

표준번호 TTA.KO-07.001

# 디지털 위성방송 제한수신 정합표준

(Standard of Conditional Access for Digital Satellite Broadcasting)



장규상

TTA 방송기술위원회(TC05) 부의장/한국통신 위성방송팀 부장

## 1. 개요

통합방송법 제정으로 무궁화위성을 이용한 본격적인 위성방송이 곧 제공될 예정이다. 위성방송은 다채널 유료방송을 중심으로 하는 상업방송이기 때문에 유료방송 시청관리를 위한 기술, 즉 요금을 지불한 가입자만이 특정 프로그램을 시청 가능하도록 하는 “제한수신(Conditional Access)시스템”을 필요로 한다. 오래 전부터 유료방송이 보급되어 운영중인 외국에서는 여러 종류의 상용 제한수신시스템이 사용되고 있으며, 국내에서는 케이블방송에서 아나로그 방식의 간단한 수신제한시스템이 사용되고 있다. 한국전자통신연구원에서 위성방송용 제한수신시스템을 개발하였으며 향후 상용화를 위한 충분한 현장시험을 통한 기능보완이 이루어질 것이다.

제한수신시스템은 특성상 극도의 보안이 요구되는 제품으로, 상호 기술공유 및 표준화가 어려워 서로 상이한 시스템이 시장에 혼재해 있는

상황이다. 디지털 위성방송의 송수신 정합규격은 국제적으로 DVB-S로 표준화 되었으나[1], 제한수신 규격은 위성방송이 상업방송인 관계로 일반적으로 국가 표준을 지정하지 않고 방송사업자가 선정하여 독자적으로 운영하고 있다. 유일하게 일본만 제한수신 국가표준을 제정하였으나 그 내용은 매우 일반적인 사항만 규정하고 있다. 국내에서도 위성방송 도입을 위한 제한수신 국가표준 제정을 위하여 1998년 1년간 TTA에서 관련업체 및 국내 전문가들이 참여하여 논의한 결과 본 표준을 만들게 되었다.

본 표준은 11/12GHz(Ku-band) 주파수 대역을 사용하는 디지털 위성방송에 제한수신 기능을 제공하기 위한 표준으로, 적용 범위는 송신기와 수신기에 필요한 인터페이스를 정의하고 있으며 다음과 같은 사항을 구현하는 것을 목적으로 하고 있다 :

첫째, 현재 및 향후 개발될 여러 방식의 제한수신 시스템들을 수용할 수 있어야 한다.

둘째, 각 제한수신 시스템들의 특성을 최대한 살리고, 다양한 서비스를 수용하여야 한다.

셋째, 여러 제한수신 시스템을 사용할 수 있도록 최소한의 인터페이스만을 규정한다.

2장에서 본 표준에 적용할 제한수신시스템의 구조와 기능을 설명하였고, 3장에서 본 제한수신 표준에서 정의하고 있는 아래의 인터페이스들을 설명하였다 :

- 스크램블 및 디스크램블 방식은 DVB-Common Scrambling 규격을 따른다.
- 제한수신 메시지인 EMM 전송위해(危害) CAT와 CA\_descriptor를 사용하고, ECM은

기존의 PMT에서 CA\_descriptor를 사용하여 전송한다.

- Return Path와 IC Card는 선택사항으로 정한다.
- 내장형(Embedded) 제한수신시스템을 기본으로 하며, CI(Common Interface) 방식은 선택사항으로 한다.

## 2. 디지털 위성방송 제한수신 시스템

그림 1은 디지털 위성방송 시스템과 제한수신 시스템의 구성 요소들과의 관계를 나타낸다. 압축된 비디오·오디오·데이터 스트림(stream)들은 선택적으로 암호화(scramble)되고, 서비스

