의미하며, DP 시스템에서는 '0x20'을 사용한다.
- **Type** (1 byte): 다음 Command의 분류를 위해 사용한다.
  - ✓ 0x00 : CA Token Command
  - ✓ 0x01 : CAS SW Command

- ✓ 0x02 : 단방향 환경에서의 CA Token Command
- ✓ 0x03 : 단방향 환경에서의 CAS SW Command
- ✓ Others are reserved.

- **Command** (2 bytes): 전송 메시지 구분을 위한 세부 Command를 의미하며, 방송망 환경의 DP 시스템에서는 '0x11'을 사용한다.
  - ✓ 0x00 : CA Token Request Message (SSL/TLS 방식)
  - ✓ 0x01 : CA Token Response Message (SSL/TLS 방식)
  - ✓ 0x10 : CA Token Request Message (전자 봉투 방식)
  - ✓ 0x11 : CA Token Response Message (전자 봉투 방식)
  - ✓ Others are reserved.
- **Length** (4 bytes): Version, Type, Command, Length를 제외한 나머지 부분의 길이 (Result부터 암호화된 CA Token까지의 길이를 의미한다.)
- **Result** (1 byte): Request Message의 처리 결과로, 여기에서는 항상 '0x00'를 사용한다.
  - ✓ 0x00 : Success
  - ✓ 0x01 : Failure
  - ✓ Others are reserved.

11.2.1.2 CA Token Format

CA Token Format은 iCAS 표준[6] 3.5.1절 내의 CA Token Format을 사용하되, 방송망 환경 적용을 위해 아래와 같이 일부 수정한다.

- **Device ID** (32 bytes): CA Token을 발급 요청한 Device ID로, 상위 4 bytes를 Model Type ID, 하위 28 bytes를 Device SN(Serial Number)으로 구분해서 사용한

다.

- ✓ Device SN 값의 모든 bits가 0값을 갖는 경우 해당 모델의 모든 수신기를 지칭한다.

- **Number of Content ID** (4 bytes): Content ID의 개수
  - ✓ 값이 0일 경우 하위 Content ID 리스트 항목은 생략한다.
  - ✓ 값이 0일 경우는 모든 서비스를 시청할 수 있다는 의미로 해석한다.

11.2.2 CA Token Revocation List

CTRL (CA Token Revocation List)은 그림 11-3과 같이 iCAS 표준[6] 중 3.5.2절 CA Token Revocation List (CTRL) 내의 CTRL Format을 따르되 방송망 환경 적용을 위해 아래와 같이 일부 수정한다.

(msb) (lsb)

bit	7	6	5	4	3	2	1	0
0	Version(1byte)							
1 2 3	CTRL Length(3bytes)							
4 5 6 7	CTRL Issuer ID(4bytes)							
8 ... 15	CTRL Issue Date(8bytes)							
16 ... 23	CTRL Next Issue Date(8bytes)							
24 25 26 27	Number of Revoked (CA Token ID + Device ID) (=n) (4bytes)							
28 ...	(Revoked (CA Token ID 1 + Device ID 1) || ... || Revoked (CA Token ID n + Device ID n)) (n * 40bytes)							
O1	Signature Algorithm (1byte)							
O1 + 1 O1 + 2 O1 + 3	Signature Length (=z) (3bytes)							
O1 + 4 ...	Signature (z bytes)							

※ O1=(n*40) + 28

그림 11-3. CTRL Format (iCAS 표준[6]에서 발췌 후 수정)

- **Version** (1 byte): CTRL의 version을 의미하며, DP 시스템에서는 '0x20'를 사용한다.
- Number of Revoked CA Token ID와 (Revoked CA Token ID 1|| ... || Revoked CA Token ID N)는 각각 다음과 같은 두 항목으로 변경 한다.
  - ✓ Number of Revoked (CA Token ID + Device ID) (=n) (4bytes) : Revoked (CA Token ID + Device ID) 의 수
  - ✓ (Revoked (CA Token ID 1 + Device ID 1) || ... || Revoked (CA Token ID n + Device ID n)) (n * 40bytes): Revoked CA Token ID의 목록으로, Number of Revoked (CA Token ID + Device ID) 만큼 Revoked (CA Token ID + Device ID)를 포함한다. Revoked (CA Token ID 1 + Device ID 1)는 첫 번째 Revoked ID, Revoked (CA Token ID n + Device ID n)은 n번째 Revoked ID를 의미한다.

