情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

(Mobile) IPTV 보안 기술 및 표준화 동향

최 현 우*, 정 영 곤*, 염 흥 열**

요 약

본격적인 IPTV 서비스의 상용화에 따라 다양한 서비스 시나리오에서 안전하게 양방향의 디지털 콘텐츠를 제공하기 위한 IPTV 보안 기술의 필요성이 중요시 되고 있다. 본 고에서는 유·무선망의 (모바일)IPTV 보안 기술과 현재까지 진행되고 있는 국내외 표준화 동향에 대해서 살펴본다.

Ⅰ. 서 론

IPTV(Internet Protocol TeleVision)는 초고속 인터넷망을 통하여 이용자의 요청에 따라 양방향으로 다양한 멀티미디어 콘텐츠를 제공하는 통신방송융합서비스이다. 인터넷이라는 개방된 망을 통해 서비스가 제공되는 IPTV의 특징은 콘텐츠 및 서비스 제공자와 이용자를 수많은 보안 위협으로부터 노출시키게 한다. 특히, 언제 어디서나 어떤 단말로도 원하는 콘텐츠는 무엇이든 사용할 수 있어야 하는 IPTV 2.0 에서는 이와 같은 보안 위협이 더욱 심각해 질 것으로 예상된다.

일찍이 국외 표준화 단체에서는 de facto 표준으로써 유·무선망에서의 IPTV 보안 기술에 대한 연구를 활발히 진행해 오고 있다. 유럽의 DVB(Digital Video Broadcasting), 북미의 ATIS(Alliance for Telecommunications Industry Solutions), 모바일 중심의 OMA(Open Mobile Alliance) 그리고 산업체들을 중심으로 구성된 OIPF(Open IPtv Forum) 등이 대표적인 표준화 단체들이다.

본 고에서는 CAS(Conditional Access System), DRM(Digital Right Management)을 중심으로 하는 IPTV 보안 기술과 ITU-T(International Telecommunication Union Telecommunication Standardization Sector)를 비롯하여 현재 국내외 표준화 단체에서 진행되고 있는 유·무선 IPTV관련 보안 기술들의 표준화 동향에 대해 살펴본다.

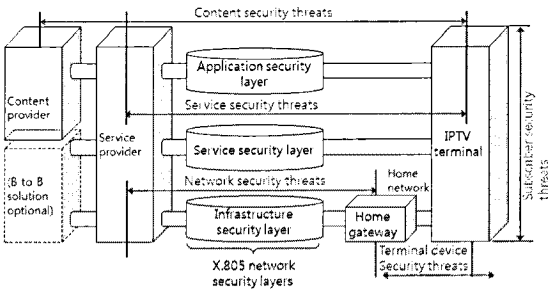
Ⅱ. IPTV 보안 기술

IPTV는 기본적으로 IP망을 통해 서비스가 이루어지기 때문에 IP망의 특징인 양방향 통신은 방송과 연계되는 부가 서비스의 개발 및 다양한 형태의 시스템적용을 용이하게 했다. 하지만 개방형이라는 IP망의 특징은 방송 채널의 불법적인 시청과 디지털 콘텐츠의 불법복제 등과 같이 다양한 보안 문제들을 발생시킨다.

2009년 2월에 제정된 ITU-T X.1191 권고안에서는 IPTV 보안 위협 모델을 [그림 1]과 같이 정의한 바 있다[1]. IPTV 서비스의 보안 위협들은 콘텐츠, 서비스, 네트워크, 단말 장치 수준에서 발생할 수 있으며, 구체적으로는 콘텐츠에 대한 불법적인 복사와 비인가 된 접근, 서비스제공자 및 단말의 스푸핑, 전송중인 콘텐츠의 도청 등을 그 예로들 수 있다.

