특집

DTV용 DRM 기술 및 동향

김윤상, 이석필, 임태범, 정종진(전자부품연구원)

I. 서 론

인터넷/디지털 시대의 도래는 Analog to Digital 변환의 용이함과 압축 기술의 비약적인 발전(예: DivX, mp3)을 가져다줌으로 인해 디지털 콘텐츠의 저장 및 배포가 용이한 실정이다. 방송환경 측면에서도 지난 수십 년간 지속되어 온 아날로그 방송시스템에서 디지털방송 시스템으로 변모해가는 과도기를 맞고 있다. 디지털 위성 본방송이 이미 시작하였으며, 지상파에서도 일부 프로그램을 고선명 디지털 프로그램으로 송출하고 있다. 또한 케이블방송 역시 디지털 방송 체계로의 전환을 서두르고 있다.

이러한 디지털 형태로의 변화 과정 속에서 디지털 콘텐츠 산업의 중요성이 날로 부각되어 가고 있으며, 이와 더불어 고부가가치의 디지털콘텐츠에 대한 지적재산권 보호 문제가 심각하게 대두되고 있는 실정이다. 디지털 콘텐츠는 아날로그 콘텐츠와는 달리 누구나 자신의 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있고, 복제품은 원본과 질적인 면에서 동일하며 확산 속도가 빠른 속성을 가지고 있다. 따라서 디지털 콘텐츠에 대한 불법복제, 저작권 침해, 기밀 누출이 상대적으로 용이한 실정이다. 이에 따라 불법 사용의 제한에 대한 디지털 콘텐츠 제공자들의 강력한 요구가 수반되면서, 이러한 문제점들을 극복하기 위하여 "DRM(Digital Right Management)" 기술들이 등장하였다.

DRM 기술은 미디어 특성 및 전달방식, 사용환경에 따라 여러 형태로 기술개발이 이루어져 왔다. 예를 들어 디지털 콘텐츠 전달방식에 따라서 사용되는 DRM 기술들을 간단하게 분류하면, 패키지화된 미디어에 담겨진 디지털 콘텐츠를 보호하기 위한 기술, 인터넷 환경에서 유통되고 소비되는 디지털 콘텐츠를 위한 기술, 핸드폰이나 모바일 기기에서 사용되는 디지털 콘텐츠 보호 기술, 디지털방송 환경에서 불법복제 및 무분별한 불법배포를 방지하기 위한 기술 등으로 분류할 수 있다. 이러한 기술들은 de-facto 표준 또는 국제표준화 기구들을 통하여 제조업체, 콘텐츠 제공자, 서비스 사업자 등의 여러 이해관계자들의 요구사항들을 수용하여 기기나 미디어, 전달경로에 쉽게 사용될 수 있게끔 특성화 하여 기술들을 발전시켜 나가고 있다.

본고에서는 디지털방송 환경에서 DTV를 중심으로 사용되고 있는 DRM 기술 및 동향, 주요

이슈사항들을 중심으로 살펴보고자 한다.

먼저 II절에서는 디지털방송 콘텐츠 전송 및 수신시 사용이 의무화 되어 있는 DRM 기술인 "CAS(Conditional Access System)"라고 불리 우는 제한수신시스템에 대하여 알아보고, 제 III절에서는 디지털 지상파 방송의 콘텐츠를 보호하기 위하여 진행되고 있는 복제방지 시스템 및 이슈사항들을 소개한다.

II. 디지털방송 제한수신 시스템 (CAS - Conditional Access System)

CAS는 사용자에게 유료방송을 시청할 수 있는 권한을 부여하는 시스템으로, 가입자가 시청료를 내면 그에 대한 서비스를 받을 수 있도록 제한하는 것이 주된 기능이다. 즉, 방송콘텐츠에 암호를 걸어 유선이나 위성, 인터넷 등을 통해 수신자 측으로 보내면, 받는 측이 시청료를 지불한 경우에 한해서만 암호를 풀 수 있는 권한을 부여함으로써 유료서비스를 가능하게 하는 기술이다. CAS의 주요기능은 스크램블링/디스크램블링(Scrambling/De-scrambling) 기능, 자격제어(Entitlement Control) 기능, 자격관리(Entitlement Management) 기능으로 나눌 수 있다[1].