11.2.3 UHDCP 클라이언트 이미지

UHDCP 클라이언트 이미지 전송을 위한 메시지는 iCAS 표준[6]의 3.6.2절 CAS S/W Response를 따른다. 그러나 방송망 환경에서 동작하기 위해 SSL/TLS 방식이 아닌 전자봉투 방식으로 메시지를 보호하여 보내고, 이를 위해 iCAS 표준의 CAS S/W Response 메시지의 마지막 부분에 Signature Algorithm, Signature Length, Signature를 추가한다.

(msb) (lsb)

bit	7	6	5	4	3	2	1	0
0	Version(1byte)							
1	Type(1bytes)							
2 3	Command(2bytes)							
4 5 6 7	Length(4bytes)							
8	Result(1byte)							
9 10 11	Reason(3bytes)							
12 ... 43	DeviceID(32bytes)							
44 ... 75	newDynId(32bytes)							
76	Response Type(1byte)							
77 78 79	Response Length(3bytes)							
80 81 82 83	CAS SW ID(4bytes)							
84 ...	CAS SW Package(Response Length – 4)							
O1	Signature Algorithm (1byte)							
O1 + 1 O1 + 2 O1 + 3	Signature Length (=z) (3bytes)							
O1 + 4 ...	Signature (z bytes)							

※ O1= (Response Length) + 80

그림 11-4. CAS S/W Response Message (iCAS 표준[6]에서 발췌 후 수정)

- **Version** (1 byte): 현재 Message의 version을 의미하며, DP 시스템에서는 '0x20'을 사용한다.

- **Type** (1 byte): 다음 Command의 분류를 위해 사용한다.
  - ✓ 0x00 : CA Token Command
  - ✓ 0x01 : CAS S/W CAS SW Command
  - ✓ 0x02 : 단방향 환경에서의 CA Token Command
  - ✓ 0x03 : 단방향 환경에서의 CAS SW Command
  - ✓ Others are reserved.
- **Command** (2 bytes): 전송 메시지 구분을 위한 세부 Command를 의미하며, 방송망 환경의 DP 시스템에서는 '0x03'을 사용한다.
  - ✓ 0x00 : CAS SW Request Message
  - ✓ 0x01 : CAS SW Response Message
  - ✓ 0x02 : CAS SW Acknowledgement Message
  - ✓ 0x03 : CAS SW Response Message(전자 봉투 방식)
  - ✓ Others are reserved.
- **Length** (4 bytes): Version, Type, Command, Length를 제외한 나머지 부분의 길이 (Result부터 Signature까지의 길이를 의미한다.)
- **Result** (1 byte): Request Message의 처리 결과를 의미하며, 여기에서는 항상 '0x00'을 사용한다.
  - ✓ 0x00 : Success
  - ✓ 0x01 : Failure
  - ✓ Others are reserved.
- **Device ID** (32 bytes): CAS S/W 갱신 대상이 되는 Device ID를 의미하며, 상위 4 bytes를 Model Type ID, 하위 28 bytes를 Device SN(Serial Number)으로 구분한다.

- ✓ Device SN 값의 모든 bits가 0값을 갖는 경우 해당 모델의 모든 수신기를 지칭한다

- **New Dynamic ID** (32 bytes): 방송망 환경에서 Dynamic ID는 사용되지 않으며, 여기서는 항상 '0x00'을 사용한다. 즉, 단방향에서는 Clone Detection은 동작하지 않는다.

- **Signature Algorithm** (1 byte): Signature Algorithm

  - ✓ 0x00: RSASSA-PSS-SHA1 (PKCS #1 :RSA Cryptography Standard" Version 2.1)

  - ✓ 0x01: EC-DSA

  - ✓ Others are reserved.

- **Signature Length** (3 bytes): Signature의 길이

- **Signature** (Signature Length bytes): 본문(Version부터 CAS S/W Package까지)에 대한 서버의 서명값

12. 포렌식 워터마킹 정보

본 장에서는 지상파 UHDTV 방송프로그램 보호를 위한 포렌식 워터마킹 정보 값을 정의한다.