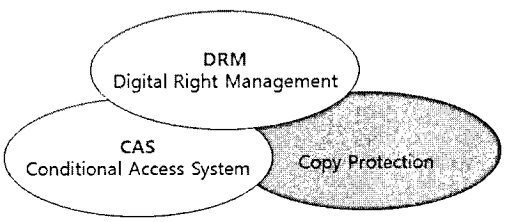
이와 같은 보안 위협들에 대비하고 안전한 IPTV 서비스를 보장하기 위해서, IPTV 보안 기술은 [그림 2]에서와

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음.
(NIPA-2010-(C1090-1031-0005))
* 순천향대학교 정보보호학과 석사과정 ({zemisolsol, txbluesky}@sch.ac.kr)
** 순천향대학교 정보보호학과 교수 (hyyoum@sch.ac.kr)



〔그림 1〕 IPTV 서비스 보안 위협 모델[1]

같이 기존 방송시스템의 보호 기술인 CAS(Conditional Access System)와 디지털 콘텐츠 보호 기술인 DRM(Digital Right Management), 그리고 저장매체 보호 기술인 CP(Copy Protection)등에 기반을 두고 있다.

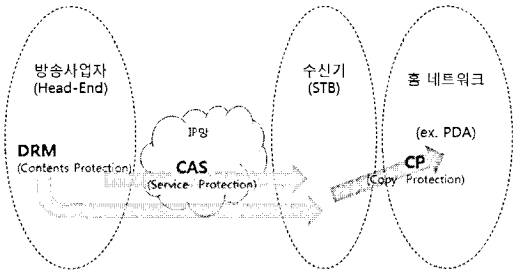


〔그림 2〕 방송 및 디지털 콘텐츠 보호 기술

〔그림 3〕은 〔그림 2〕에서 소개한 DRM, CAS, CP의 관계를 나타낸 그림이다. IPTV 서비스에서 디지털 콘텐츠 자체를 보호하기 위해서는 DRM 기술이, 네트워크 단에서 서비스 보호를 위해서는 CAS 기술이, 그리고 수신기의 출력 단에서 콘텐츠 분배의 보호를 위해서는 CP 기술이 적용된다.

현재 IPTV 보안 기술은 기존의 디지털 콘텐츠 보호기 기술들을 확장하여 서로 상호 연동 및 운용하는 형태로 발전하고 있으며, 특히, 디지털 케이블 방송 및 위성 방송에 적용 되어온 CAS 시스템을 이용하여 IPTV 서비스를 보호하려는 시도들이 많이 일어나고 있다. 또한, 최근에는 IPTV 서비스 및 콘텐츠 보호를 위해 CAS와 DRM 기술의 융합이 이루어지고 있는 추세이다.

본 절에서는 CAS, DRM, 그리고 CP 기술에 대해서 자세히 살펴본다.



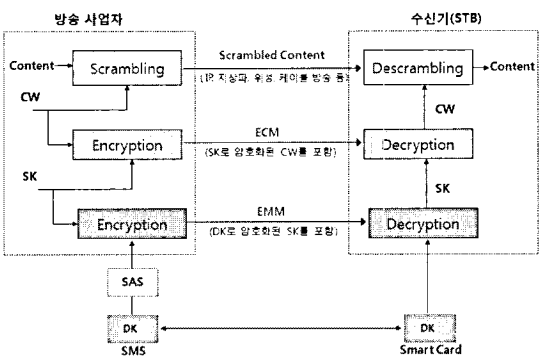
〔그림 3〕 DRM, CAS, CP 관계

2.1 CAS (Conditional Access System)

제한수신시스템(CAS)은 과거 아날로그 방송 시절부터 유료 방송 서비스를 위해 방송 서비스에 대한 고객의 접근 여부를 제어하는 기본 시스템으로 사용되어 왔다. 주로 방송사업자가 신호를 스크램블(scramble) 하여 멀티캐스트 방식으로 송출하면 가입자의 수신기(Set-Top Box, STB)에서 디스크램블(descramble)하는 방식으로 사용된다[2]. 따라서 서비스에 가입한 사용자의 수신기만이 암호화된 콘텐츠를 복호화하여 해당 방송 콘텐츠를 시청할 수 있게 된다.