- 스크램블링/디스크램블링(Scrambling/De-scrambling) 기능

수신자격이 없는 수신자는 시청이 불가능 하도록 콘텐츠를 암호화하여 보내며, 암호화된 방송 콘텐츠의 제어는 제어단어(Control Word)를 이용하여 암호화 및 복호화를 수행한다.

- 자격제어(Entitlement Control) 기능

CW를 인증키로 암호화하여 ECM(Entitlement Control Message, 자격제어메시지)에 실어서 수신자에게 전송한다. 보안을 위해 CW는 주기적으로 전송되며, 그때마다 새로운 CW가 생성되고 암호화 되서 전달된다. ECM에서는 암호화된 CW외에 제어변수(Control parameter)가 포함되며, 모든 수신기는 수신된 제어변수와 수신기의 인증변수(authentication parameter)를 비교하여 정당한 사용자로 판단될 경우에만 스마트카드 내의 비밀키를 이용하여 CW를 복호화하고, 이를 이용하여 수신된 콘텐츠를 디스크램블링 한다.

Access Parameter	Control Words	Hash Function

〈그림 1〉 ECM의 구성

- 자격관리(Entitlement Management) 기능

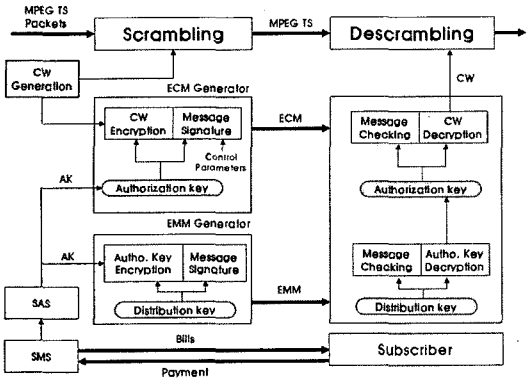
수신기에 자격을 부여/갱신/관리 하는 기능으로, 인증키를 분배키로 암호화하여 EMM (Entitlement Management Message, 자격관리메시지)을 생성하고 암호화하여 TS(Transport stresam) 패킷을 이용하여 수신측으로 전송한다. EMM은 수신기의 보안장치인 스마트카드에 자격을 부여하거나 갱신하는 기능을 한다.

Entitlement	Authorization Key	Hash Function

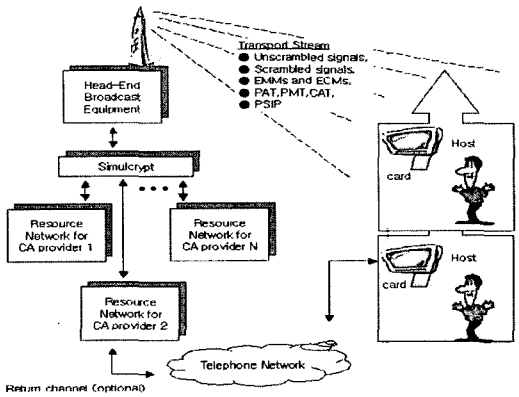
〈그림 2〉 EMM의 구성

CAS의 전체적인 구성도를 살펴보면 그림 3과 같다.