워터마킹 기술은 멀티미디어 저작물에 소유권자의 저작권 정보를 워터마크로 삽입하고 불법 복제된 저작물에서 워터마크를 다시 추출함으로써 소유권을 주장할 수 있도록 하는 기술이다. 이는 사전적 보호시스템인 DRM과 상호 보완적인 수단으로 활용될 수 있다. 포렌식 워터마킹은 워터마킹 기술의 확장 기술로 저작물에 소유자의 정보 뿐만 아니라 수신자의 정보도 포함하도록 하여 불법 배포가 어느 수신자로부터 시작되었는지를 추적 할 수 있도록 하는 저작권 보호기술이다. 포렌식 워터마킹은 디지털 콘텐츠가 불법적으로 무단 복제된 경우, 콘텐츠 제공자로 하여금 복제된 복사본의 원 수신자를 식별할 수 있는 사후 검출기능을 제공함으로써, 수신자가 디지털 데이터를 불법적으로 배포하지 못하도록 보호한다.

지상파 UHDTV 수신기에서 외부 디지털 출력 시 지상파 UHDTV 방송프로그램 보호를 위해 최소한의 포렌식 워터마킹을 해야하고, 그 정보는 표 12-1과 같이 정의한다.

단, 720x480 이하의 디지털 출력 시 포렌식 워터마킹을 적용하지 않을 수 있다.

표 12-1. 포렌식 워터마킹 정보 정의

항목	M/O	비고	예제
제조사 인덱스	M	디바이스 제조사를 구별 할 수 있는 Index	SS, LG, SN
Device Model Name (Number)	O	해당 디바이스의 모델명(모델 넘버)	S55xxxxx, L55xxxxx
Watermark ID	M	해당 디바이스 또는 세션을 구분/구별 할 수 있는 ID. 양방향의 경우 License 서버가 발급한 유일한 Unique ID 이어야 함.	UHDCP ID, Session ID

부 속 서 (Annex)

A. CPT XML 스키마 정의

표 8-2에서 정의한 CPT의 XML 스키마 정의는 다음과 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:cpt="http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Delivery/CPT/1.0/"
  xmlns:routesls="http://www.atsc.org/XMLSchemas/ATSC3/Delivery/ROUTESLS/1.0/"
  targetNamespace="http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Delivery/CPT/1.0/"
  elementFormDefault="qualified">
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
    schemaLocation="http://www.w3.org/2001/xml.xsd"/>
  <xs:import namespace="http://www.atsc.org/XMLSchemas/ATSC3/Delivery/ROUTESLS/1.0/"
    schemaLocation="ROUTESLS.xsd"/>
  <xs:element name="CPT" type="cpt:cptType"/>
  <xs:complexType name="cptType">
    <xs:sequence>
      <xs:element name="CP" type="cpt:cpType" minOccurs="1" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="bsid" type="xs:unsignedShort" use="required"/>
  </xs:complexType>
  <xs:complexType name="cpType">
    <xs:sequence>
      <xs:element name="BroadcastDelivery" type="cpt:BroadcastDeliveryType" minOccurs="0"
        maxOccurs="unbounded"/>
      <xs:element name="InetUrl" type="cpt:URLType" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="operatorId" type="xs:unsignedByte" use="required"/>
    <xs:attribute name="cpUuid" type="cpt:UUID" use="required"/>
  </xs:complexType>
  <xs:complexType name="BroadcastDeliveryType">
    <xs:sequence>
      <xs:element name="SrcFlow" type="routesls:srcFlowType" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="dataType" type="xs:unsignedByte" use="required"/>
```

```
    <xs:attribute name="dataSeqNum" type="xs:unsignedByte" use="optional"/>
    <xs:attribute name="cpProtocol" type="xs:unsignedByte" use="required"/>
    <xs:attribute name="plpId" type="cpt:PLPIdType" use="required"/>
    <xs:attribute name="dIpAddr" type="cpt:AddressType" use="required"/>
    <xs:attribute name="dPort" type="cpt:PortType" use="required"/>
    <xs:attribute name="sIpAddr" type="cpt:AddressType" use="required"/>
    <xs:attribute name="tsi" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="bw" type="xs:unsignedInt" use="optional"/>
  </xs:complexType>
  <xs:complexType name="URLType">
    <xs:simpleContent>
      <xs:extension base="xs:anyURI">
        <xs:attribute name="dataType" type="xs:unsignedByte" use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
  <xs:simpleType name="UUID">
    <xs:restriction base="xs:string">
      <xs:pattern value="[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="PLPIdType">
    <xs:restriction base="xs:unsignedByte">
      <xs:maxInclusive value="63"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="AddressType">
    <xs:restriction base="xs:token">
      <xs:pattern value="(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])₩.){3}([0-9]|[1-9][0-9]|1[0-
9][0-9]|2[0-4][0-9]|25[0-5])"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="PortType">
    <xs:restriction base="xs:unsignedShort">
      <xs:minInclusive value="1"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