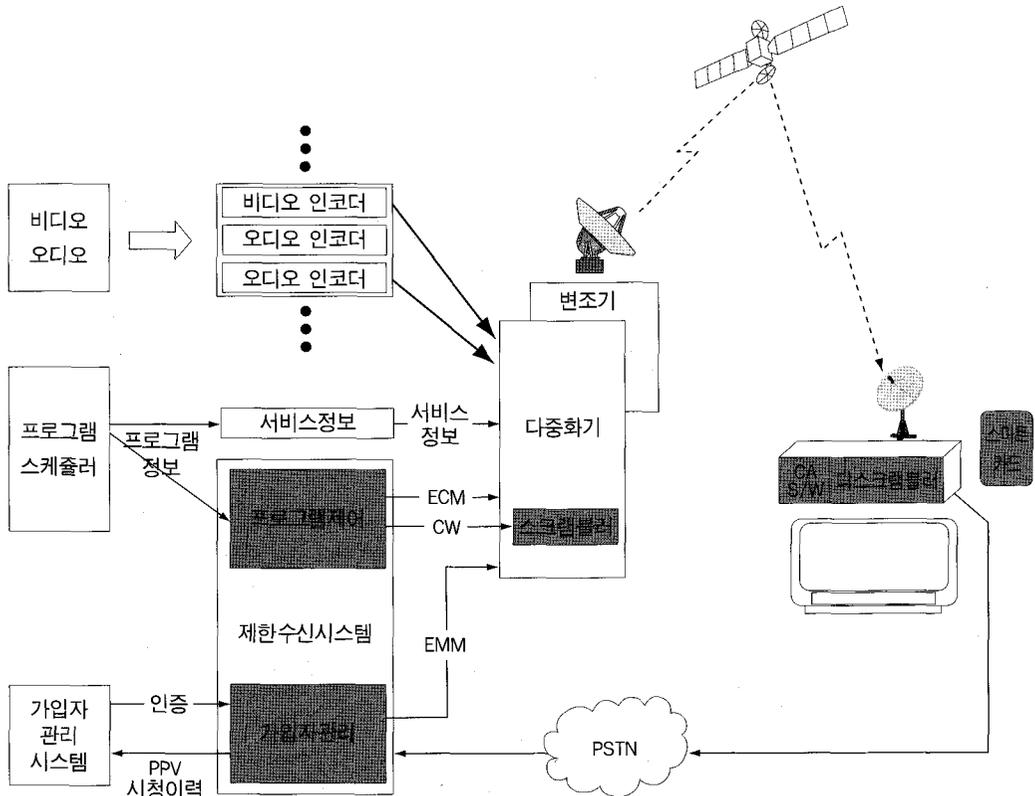


그림 1. 디지털 위성방송 시스템 및 제한수신 시스템

정보 및 제한수신 정보와 함께 트랜스포트 스트림(Transport Stream)으로 다중화된 후 위성을 통해 수신기로 전송된다. 수신기에서는 전송된 제한수신 정보와 IC 카드에 있는 보안 정보를 이용하여, 스트림의 어느 부분이 시청 가능 여부를 결정하고 필요한 부분의 역암호화(descramble)를 수행한다. 과금 및 시청률 조사를 위한 시청이력 데이터를 수집하기 위해 모델을 이용한 Return Path가 제공될 수 있다.

디지털 위성방송 시스템의 제한수신 기능은 다음과 같다.

- 프로그램 수신 제어기능 : 특정한 시청자격을 부여 받은 가입자에게 지정된 프로그램을 제공하기 위한 기능이며 이를 위하여 ECM (Entitlement Control Message)을 사용할 수 있다. ECM은 프로그램의 제한수신 특징을 나타내는 메시지이며 IC 카드가 프로그램을 역암호화(디스크램블) 하는데 필요한 CW(Control Word)를 생성한다.
- 가입자 자격 관리기능 : 가입자의 시청권한을 관리하기 위한 기능으로 이를 위하여 EMM (Entitlement Management Message)을 사용할 수 있다.

디지털 위성방송 시스템의 제한수신 구조는 다음과 같다.

디지털 위성방송의 제한수신 시스템은 송신국, 수신기, IC 카드 등으로 구성된다. 그림 1은 제한수신 시스템의 주요부분과 프로그램 관련 스트림(ECM, 서비스 정보) 및 가입자 관련 스트림(EMM)의 흐름을 나타낸다.

각 프로그램에 대한 가입자의 시청권한 정보를 포함하는 EMM 스트림은 다중화기로 전송된다. 프로그램의 제한수신 정보는 ECM에 의해 전달된다. CW는 프로그램 구성요소(비디오, 오디오, 데이터 등)를 암호화하고, 수신기가 프로그램을 역암호화(디스크램블)하기 위해 사용된다. 제한수신 시스템은 ECM과 CW를 다중화기로 전달하고, 다중화기는 ECM스트림 및 여

러 프로그램(비디오, 오디오, 데이터 등) 등을 다중화 하고, CW와 스크램블러를 이용하여 다중화된 스트림을 암호화(스크램블) 한다.

EMM, ECM, 서비스정보(SI)가 추가되어 스크램블된 트랜스포트 스트림은 위성을 통해 수신기로 전송된다[2].

디지털 위성방송의 스크램블된 프로그램을 시청하고자 하는 경우, 수신기는 MPEG표준에서 정의한 CAT(Conditional Access Table)에 할당된 PID(Packet Identifier)를 이용하여 EMM스트림을 찾아 해당 가입자의 EMM과 PMT(Program Map Table)에 할당된 PID를 이용하여 ECM 스트림내의 해당 프로그램 관련 ECM을 추출하고 처리한다. 시청하고자 하는 프로그램과 관련된 ECM의 제한수신 특성(parental rating, blackout 등)을 IC카드에 저장되어 있는 시청자격 정보와 비교하여 시청자격을 확인한다.