그림 3에서 먼저 EMM의 동작원리를 간략하



〈그림 3〉 CAS 구성도



〈그림 4〉 ATSC CAS 구성도

게 설명하면 다음과 같다. 수신자 고유의 분배키(DK)로 암호화된 인증키(AK)와 권한변수(Authorization parameter)에 전자서명을 추가한 EMM을 가입자의 수신기에 전송하고, 수신기에서는 EMM 변조여부 확인 후 이상이 없을시 인증키를 해독하여 ECM을 해석하기 위한 키를 얻을 수 있다. ECM에서는 제어단어(CW)를 인증키(AK)로 암호화하고, 제어변소(CP)가 포함된 ECM을 생성하여 전자서명을 수행한 후 수신부에 전송한다. 수신기에서는 전자서명을 검사하여 ECM의 변조여부를 확인하고, 인증변수 및 제어변수를 비교하여 정당한 가입자이면 EMM 해석을 통하여 얻은 인증키로 암호화된 제어단어를 복호화 하여 해당 프로그램을 디스크램블링 함으로서 원하는 방송콘텐츠를 시청할 수 있다.

이러한 CAS 기술을 사용하기 위해서는 디지털 방송 표준인 DVB(Digital Video Broadcasting), ATSC(Advanced Television system Committee), OpenCable에서 정한 인터페이스 및 콘텐츠 보호 규격을 만족해야 한다. 각각의 방송규격에서 요구하는 CAS 시스템에 대하여 간략하게 살펴보면 다음과 같다.

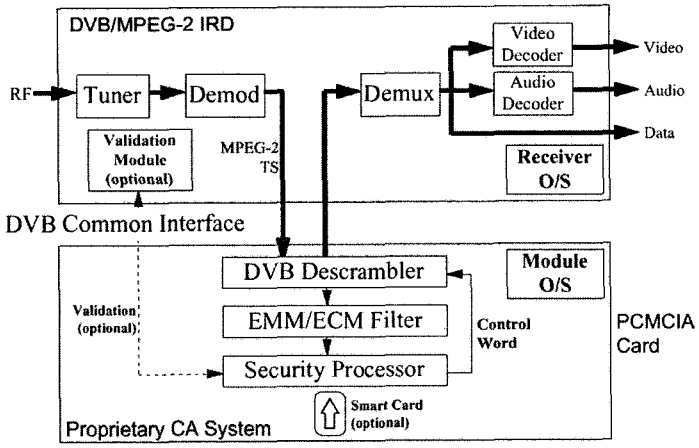
1. ATSC 제한수신시스템

ATSC에서 규격화된 CAS의 구성요소는 그림 4와 같다.

그림 4에서와 같이 ATSC에서는 하나의 프로그램에 여러 개의 CAS가 동시에 적용될 수 있는 Simulcrypt 방식을 채택하고 있다. 콘텐츠를 암호화하는데 사용되는 스크램블링 알고리즘은 168 bits의 키를 가진 CBC(Cipher Block Chaining) 모드의 Triple-DES가 규격화 되어 있다. 또한 수신부에서 사용되는 보안 인터페이스 모듈에 대한 규격은 두 종류를 허용하고 있다. 스마트카드 타입의 NRSS(National Renewable Security Standard)-A, PCMCIA 타입의 NRSS-B가 허용되어 있다. 수신기와 보안 모듈간의 통신규격에 대한 별도의 규정은 하지 않지만 대신 NRSS 사용을 의무화 하고 있다[2].

2. DVB 제한수신시스템

DVB에서 규격화된 CAS의 가장 큰 특징은 Simulcrypt 기술의 표준화이다. 이 기술은 여러 CAS 공급자를 수용하기 위하여 가입자의 수신