CAS는 가입자의 시청료 납부에서부터 가입자관리 시스템(Subscriber Management System, SMS)과의 연동을 통해 가입자가 원하는 방송 프로그램의 제공 및 PPV(Pay Per View), VOD(Video On Demand) 등의 부가서비스를 제공할 수 있다. 따라서 방송사업자는 과거 광고를 통한 수익모델에서 벗어나 유료방송 사업을 통해 다방면으로 수익을 창출할 수 있게 된다.

〔그림 4〕은 CAS에서 디지털 콘텐츠를 scramble



〔그림 4〕 CAS 구조

/descramble 하는 과정을 나타낸다. CAS는 자격관리메시지(Entitlement Management Message, EMM)와 자격제어메시지(Entitlement Control Message, ECM)를 사용하여 시청권한이 있는 사용자만이 가입한 채널을 시청할 수 있게 한다. ECM과 EMM은 아래에 기술한 역할을 수행하며, 방송사업자의 네트워크에서 사용자의 STB로 주기적으로 전송된다.

- ECM: 서비스키(Service Key, SK)로 암호화된 제어단어(Control Word, CW)가 포함되어 있다. ECM은 가입자의 채널변환에 대응하기 위해 주기적으로 전송되며, 이때마다 CW가 새롭게 생성되고 암호화된다.
- EMM: 사용자의 STB에 자격을 부여, 갱신, 관리하는 기능을 한다. 분배키(Distribution Key, DK)로 암호화된 SK가 포함되어 있다. 방송사업자와 STB간에는 반드시 같은 DK를 공유하고 있어야 한다.

방송사업자는 디지털 콘텐츠를 scramble 하여 IP망 또는 지상파, 위성, 케이블망 등을 통해서 가입자의 STB로 송출한다. 이때 방송사업자의 네트워크에서 콘텐츠의 scramble을 위해 사용되는 키를 CW라고 하며, CW는 가입자의 STB에서 scramble된 콘텐츠를 descramble 하기 위해서도 사용된다. CW는 SK에 의해서 암호화된 후 ECM에 포함되어 MPEG-2 TS(Transport Stream)와 함께 STB로 전송된다. 또한 SK는 방송사업자와 STB가 사전에 공유하고 있는 DK를 통해 암호화된 후 EMM에 포함되어 STB로 보내지게 된다. 여기서 말하는 DK는 스마트카드 안에 내장되어 고객 정보를 관리하는 SMS에 의해서 사전에 가입자에게 배포되어 있는 비밀키를 의미한다.

한편 STB에서는 수신한 신호의 descramble을 위해 방송사업자가 scramble한 과정을 역으로 수행한다. 먼저, STB의 접근제어 모듈은 스마트카드 내에 저장된 DK를 사용하여 EMM으로부터 SK를 추출해 낸다. 그 뒤, 추출한 SK는 ECM에 포함되어 있는 CW를 복호화하기 위해 사용된다. 이렇게 복호화 된 CW는 scramble된 콘텐츠를 실시간으로 descramble 하는데 사용된다.

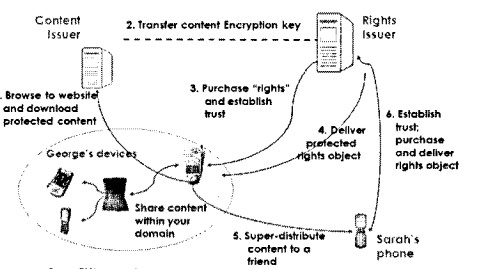
현재 CAS는 가입자 단말기 내에 내장된 형태로 존재하거나 혹은 케이블카드의 형식으로 STB에 탈착 가능한 방식으로 존재하는 것이 일반적이다. 하지만 최근에는 소프트웨어 방식의 CAS를 방송사업자로부터 STB에 다운로드 가능한 DCAS(Downloadable CAS)에 대한 표준화 작업이 진행 중에 있다.

2.2 DRM (Digital Right Management)

DRM은 디지털 콘텐츠에 대한 지적 재산권을 관리하고 제어하기 위해 인터넷망에서 주로 사용되는 기술이다. 불법 복제를 방지하기 위하여 디지털 콘텐츠를 암호화하고, 인증된 사용자와 단말기에 한해서만 라이센스(License)를 발급함으로써 라이센스에 포함된 콘텐츠에 대한 사용 권한에 따라 콘텐츠를 보호한다.