가입자 시청자격이 확인되면, IC카드는 스크램블링 시에 사용한 CW를 재구성하고, 수신기는 해당 프로그램과 관련된 스트림들(비디오, 오디오, 데이터 등)을 디스크램블 한다. 디스크램블된 스트림들은 MPEG 복호(디코딩) 후 TV, PC 등 외부 기기로 출력된다.

### 3. 제한수신 시스템의 인터페이스

위성방송 제한수신 시스템과 송·수신기간에 호환을 이룰 수 있도록 표준 인터페이스를 다음과 같이 정의한다.

#### 3.1 송·수신부 스크램블링 및 디스크램블링 방식

송·수신기에서는 스크램블링 및 디스크램블링 방식으로 DVB Common Scrambling Algorithm을 사용하며 상세 규격은 ETR 289

(Digital Video Broadcasting; Support for use of scrambling and Conditional Access(CA) within digital broadcasting systems)를 따른다[3].

### 3.2 제한수신 메시지

3.2.1 CAT 구문의 주요내용은 다음과 같다.

CAT 구문	비트 수	값
CA_section(){		
table_id	8	0x01
version_number	5	X
section_number	8	X
last_section_number	8	X
for(i = 0 : i < N : i++) {		
descriptor( )		
}		
}		

descriptor( )는 아래에 표시한 CA descriptor를 포함할 수 있다.

CAT descriptor 구문	비트 수	값
CA_descriptor(){		
descriptor_tag	8	0x09
CA_system_ID	16	X
CA_PID	13	X
for(i = 0 : i < N : i++){		
private_data_byte	8	X
}		
}		

CA\_system\_ID : 각 제한수신 시스템을 구별하기 위해 사용하는 구별자

CA\_PID : EMM(또는 ECM)이 전송되는 트랜스포트 스트림 패킷들의 PID

private\_data\_byte : 각 제한수신 시스템에서 정의하여 사용

### 3.2.2 PMT 구문 및 정의

PMT 내의 descriptor loop에 현재 방송되는 프로그램과 관련된 ECM의 CA descriptor들을 삽입한다. 비디오, 오디오 및 기타 프로그램에 관련된 스트림의 scrambling 여부는 TS 패킷 헤더에 있는 scrambling\_control bit field에서 정의한다. 단, CA\_PID는 ECM이 전송되는 패킷의 PID를 의미한다.

MPEG-2 시스템에서 정의된 PMT의 주요내용은 다음과 같은 형식을 따른다.

PMT 구문	비트 수	값
TS_program_map_section(){		
table_id	8	0x02
program_number	16	X
version_number	5	X
PCR_PID	13	X
for(i = 0; i < N; i++) {		
descriptor()		
}		
for(i = 0; i < N1; i++) {		
stream_type	8	X
elementary_PID	13	X
ES_info_length	12	X
for(i = 0; i < N2; i++){		
Descriptor() }		
}		
}		

program\_number : 프로그램을 지정하는 번호

PCR\_PID : 프로그램 번호에 의해 지정된 프로그램에 맞는 PCR정보를 포함하는 TS packet들의 PID값

stream\_type : elementary\_PID에 의해 지정되는 패킷들이 전달하는 프로그램 요소의 형태

elementary\_PID : 관련된 프로그램 요소(비

디오, 오디오 등)를 전달하는 TS 패킷들의 PID

### 3.2.3 ECM

ECM은 수신기에서 CW를 얻기 위해 필요한 정보를 가지고 있다. ECM의 PID는 선택된 서비스 스트림의 PMT 섹션에서 찾으며, 각 제한수신 시스템에 할당된 CA\_system\_ID에 따라 결정되는 서로 다른 PID를 갖는다.

CA\_system\_ID는 제한수신 시스템이 하나 이상일 경우 사용한다. 2바이트로 구성되며 상위 1바이트는 제한수신 시스템을 구별하는 ID이고, 하위 1바이트는 제한수신 시스템별로 사용할 수 있는 값이다.

### 3.2.4 EMM

EMM 필드의 형식과 구체적인 사용 방법은 각 제한수신 시스템별로 정의하여 사용한다. 다만 각 제한수신 시스템의 요구에 의하여 정의된 EMM 메시지에 각 제한수신 시스템의 CA\_system\_ID에 따른 PID를 할당하고 수신기로 다중화하여 전송한다. 이때, 각 제한수신 시스템에서 정의한 메시지는 타 제한수신 시스템에 영향을 주지 않아야 한다.