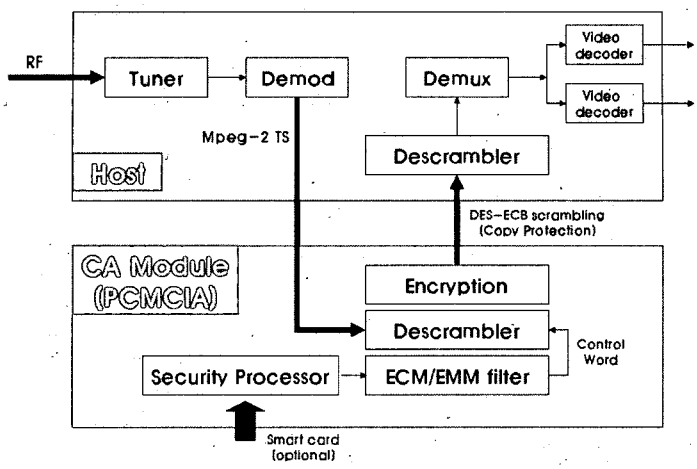


〈그림 5〉 DVB Common Interface 및 보안모듈 구성도

기에서 디스크램블링과 암호화 기능을 분리하여 디스크램블링 방식은 DVB-CSA(Common Scrambling Algorithm) 이라는 기술을 사용하도록 하고, 암호화 방법은 각 제한수신시스템마다 다르게 사용하도록 하여 가입자 수신기는 서로 다른 제한수신시스템을 갖는 보안 인터페이스 모듈을 수용할 수 있도록 하였다. DVB에서 쓰이는 CSA 기술은 MPEG-TS 스트림을 스크램블링 하는 방법으로 TS를 8 bytes 블록으로 구분하여 작동한다. 암호방법은 리버스 CBC 모드를 사용하여, 출력되는 값과 입력되는 값을 조합하는 스트림 암호를 사용한다. TS의 페이로드만 스크램블링 하여 전송하는 특성을 갖고 있다. 또한 서로다른 CAS를 구별하기 위하여 "CA System ID"에 대한 정의를 추가하였고, 이로 각각의 CAS 제공업자들을 구분하고 있다. 보안 인터페이스 모듈로서는 PCMCIA 타입의 카드를 사용하는 "Common Interface" 규격을 요구하고 있다. 방송 콘텐츠가 호스트에 수신되면 Common Interface를 통해 보안 모듈로 전송되며, 보안모듈 안에서 디스크램블 된 콘텐츠가 다시 스크램블 되어 호스트로 전송되는 방식으로 작동한다[3][4].

3. OpenCable 제한수신시스템

1998년 9월 FCC(Federal Communications Commission, 미연방통신위원회)에서 NRSS 표준규격을 제정하여 수신기와 PCMCIA와 같은 보안모듈의 분리를 제시하였으며, 2000년 3월 표준안에서 복제방지 장치에서 사용할 프로토콜과 기술들에 관하여 구체적으로 언급하였다. OpenCable의 제한수신시스템은 송신부의 시스템과 수신부의 호스와 분리된 POD(Point of Deployment)로 구성되어 있다. 기존의 디지털 방송 수신 장치 시스템에서는 암호화된 콘텐츠를 수신하여 복원하는 기능이 수신 장치 내부에 내장되어 있었으나 POD에서는 수신 장치로부터 분리한 별도의 보안 모듈로 정의하고 있다. OpenCable에서는 DVB나 ATSC와 같이 특정 암호 알고리즘을 표준으로 규정하지 않고, 수신기와 보안모듈 간의 인터페이스만을 규정하고