[그림 5]는 대표적인 DRM 기술인 OMA DRM 기술의 사용 예를 보여준다. [그림 5]에서 George는 콘텐츠발급자(Content Issuer)로부터 보호된 콘텐츠를 다운로드 받는다. 동시에 콘텐츠발급자는 George가 다운로드 한 콘텐츠에 대한 암호화키를 권리발급자로 전송 한다. 조지는 다운로드 받은 콘텐츠의 이용을 위해 권리발급자로부터 권리오브젝트(Right Object)를 발급받는다. 발급받은 권리오브젝트를 이용하여 George의 도메인 내에서 자유롭게 콘텐츠를 이용할 수 있지만, 만일 다른 도메인으로 콘텐츠를 분배할 필요가 있을 경우 다시 권리객체를 구매·발급 받아야만 콘텐츠를 이용할 수 있다.

DRM이 CAS와 구별되는 가장 큰 특징은 CAS는 방송 서비스의 채널을 보호하는 반면, DRM은 방송 콘텐츠 자체를 보호 한다는 것이다. DRM 기술의 표준화는 MPEG-21, OMA, DMP(Digital Media Project), ISMA(Internet Streaming Media Alliance), DHWG(Digital Home Working Group), DVB-CPCM(Content Protection



[그림 5] OMA DRM 사용 예

and Copy Management), Coral, Marlin, EXIM (Export/Import) 등이 대표적이다.

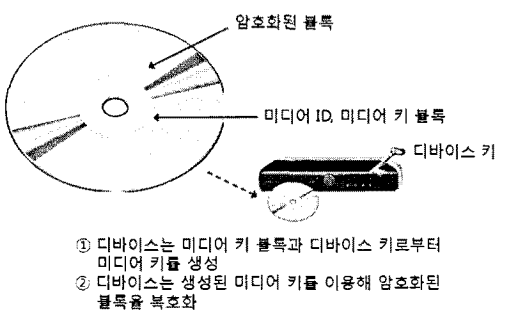
2.3 CP (Copy Protection)

복제방지(CP) 기술은 HDD, DVD-RW 등의 디지털 저장매체, 또는 IEEE-1394와 같은 인터페이스 신호 및 DVI와 같은 디스플레이 신호를 통한 디지털 콘텐츠의 복제를 제어하는 기술이다[3]. CP는 STB에 저장된 콘텐츠를 외부 인터페이스를 통해 무단으로 복제하는 것을 방지한다. 따라서 복제방지 기술을 사용하면 장비간 인증을 통해 미리 정의된 방식으로만 콘텐츠를 복사하거나 이동시킬 수 있게 된다.

[그림 6]은 복제방지 기술의 예로써, IBM, Intel, Matsushita, Toshiba에 의해 1998년 CPTWG (Copy Protection Technical Working Group)에서 제안된 CPRM (Content Protection for Recordable Media) 기술을 보여준다. CPRM은 DVD와 같은 이동식의 저장 미디어를 이용해서 배포되는 콘텐츠의 복제방지를 위한 기술이다.

[그림 6]에서, CPRM을 지원하는 미디어에는 미디어 고유의 ID와 미디어 키 블록을 가지고 있으며, 디바이스는 미디어 ID와 미디어 키 블록을 이용해 해당하는 미디어의 미디어 키를 생성한다(①). 그 후 생성된 미디어 키를 이용해 암호화된 블록을 복호화하게 된다(②).

이 외에도 복제방지 기술로는 디지털 입출력 보호를 위한 DTCP(Digital Transmission Content Protection)와 HDCP(High-bandwidth Digital Content Protection), 미니디스크/메모리스틱에 안전하게 콘텐츠를 복사하기 위한 기술인 MagicGate, 그리고 이동 가능한 저장 미디어에 대한 보호 기술인 ViDi 등이 있다.