B. CMI XML 스키마 정의

표 9-3에서 정의한 SLS USBD의 CMI XML 엘리먼트와 표 9-4에서 정의한 Service Announcement의 CMI XML 엘리먼트에 대한 XML 스키마 정의는 다음과 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:cmi="http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Protection/CMI/1.0/"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  targetNamespace="http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Protection/CMI/1.0/"
  elementFormDefault="qualified">
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
    schemaLocation="http://www.w3.org/2001/xml.xsd"/>
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
  <xs:element name="ContentManagementInfo" type="cmi:ContentManagementInfoType"/>
  <xs:complexType name="ContentManagementInfoType">
    <xs:sequence>
      <xs:element name="RedistributionControlCode"
        type="cmi:RedistributionControlCodeType" minOccurs="1" maxOccurs="1"/>
      <xs:element name="Signature" type="ds:SignatureType" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:unsignedShort" use="required"/>
    <xs:attribute name="redistributionArea" type="xs:unsignedByte" use="required"/>
  </xs:complexType>
  <xs:complexType name="RedistributionControlCodeType">
    <xs:sequence>
      <xs:element name="RedistributionCondition" type="cmi:RedistributionConditionType"
        minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="code" type="cmi:CodeType" use="required"/>
  </xs:complexType>
  <xs:complexType name="RedistributionConditionType">
    <xs:attribute name="holdbackTime" type="cmi:holdbackTimeType" use="required"/>
    <xs:attribute name="allowedMaxResolution" type="cmi:allowedMaxResolutionType"
      use="required"/>
    <xs:attribute name="allowedCopy" type="cmi:allowedCopyType" use="required"/>
  </xs:complexType>
```

```
  <xs:simpleType name="CodeType">
    <xs:restriction base="xs:unsignedByte">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="3"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="holdbackTimeType">
    <xs:restriction base="xs:unsignedByte">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="7"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="allowedMaxResolutionType">
    <xs:restriction base="xs:unsignedByte">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="3"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="allowedCopyType">
    <xs:restriction base="xs:unsignedByte">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="3"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

C. DP Message XML 스키마 정의

표 11-1에서 정의한 DP Message의 XML 스키마 정의는 다음과 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:dpm="http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Protection/DPM/1.0/"
  xmlns:routesls="http://www.atsc.org/XMLSchemas/ATSC3/Delivery/ROUTESLS/1.0/"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  targetNamespace="http://www.nextb.or.kr/XMLSchemas/T-UHDTV/Protection/DPM/1.0/"
  elementFormDefault="qualified">
```

```
<xs:import namespace="http://www.w3.org/XML/1998/namespace"
  schemaLocation="http://www.w3.org/2001/xml.xsd"/>
<xs:import namespace="http://www.atsc.org/XMLSchemas/ATSC3/Delivery/ROUTESLS/1.0/"
  schemaLocation="ROUTESLS.xsd"/>
<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
  schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<xs:element name="DPM" type="dpm:DpmType"/>
<xs:complexType name="DpmType">
  <xs:sequence>
    <xs:element name="DpInfo" type="dpm:DpInfoType" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Ctrl" type="dpm:CatCtrlType" minOccurs="0" maxOccurs="1"/>
    <xs:element name="DeliveryInfo" type="dpm:DeliveryInfoType" minOccurs="0"
      maxOccurs="unbounded"/>
    <xs:element name="Signature" type="ds:SignatureType" minOccurs="1" maxOccurs="1"/>
  </xs:sequence>
  <xs:attribute name="operatorId" type="dpm:OperatorIdType" use="required"/>
  <xs:attribute name="version" type="xs:unsignedShort" use="required"/>
</xs:complexType>
<xs:complexType name="DpInfoType">
  <xs:sequence>
    <xs:element name="ServiceList" type="dpm:ServiceListType" minOccurs="1"
      maxOccurs="1"/>
    <xs:element name="DeviceList" type="dpm:DeviceListType" minOccurs="1"
      maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="ServiceListType">
  <xs:sequence>
    <xs:element name="Service" minOccurs="1" maxOccurs="unbounded">
      <xs:complexType>
        <xs:attribute name="globalServiceID" type="xs:anyURI" use="required"/>
        <xs:attribute name="serviceId" type="xs:unsignedShort" use="required"/>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="DeviceListType">
  <xs:sequence>
    <xs:element name="Device" type="dpm:DeviceType" minOccurs="1"
```