〈그림 6〉 Open Cable POD 복제방지시스템

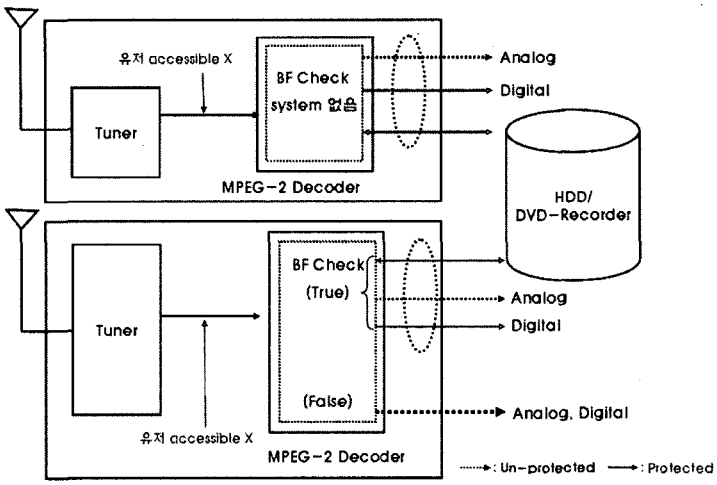
있다. 수신기와 보안모듈간의 인터페이스에는 인증서 (X.509) 기반의 상호인증을 기초로 하고 있으며, DFAST(Dynamic Feedback Arrangement Scrambling Technique) 기술이 사용된다. OpenCable 제한수신시스템의 구성은 그림 6와 같다[5][6].

III. 디지털지상파 복제방지 시스템

미국 디지털지상파(ATSC) 에서는 암호화 되어 있지 않은 디지털방송이 불법적으로 인터넷과 같은 장소로 배포될 때 막을 수 있는 기술적인 방법을 갖고 있지 않다. 이러한 문제점을 해결하기 위한 방법으로 권한이 없는 배포를 막고 각각의 출력마다 인증된 방식을 통해 암호화 하여 보내는 방식을 의무화 하기 위하여 FCC 에서는 단계적으로 그 관련 내용을 발표 하였다.

- 2002년 4월: 디지털 전환 이행 촉진을 위한 조치 강구
- 2002년 8월: 방송플래그(BF, Broadcast Flag)에 대한 검토 요구
- 2003년 11월: BF 규정 채택
- 2004년 8월: 13개의 디지털출력 보호기술 및 녹화방법을 승인
- 2005년 7월: 디지털지상파 수신기기의 BF 지원 의무화

특히 2003년 11월 발표한 "FCC Report and Order and Futher Notice of Proposed Rulemaking"에서는 디지털 지상파 방송 프로그램의 무차별적 재배포를 금지할 목적으로 2005년 7월 이후 출시되는 디지털 지상파 수신기기는 "BF(Broadcast Flag)"를 인식하여 동작하도록 의무화 하는 내용을 담고 있다[7]. 그러나 이에 반발한 각종 소비단체로부터 소비자 권익을 침해하는 월권행위로 FCC는 제소되고 2005년 5월 미 연방공소재판에서는 FCC가 방송플래그 대응 기기의 강제에 의해서 전파 수신후의 소비자의 행위를 규제하는 것은 FCC에 인정된 권한의 범위를 넘고 있다고 판결하였다. 이 판결로 PVR이나, Set-top-Box, DTV와 같은 디지털방송수



〈그림 7〉 방송플래그(Broadcast Flag) 동작 구조도

신기기를 만드는 가전업계나 PC에서는 방송플래그 대응의 데드라인이 사라져 한숨 돌리게 되었다. FCC 에서는 이에 대한 대응 방안을 여러 각도로 검토하고 있으며, 결국 미 의회에서 최종 결정권을 취하리라 예상된다. 그 동안에는 별도의 복제방지 기술 없이 표류 할 수 밖에 없는 실정이다.

1. 방송플래그(Broadcasst Flag) 개요

BF는 디지털지상파 방송 콘텐츠, MPEG-TS에 실려오는 1 bit 플래그의 부가정보이다. 암호화되지 않은 콘텐츠의 재분배 시에 인증된 방식으로 재분배 할 건지 아닌지를 결정하는 플래그이다. 콘텐츠를 복사 횟수에 상관없이 자유롭게 재분배 할 수 있으나 반드시 각 출력의 인증된 암호방법을 통해 이루어져야 한다. BF가 "true"일 경우 수신기는 콘텐츠를 분배할 때 인증된 방법으로만 가능하며, "false"인 경우 수신기는 어떠한 제약도 없이 원하는 출력을 통해 무한배포가 가능하다. 아날로그 신호의 출력은 제한이 없으며, 기존 아날로그 기기로 수신이 가능하다. 방송콘텐츠에 BF 내장 여부는 콘텐츠 제공자 및 방송국에서 BF를 추가할 지 여부를 결정한다. 유선이나 위성방송을 통한 지상파 프로그램의 재전송의 경우 지상파 프로그램에 추가된 BF가 손상 받지 않고 전달되도록 보장을 요구하고 있다.