[그림 6] CPRM 구조

Ⅲ. IPTV 보안 기술 표준화 동향

IPTV 보안 기술 표준화는 국내외 표준화 단체 및 산업체 별로 활발히 진행 중에 있다. 그 중 본 고에서는 국내의 정보통신기술협회(TTA)에서 제정되거나 논의 중인 관련 표준화 동향과, 국제 표준화 기구인 ITU-T를 비롯하여 ATIS, DVB, OMA, OIPF 등에서 진행되고 있는 관련 기술의 표준화 동향에 대해서 살펴본다.

3.1 국내 표준화 동향

2006년, TTA 표준화 위원회에서는 IPTV 프로젝트 그룹(PG219)을 신설하여 ITU-T FG(Focus Group)에서 시작된 IPTV 국제 표준화 활동에 대비하고자 했다. 현재는 [표 1]에서와 같이 TTA 표준화 위원회 산하 해당 프로젝트그룹 및 실무반에서 IPTV 보안 관련 표준화 작업을 진행 중에 있다.

[표 2]는 TTA의 표준화위원회에서 단체표준으로 제정됐거나 현재 진행 중인 표준화과제의 현황을 보여준다. 본 절에서는 [표 2]의 각 표준화 과제들에 대해서 간략히 살펴본다.

3.1.1 IPTV 용 교환 가능한 CAS (iCAS)[5]

IPTV 환경에서 효율적이고 안전한 콘텐츠 서비스를 가능하도록 지원하기 위해 필요한 보안 기술을 서

[표 1] IPTV 보안 관련 TTA 표준화위원회

기술위원회 (TC)	프로젝트그룹 (PG)	실무반 (WG)
전송통신 기술위원회 (TC2)	IPTV 프로젝트 그룹(PG219)	Mobile IPTV 실무반(WG2193)
		IPTV Security 실무반(WG2194)
정보보호 기술위원회 (TC5)	응용보안 및 평가인증 프로젝트 그룹(PG504)	-
	DRM 프로젝트 그룹(PG506)	DRM 연동 기술(WG5062)

〔표 2〕 TTA 표준화위원회 IPTV 표준화과제 현황

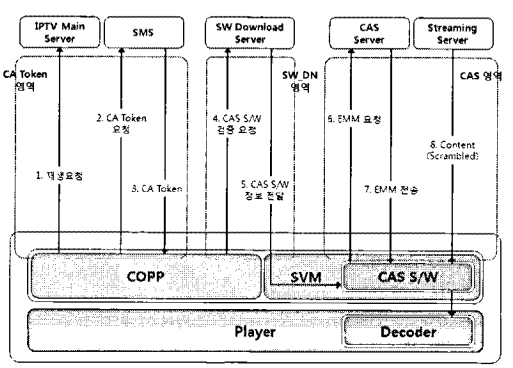
No.	과제번호	초안명	처리단계	위원회	기타
1	2007-086	IPTV Security 기술	초안통합	PG219	-
2	2008-685	IPTV HW 보안 기술	초안작성중	PG219	-
3	2008-686	IPTV 용 교환 가능한 CAS (iCAS)	표준공고	PG219	2009-03-26 제정 (TTAK.KO-08.0023)
4	2008-689	Non-NGN 기반 Mobile IPTV 요구사항	표준공고	PG219	2009-06-18 제정 (TTAK,KO-08.0021)
5	2009-841	IPTV 보안 요구사항 및 구조	표준공고	PG504	2009-12-22 제정 (TTAE.IT-X1191)
6	2009-847	스케일러블 비디오 코딩 암/복호화 지침	표준공고	PG504	2009-12-22 제정 (TTAK
7	2009-854	IPTV 서비스를 위한 CAS-DRM 연동 인터페이스 확장	초안작성중	PG506	-
8	2009-1328	IPTV 서비스 보호를 위한 SEED/ARIA 스크램블링 알고리즘	표준공고	PG504	2009-12-22 제정 (TTAK.KO-12.0123)

버로부터 다운로드 받아 사용하는 다운로드 형태의 CAS 시스템을 표준화 하려는 움직임들이 활발히 진행되고 있다[4].