```
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="DeviceType">
    <xs:sequence>
      <xs:element name="Dpm" type="dpm:DeviceDpmDpcType" minOccurs="0"
        maxOccurs="1"/>
      <xs:element name="Dpc" type="dpm:DeviceDpmDpcType" minOccurs="0"
        maxOccurs="unbounded"/>
      <xs:element name="Cat" type="dpm:CatCtrlType" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="modelType" type="dpm:ModelTypeHexaType" use="required"/>
  </xs:complexType>
  <xs:complexType name="DeliveryInfoType">
    <xs:sequence>
      <xs:element name="BroadcastDelivery" type="dpm:BroadcastDeliveryType" minOccurs="0"
        maxOccurs="1"/>
      <xs:element name="InetUrl" type="xs:anyURI" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="id" type="xs:anyURI" use="required"/>
    <xs:attribute name="type" type="dpm:DeliveryInfoDataType" use="required"/>
    <xs:attribute name="sysUuid" type="dpm:UUID" use="required"/>
  </xs:complexType>
  <xs:complexType name="DeviceDpmDpcType">
    <xs:attribute name="sysUuid" type="dpm:UUID" use="required"/>
    <xs:attribute name="version" type="xs:string" use="required"/>
    <xs:attribute name="refUri" type="xs:anyURI" use="optional"/>
  </xs:complexType>
  <xs:complexType name="CatCtrlType">
    <xs:attribute name="version" type="xs:string" use="required"/>
    <xs:attribute name="refUri" type="xs:anyURI" use="optional"/>
  </xs:complexType>
  <xs:complexType name="BroadcastDeliveryType">
    <xs:sequence>
      <xs:element name="SrcFlow" type="routesls:srcFlowType" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="plpId" type="dpm:PLPIdType" use="optional"/>
    <xs:attribute name="dIpAddr" type="dpm:AddressType" use="optional"/>
```

```
    <xs:attribute name="dPort" type="dpm:PortType" use="optional"/>
    <xs:attribute name="sIpAddr" type="dpm:AddressType" use="optional"/>
    <xs:attribute name="tsi" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="bw" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="Content-Location" type="xs:anyURI" use="optional"/>
  </xs:complexType>
  <xs:complexType name="URLType">
    <xs:simpleContent>
      <xs:extension base="xs:anyURI">
        <xs:attribute name="dataType" type="xs:unsignedByte" use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
  <xs:simpleType name="OperatorIdType">
    <xs:restriction base="xs:unsignedByte">
      <xs:maxInclusive value="127"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="UUID">
    <xs:restriction base="xs:string">
      <xs:pattern value="[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="PLPIdType">
    <xs:restriction base="xs:unsignedByte">
      <xs:maxInclusive value="63"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="AddressType">
    <xs:restriction base="xs:token">
      <xs:pattern value="(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])₩.){3}([0-9]|[1-9][0-9]|1[0-
9][0-9]|2[0-4][0-9]|25[0-5])"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="PortType">
    <xs:restriction base="xs:unsignedShort">
      <xs:minInclusive value="1"/>
    </xs:restriction>
  </xs:simpleType>
```

```
  <xs:simpleType name="ModelTypeHexaType">
    <xs:restriction base="xs:hexBinary">
      <xs:maxLength value="8"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="DeliveryInfoDataType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="dpm"/>
      <xs:enumeration value="dpc"/>
      <xs:enumeration value="cat"/>
      <xs:enumeration value="ctrl"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