## 3.3 Return Path

각 제한수신 시스템은 수신기를 관리하고 부가 서비스 등을 제공하기 위하여 모뎀 등을 이용한 Return Path를 사용할 수 있다. Return Path의 기본 기능은 Pay-Per-View(PPV)에 대한 가입자 시청정보 업로드 등이다.

## 3.4 Common Interface

수신기에서 제한수신 기능을 구현하기 위하

여 Common Interface를 사용할 수 있다[4].

## 3.5 IC 카드

수신기에서 제한수신 기능을 구현하기 위하여 IC 카드를 사용할 수 있다.

IC 카드의 기계적 특성은 ISO 7816-1[5] “접점이 있는 집적회로 ID 카드의 설계 및 사용”에 명시된 규정을 따른다.

IC 카드의 접점 특성은 ISO 7816-2에서 정의한 “접점 위치와 최소 크기”의 규정을 따른다.

카드의 접점은 카드의 세로축에 가까이 위치해 있으며, 접점은 카드의 앞쪽에 위치한다. 즉, 카드는 접점이 있는 모서리가 먼저 삽입된다.

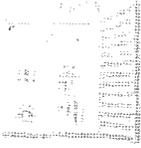
IC 카드는 8개의 접점을 가지고 있으며, 접점은 다음의 신호를 제공한다.

기호	접점	설명
VCC	C1	전원
RESET	C2	Low active reset
CLK	C3	System clock
Reserved	C4	Reserved
GND	C5	Ground
VPP	C6	Programming voltage
I/O	C7	Input/output
Reserved	C8	Reserved

VCC, RESET, CLK, I/O는 ISO 7816-3의 규정에 적합하여야 한다.

IC 카드의 전송 프로토콜은 ISO 7816-3에 정의된 규정을 따른다.

ATR(Answer-to-Reset)의 기록 문자(Historical Character)는 카드에 대한 일반정보를 제공하는데 사용할 수 있다. 기록 문자의 일부는 수신기로 제한수신 시스템의 CA\_system\_ID를 전달하는데 사용할 수 있다. 단, 사용하는 경우 기록 문자의 영역은 모든 제한수신 시스템에서 동일해야 한다.



#### 4. 용어 설명

MPEG-2	ISO/IEC 13818를 지칭하며, 동화상의 압축/복원 및 전송에 대하여 명시한 규약이다. MPEG은 Motion Pictures Expert Group의 머릿글자를 딴 약어이다.
Pay-Per-View(PPV)	채널별로 설정할 수 있는 운영 형태의 하나로, 이 형태로 방송되는 채널은 방송 프로그램 단위로 가격을 설정할 수 있다. IC 카드 안에 시청정보가 기록된다. 수신기는 프로그램을 보여주기 전에 가입자에게 프로그램 수신을 허락하는 요구를 할 수 있다.
PID	Packet Identifier의 약어로, MPEG-2의 기본이 되는 패킷을 지칭한다.
PES	Packetized Elementary Stream의 첫 글자를 딴 약어로, MPEG-2규약에 따라 나누어진 Elementary Stream을 지칭한다.
사용량 정보	가입자가 시청한 pay-per-view 프로그램의 시청이력을 의미한다.
서비스정보(SI)	SI 데이터는 PSI 데이터와 프로그램 안내정보를 구성하는데 필요한 부가정보, 그리고 선택된 프로그램이 포함된 위성방송 반송파를 찾도록 수신기의 자동동조에 필요한 정보를 포함한다.
서비스 스트림	프로그램 서비스 스트림 혹은 데이터 서비스 스트림을 지칭한다.
IC 카드	특정 프로그램을 시청하기 위해서 필요로 하는 휴대가 편하고 작은 크기의 카드를 지칭하며, 수신기에 삽입하여 사용한다.
가입자	위성방송 시스템을 통하여 전달되는 서비스를 받을 수 있도록 가입된 사람을 의미한다.
트랜스포트 스트림	MPEG-2 규정에 부합하는 데이터 스트림으로, PES 혹은 PSI를 전송하는 188 바이트 크기의 패킷들의 스트림을 지칭한다.
제한수신 메시지	제한수신 시스템이 운영되는데 필요한 메시지로, EMM, ECM을 지칭한다.



#### 참고 문헌

- [1] ETSI/DVB Framing structure, channel coding and modulation for 11/12GHz satellite services, EN 300 421, ver 1.1.2., August 1997.
- [2] ETSI/DVB Specification for Service Information(SI) in DVB systems, EN 300 468, ver 1.3.1, February 1998.
- [3] ETR 289 : Digital Video Broadcasting(DVB); Support for use of scrambling and Conditional Access(CA) within digital broadcasting systems, October 1996.
- [4] ETSI/DVB Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, EN 50221, ver 1, February 1997.
- [5] ISO 7816 Standards for Smart Cards