최근 WG2194에서 제정된 iCAS 표준에서는, IPTV에서 CAS 모듈을 네트워크를 통하여 안전하게 다운로드 받고 관리하기 위한 필요 요구사항들을 정의하고, 이를 만족시키기 위한 세부 기술들을 정의하고 있다.

세부 기술로는, CAS 모듈을 안전하게 다운로드 받기 위한 서버와 IPTV 수신 단말과의 프로토콜들을 정의하며, 다운로드 받은 서비스 및 콘텐츠 보호 기술을 안전하게 관리하고 실행시키기 위하여 IPTV 수신 단말에서 필요한 컴포넌트들을 정의하고 있다.

〔그림 7〕은 본 규격에서 정의한 다운로드 가능한 CAS 시스템의 구조이다. 규격에서는 콘텐츠 획득을



〔그림 7〕 iCAS 시스템 구조[5]

CA Token 영역, SW_DN 영역, CAS 영역으로 정의했으며, 구체적인 각 단계는 다음과 같다.

① 서버와 단말의 인증을 통해 CAS SW의 다운로드 권한을 획득하는 단계 (CA Token 영역)
② 인가된 단말에 한해 안전하게 보호된 형태로 CAS SW를 내려주는 단계 (SW_DN 영역)
③ 내려 받은 CAS SW를 안전하게 저장하고 실행하는 단계 (CAS 영역)

특히, ③의 단계는 VM(Vitual Machine) 개념을 이용하여 CAS SW가 하드웨어에 독립적이게 동작가능 하도록 설계하고 있으며, 다운로드 된 CAS SW는 로딩 되어 사용될 때를 제외하고는 암호화된 형태로 단말에 저장되어 있게 정의하고 있다.

iCAS 표준은 2010년 2월에 1차 규격의 작성이 완료 되었으며, 콘텐츠 사업자, 서비스사업자, 단말 제조업체 그리고 보안 솔루션 업체들과의 충분한 의견수렴 과정을 거친 후, 최근 정보통신단체표준으로 제정되었다.

3.1.2 Non-NGN 기반 Mobile IPTV 요구사항[6]

Mobile IPTV 실무반(WG2193)은 유선망에서의 IPTV 서비스가 향후 무선망으로 이동할 것으로 인식하여, ITU-T에서 모바일 IPTV가 논의되기 이전에 국제표준을 선행 준비하고자 관련 기술 규격을 표준화하기 시

〔표 3〕 Mobile IPTV 요구사항 - 보안 요구사항

범주	요구사항
공통	·적용되는 보안 기술들은 서비스 종단 간 성능 및 그 기능에 있어 Mobile IPTV 환경에서 효율적이어야 한다. ·서비스 사업자로부터 Mobile IPTV 단말로 전송되는 과정이나 Mobile 저장장치에 저장하는 과정에서 Contents가 불법적으로 유출되는 것을 막을 수 있어야 한다.
서비스 보안	·Mobile IPTV 환경에서 서비스에 대한 접근제어(Access Control)는 이동성을 지원해야 한다. ·서비스 보안을 위한 접근 제어 모듈은 Device Mobility를 고려한 안전한 변경 및 관리가 가능해야 한다. ·Mobile 환경에서 서비스에 대한 보안레벨의 변경이 가능할 수 있다. ·트랜스코딩이 발생하는 중간경로에서 서비스의 불법적인 사용, 전달 및 삽입을 방지할 수 있어야 한다. ·서비스 중간경로에 설치된 악의적인 액세스 장치가 사용자의 서비스 자격 관련 데이터의 가로채기, 변조, 삭제 및 부정생성 등을 방지할 수 있어야 한다.
Contents 보안	·Mobile IPTV 환경에서 Contents 복사방지 및 재분배 관리 기능은 이동성을 지원해야 한다. ·Mobile IPTV는 Contents 특성에 따라 차별화된 usage rule 및 보안 기능 적용을 지원해야 한다. ·서비스 제공자는 무선 환경에서 단말에 대해 불법 Contents 추적이 가능해야 한다. ·트랜스코딩이 발생하는 중간경로에서 콘텐츠의 불법적인 사용, 전달 및 삽입을 방지할 수 있어야 한다. ·서비스 중간경로에 설치된 악의적인 액세스 장치가 사용자의 콘텐츠 및 메타데이터의 가로채기, 변조, 삭제 및 부정생성 등을 방지할 수 있어야 한다.
단말 보안	·Mobile IPTV 단말은 사용자/단말 이동성을 보장하기 위하여 안전한 소프트웨어 다운로드 및 관리를 지원해야 한다.
가입자 보안	·서비스 제공자는 Mobility 환경, 즉 이동성을 가지는 사용자에 대한 인증이 가능해야 한다.