그림 7은 디지털지상파 콘텐츠가 기기에 전송되서 출력할 때 BF가 어떻게 작동하는지를 나타낸 그림이다. BF 검사기능이 없는 기기는 BF 값에 상관없이 FCC에 의해 승인된 기술을 사용하여 출력 및 저장 할 수 있으며, BF 검사기능이 있는 기기는 BF 값이 "true"인 경우만 인증된 기술을 사용하여 출력 및 저장한다. 아날로그인 경우나 BF 값이 "false"인 경우는 아무런 제약 조건 없이 출력 및 저장이 가능하다[7].

2. FCC 승인 기술

2003년 11월 FCC에서는 BF 재정과 더불어 BF를 위한 디지털 출력 보호 및 녹화기술 제안을 업계에 요청하였다. 기술승인을 위한 주요한

〈표 1〉 FCC 승인기술

적용 분야	해당 기술	적용 Interface or Media	기술 Owner
Output Protection Technologies	DTCP	1394, IP, USB	DTLA(5C)
	HDCP	DVI, HDMI	Intel
	TiVoGuard	TCP/IP	TiVo
Recording Methods	CPRM	DVD RAM, -R/RW Disc	4C Entity
	ViDi	DVD +R/RW Disc	Philips
	MagicGate	Hi-MD, Memory Stick Pro	Sony
	D-VHS	VHS, S-VHS, D-VHS tape	JVC
Digital Rights Management Technologies	WM DRM	IP, USB	MS
	Helix	IP	RealNetwork
	SmartRight	Smart card	Thomson

판별요건으로서, 첫 번째 보안의 레벨, 재배포, 인증, 업그레이드 가능성, 갱신성, 상호호환성, 불법기기에 대한 폐기가 가능한 기술적인 요소를 포함하고 있는지에 대하여 검토를 하였으며, 두 번째로 응용 가능한 라이센스, Compliance and Robustness rule, 변경규정, 다운로드 및 녹화방법에 대한 승인절차, 라이센스 비용에 대한 타당성 여부를 점검 하였다. 세 번째로는 디지털 출력보호 기술 또는 녹화방법이 암호화되지 않은 지상파 방송 콘텐츠를 소비자가 즐기고 사용하는데 적합한 범위 안에 수용되어 있는지에 대하여 조사 하였다.

2004년 8월 FCC에서는 이러한 요구사항들을 만족시키는 13개의 디지털출력보호 기술과 녹화방법을 발표하였다. 표 1은 승인된 13개 기술을 간략하게 나타낸 표이다. 출력보호기술의 DTCP(Digital Transmission Content Protection), HDCP(High-Bandwidth Digital Content Protection), TiVoGuard, 녹화방법의 CPRM(Content Protection Recordablr Media), ViDi, MagicGate, Digital Rights Management 기술의 WM-DRM, Helix, SmartRight로 분류하여 승인된 기술을 보여 주고 있다[8].

상기 승인된 13개의 기술 외에도 향후 추가 제안이 가능하며, HDD와 같이 내장형 저장장치를 사용하여 녹화 시에는 승인된 기술 외에도 독자적으로 각각의 기기에 고유한 비밀값을 이용하여 디지털방송콘텐츠를 암호화 하고 저장이 가능하다.