부 록 (Appendix)

A. UHDTV 콘텐츠 공통 암호화 CENC (Informative)

CENC (Common Encryption)는 ISOBMFF에 대한 암호화 방식(Encryption Method), 암호화 키 맵핑(Key Mapping) 방법, 암호화 메타데이터(Encryption Metadata) 표시 방법을 포함하는 공통 암호화 표준이다. 이 표준은 서로 다른 UHDCP (CAS 또는 DRM) 시스템들이 자신만의 암호화 방법이 아닌 공통의 방법으로 ISOBMFF의 암호화/복호화가 가능하도록 하고 각 UHDCP는 암호화 방법보다는 키 관리(복호화 키 획득 방법, 저장 방법 등)와 접근 권한(Rights, License 등) 관리에 초점을 맞출 수 있도록 한다.

CENC는 AES (Advanced Encryption Standard) 128 bits 암호화 알고리즘 이용하여 ISOBMFF Segment 내 각 샘플을 암호화 한다. 암호화 방법으로 1) AES-CTR (Counter Mode) 128 bits 기반의 'cenc' Protection Scheme과 2) AES-CBC (Cipher-Block Chaining Mode) 128 bits 'cbc1' Protection Scheme (Not mandatory)을 정의하고 있다.

각 샘플 암호화 시 사용한 암호화 키의 식별자, 초기화 벡터(Initialization Vector), 암호화 된 데이터의 부분 표시 등 공통 암호화 메타데이터를 ISOBMFF Segment에 표시할 수 있다. 그리고 각 UHDCP의 특유의 정보(예를 들어 UHDCP 시스템 식별자, 접근 권한 취득 URL, 접근 제어 및 권한 데이터 등)는 Protection System Specific Header box ('pssh')를 통해 표시할 수 있다.

CENC에서는 각 샘플 암호화 방법으로 전체 샘플 암호화(Full Sample Encryption)과 부샘플 암호화(Subsample Encryption) 방법을 지원한다. 전체 샘플 암호화는 ISOBMFF Segment의 'mdat'에 있는 각 샘플 단위로 암호화 하되 하나의 샘플의 모든 데이터 영역을 암호화 하는 것을 말한다. 부샘플 암호화는 샘플을 연속된 여러 부샘플(Subsamples)로 분할하고 각 부샘플은 비암호화 부분(Unencrypted Part)와 암호화 부분(Encrypted Part)로 구성한다. 샘플의 암호화 부분에 대해서 AES-CTR 128 bits로 암호화를 하고 비암호화 부분에 대해서는 암호화를 하지 않는다. 부샘플 암호화는 NAL 구조의 비디오 샘플 암호화 시 이용할 수 있으며 NAL 길이 필드, nal_unit_type 필드는 비암호화 부분으로, Slice NAL에 있는 비디오 데이터는 암호화 부분으로 구분한다.

CENC에 대한 세부적인 기술 정보는 CENC 표준[1]을 참조한다.

B. 포렌식 워터마킹 기술 성능 평가 항목 및 방법 (Informative)

본 부록 B에서는 지상파 UHDTV 방송 프로그램 보호를 위해 적용할 수 있는 포렌식 워터마킹 기술의 성능평가 항목 및 방법에 대해 기술한다.

워터마킹 기술은 멀티미디어 저작물에 소유권자의 저작권 정보를 워터마크로 삽입하고 불법 복제된 저작물에서 워터마크를 다시 추출함으로써 소유권을 주장할 수 있도록 하는 기술이다. 이는 사전적 보호 시스템인 DRM과 상호 보완적인 수단으로 활용될 수 있다. 포렌식 워터마킹은 워터마킹 기술의 확장 기술로 저작물에 소유자의 정보뿐만 아니라 수신자의 정보도 포함하도록 하여 불법 배포가 어느 수신자로부터 시작되었는지를 추적 할 수 있도록 하는 저작권 보호기술이다.

이러한 포렌식 워터마크 기술에 대한 성능평가가 필요한 이유는 포렌식 워터마크로 사용되는 기술에 대한 객관적인 방법을 제공하여 방송국과 UHDTV 수신기 제조업체가 기술을 선택하는데 도움을 주고자 한다. 본 기고서에서 제안된 성능평가 항목은 "콘텐츠 포렌식마크 호환을 위한 추출/판별 기술 (TTAK.KO-12.0118)" 항목 중에서 현재 시장에서 요구하는 항목을 위주로 선택, 보강하여 기술되었다.