작했다. 그 결과, 2008년 2월에 TTA Technical Report (TTAR-08.001)로 표준문서가 발행되었으며, 그 후 수정보완을 거쳐 2009년 6월에 최종 TTA 국내 표준(TTAK.KO-08.0021)으로 제정되었다[7].

본 표준에서는 요구사항의 범주를 서비스 요구사항, 단말 요구사항, 네트워크 요구사항, 품질 요구사항, 보안 요구사항으로 분류했으며, 그 중 〔표 3〕은 보안 요구사항을 나타낸 표이다. 〔표 3〕에서 규정하고 있는 보안 관련 요구사항들은 ITU-T에서 규정하고 있는 요구사항들을 모두 수용하면서 사용자 및 단말 이동환경에 필요한 보안 요구사항들을 추가로 기술 하고 있다.

향후, 본 표준은 국내 IPTV 현황과 무선 네트워크 상황 등을 고려해 NGN 기반 Mobile IPTV 요구사항으로 확장할 계획이다.

3.1.3 IPTV 보안 요구사항 및 구조[8]

ITU-T X.1191[1] 표준의 국내 영문표준으로써, 2009년 12월 22일에 제정됐다. X.1191 표준의 내용을 준용하고 있으며, 주요 내용으로는 콘텐츠, 서비스, 네트워크, 단말 그리고 가입자 보호를 위한 IPTV 보안 요구사항의 도출과 안전한 IPTV 서비스 제공을 위한 보안 구조의 정의와 보안 메커니즘을 제시하고 있다.

3.1.4 스케일러블 비디오 코딩 암/복호화 지침[9]

IPTV 등 SVC(Scalable Video Coding) 기반 VoD 또는 실시간 스트리밍 서비스를 제공할 때, 영상에 대한 접근제어를 위한 암/복호화 가이드라인을 제시하기 위한 표준이다[9]. 본 표준에서는 SVC의 암/복호화 가이드라인으로 기본적인 암/복호화를 위한 고려사항과 인코딩 과정에서의 암호화 적용 방식, 인코딩 이후의 암호화 적용 방식, 그리고 계층별 차등 암호화 적용 방식에 대한 각각의 지침을 제시하고 있다.

3.1.5 IPTV 서비스를 위한 CAS-DRM 연동 인터페이스 확장

2008년 12월에 제정된 CAS와 DRM 간의 상호연동을 위한 인터페이스(TTAK.KO-12.0099) 표준을 IPTV 서비스를 위해 확장하기 위한 표준이다. 참고로 TTAK.KO-12.0099[10]에서는, CAS 기술과 DRM 기술의 연동을 통해 방송 콘텐츠가 CAS 보호 체계로부터 DRM 보호 체계로 전달되는 것을 기본 시나리오로 삼고, 상호 연동 과정을 위해 필요한 정보를 정의하며 CAS 보호 체계와 DRM 보호 체계 양자 간의 연동 절차를 기술한 프로토콜을 명시하고 있다.