Ⅳ. 맺음말

본 기고에서는 디지털방송 환경에서 사용되고 있는 DRM 기술 및 동향에 대하여 소개하였다. DVB, ATSC, OpenCable 각각의 방송규격은 독자적이면서도 유사한 제한수신시스템으로 콘텐츠를 보호하고 있으며, 미국디지털 지상파 콘텐츠인 경우 암호화 되어 있지 않은 콘텐츠를 보호하기 위해 FCC의 방송플래그 도입을 추진하고 있다.

디지털방송콘텐츠를 보호하기 위하여 사용되는 기술 자체의 자세한 내용보다도 어떠한 이유로 이러한 기술들이 도입이 되었고, 각각의 방송규격에 대한 DRM 기술은 어떠한 특징을 갖고 시스템을 구성하고 있는지와 현황 및 전망에 대하여 자세히 살펴 보았다.

이전에는 인터넷으로 연결된 PC 에서만 디지털 콘텐츠의 이용이 가능하였지만 이제는 디지털 방송 및 디지털 홈 네트워킹을 통해 가전기기 또는 모바일 기기에서도 디지털 콘텐츠 이용이 확산되고 있으며, 이러한 콘텐츠들을 보호하기 위하여 다양한 디지털 콘텐츠보호 기술이 개발되고 있다. 따라서 현재까지 인터넷 기반의 PC 플랫폼을 중심으로 발전되어 왔던 DRM 기술도 디지털 방송환경의 다양한 요구사항을 만족하기 위하여 신규기술에 대한 새로운 접근을 계속 모색하고 있으며, 기존의 CAS 기술을 비롯하여 4C Entity의 CPPM/CPRM, 5C의 DTCP, Intel의 HDCP 등 다양한 복제방지기술 등과의 연동, 그리고 새로운 요구사항의 충족을 위한 신규기술의 개발들이 절실히 필요한 실정이다.

DRM 솔루션은 전적으로 소비자를 배제하고, 권리 소유자만을 위한 기술이라고 말할 수 없다. 불법적 콘텐츠 복제는 업계 수익 저하에 따른 소비자가 콘텐츠 획득을 위해 지불해야 될 비용을 증가시키는 결과를 가져다주며, 궁극적으로 보았을 때 DRM은 저작권 소유자, 업계, 소비자 모두를 위한 솔루션이라고 할 수 있다.

참고문헌

[1] EBU, Functional Model of a Conditional Access system, EBU Project Group B/CA, October, 1995.

[2] ATSC, Draft Conditional Access System for Terrestrial Broadcast, A/70A, May, 2004.

[3] ETSI, DVB Head-end Implementation of DVB Simulcrypt, ETSI TS 103 197 V1.4.1, December, 2004.

[4] ETSI, Support for Use of Scrambling and Conditional Access(CA) within Digital Broadcasting Systems, ETR 289, February, 1997.

[5] CableLabs, CableCARD Interface Specification, OC-SP-CC-IF-C01-050331, March, 2005.

[6] CableLabs, CableCARD Copy Protection system. Interface Specificationtion, OC-SP-CCCP-IF-C01-050331, March, 2005.

[7] FCC, Report and Order and Further Notice of Proposed Rulemaking, FCC 03-273, December, 2003.

[8] FCC, FCC Order, FCC 04-193, August, 2004.

용어해설

닷모비
.mobi [단말기기]

각종 휴대용 무선단말기를 통해 바로 인터넷에 접속할 수 있도록 모바일 인터넷 환경에 특화된 인터넷 최상위 도메인.
.mobi 도메인은 .com, .net, kr과 같은 최상위 도메인(gTLD: generic Top Level Domain)으로 2005년 국제인터넷주소관리기구(ICANN: The Internet Corporation for Assigned Names and Numbers)로부터 최종 승인 받았으며 운영은 삼성전자, 마이크로소프트, 구글, 소니, 에릭슨 등 전세계 대표적인 모바일 업체들이 출자해서 아일랜드에 설립한 MTLD(Mobile Top Level Domain)사가 맡고 있다.