B.1. 비디오 포렌식마크 성능 기술 평가 항목

Item	Type of Attack	Description
1	Frame rate Conversion	120p or 60p에서 하위 Frame rate로 변경 시 Ex) 60→30, 24(fps), 120->60, 30, 24
2	D/A, A/D	디지털(Digital) 영상을 아날로그(Analog)로 변환하고, 재차 디지털로 변환 시 Digital → Analogue, Analogue ➔ Digital
3	Line-scan Conversion	Progressive→interlaced, interlaced→progressive
4	Noise Attack	White Gaussian Noise
5	Color space Conversion	입력 비디오 동영상으로부터 밝기 성분만을 가진 동영상을 생성 시 (YCbCr → Gray Scale)
6	Video format Conversion	HEVC로 부호화 된 동영상을 다른 Video 압축 포맷으로 변경 시
7	Codec/Bitrate Conversion	Change codec and each source video codec (MPEG2, MPEG4, AVC/H.264 , HEVC/H.265) and Bitrate Ex) Codec Bitrate(3840x2160 기준): MPEG-2, 20Mbps / H.264/AVC, 10Mbps / H.265/HEVC, 5Mbps
8	Resolution Conversion	3840x2160 UHD resolution에서 하위 resolution으로 변경 시 Ex) 3840x2160(1.78:1) → 1920x1080(1.78:1)

		3840x2160(1.78:1) → 1280x720(1.78:1) 3840x2160(1.78:1) → 720x480(1.50:1)
9	Aspect-ratio Conversion	3840x2160(1.78:1) 영상을 영상의 수평/수직 스케일 요소를 다르게 적용하여 변형 시 Ex) 3840x2160(1.78:1) → 958x720(1.33:1) 3840x2160(1.78:1) → 1080x720(1.5:1)
10	Rotation	영상을 다음의 각도로 회전 시 Ex) counter-clockwise rotation (< ± 5 deg)
11	Flipping	영상을 좌우 방향으로 플립 시 (horizontal flip)
12	Cropping	영상의 가장자리를 전체 영상에서 가로, 세로로 일부 제거 시 Ex) Cropping 10% of original video
13	Bits-depth change	입력된 10 비트(bit)의 동영상을 8 비트로 변환 시 (or 역 비트 변환) Ex) 8 bits <-> 10 bits

B.2. 오디오 포렌식마크 성능 기술 평가 항목

Item #	Type of Attack	Description
1	Low pass filter	< 6KHz
2	D/A, A/D	D/A, A/D converting twice
3	Change the number of channels	2Ch → Mono 7.1ch → Mono, 2ch 5.1ch → Mono, 2ch 10.2ch → Mono, 2ch
4	Amplitude compression	48kHz/24bit → 48kHz 20/16bit 48kHz/20bit → 48kHz 16bit
5	Noise addition	Adding white noise with constant level of 40 dB lower than total averaged music power
6	Changing the sample rate	96K → 48K/44.1K 48K → 44.1K
7	Echo addition	Maximum delay: 100ms Feedback coefficient: around 0.3
8	Cropping	180sec
9	Time scale modification	± 10%
10	Data compression (Codec/Bitrate)	MPEG-1 Layer 2, 3(128K) MPEG-2 ISO/IEC 13818-7, AAC(128K) MPEG-4 ISO/IEC 14496-3, LC-AAC, HE-AAC(128K) Dolby AC3(128K), E(128K)

		MPEG-H(96K/stereo) MPEG-H(208k/5.1ch) MPEG-H(384k/7.1.4ch)

차세대방송표준포럼단체표준(국문)

지상파 UHDTV 방송 송수신 정합 – 파트 5. 콘텐츠보호

(Transmission and Reception for Terrestrial UHDTV Broadcasting Service)
– Part 5. Content Protection

발행인 : 차세대방송표준포럼 의장

발행처 : 차세대방송표준포럼

06130 서울특별시 강남구 테헤란로 7 길 22 신관 1108 호

Tel : 02-568-3556, Fax : 02-568-3557

발행일 : 2016. 03. 30