〔표 4〕 ATIS IIF 보안 관련 규격 현황

표준번호	표준명	완료일
ATIS-0800001	IPTV DRM Interoperability Requirements	2006년 4월
ATIS-0800006	IIF Default Scrambling Algorithm (IDSA)	2007년 1월
ATIS-0800014	Secure Download Interoperability Specification for IPTV	2008년 3월
ATIS-0800015	Certificate Trust Management Hierarchy Interoperability Specification	2008년 8월
ATIS-0800016	Standard PKI Certificate Format Interoperability Specification	2008년 8월

3.1.6 IPTV 서비스 보호를 위한 SEED/ARIA 스크램블링 알고리즘[11]

IPTV 서비스 보호를 위해 사용되는 스크램블링 알고리즘으로 국내 암호 알고리즘인 SEED와 ARIA를 활용하기 위한 규격이다. 주요 내용으로는 IPTV 전송 스트림 패킷을 스크램블링 하기 위해 사용하는 스크램블링 알고리즘으로써 CBC(Cipher Block Chaining) 모드로 동작하는 SEED 및 ARIA를 정의하고 있다.

3.2 국외 표준화 동향

국외는 산업체 및 지역 표준화 기구 별로 IPTV 보안 기술에 대한 표준화 작업을 진행해 오고 있다. 대표적인 표준화 단체로는 유럽의 DVB와 북미의 ATIS, 산업체 중심 포럼인 OIPF와 모바일 중심의 OMA 등이 있다.

3.2.1 ATIS IIF

북미통신표준기구(ATIS)는 2005년 6월 IIF (IPTV Interoperability Forum)를 조직하여 IPTV를 위한 산업의 end-to-end 솔루션을 개발 중에 있다. ATIS IIF에는 통신업체를 비롯하여, 장비업체, 소프트웨어 업체 등 다수의 기업이 참여하여 IPTV 관련 표준 규격 작업을 활발히 진행 하고 있다. 현재까지 IIF에서 완료된 IPTV 보안 관련 규격은 〔표 4〕와 같다. 본 절에서는 〔표 4〕의 각 규격에 대해 간략히 살펴본다.

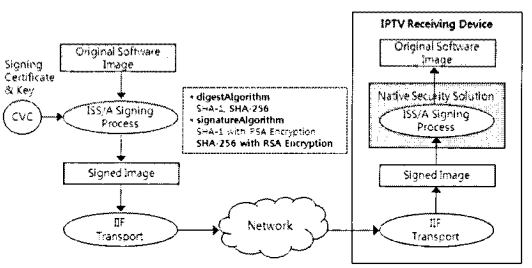
· ATIS-0800006[12]

IDSA(IIF Default Scrambling Algorithm) 규격은 전통적인 제한수신시스템과 DRM 기술을 이용해 IPTV 콘텐츠 보안을 위한 높은 수준의 DRM 구조를 정의하고 있다. IDSA는 방송콘텐츠와 같은 실시간 콘텐츠는 CAS를 이용해 실시간으로 암호화하여 전송하고, VoD와 같은 콘텐츠는 DRM 기술을 이용해 전송하게 한다. 그리고 MPEG2-TS 패킷의 전송시에 사용되는 기본 스크램블링 알고리즘과 시그널링을 정의해 놓고 있다.

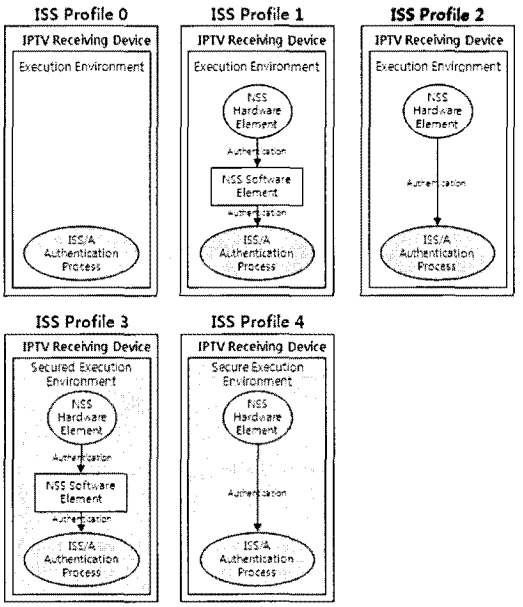
· ATIS-08000014[13]

소프트웨어 이미지와 메시지를 안전하게 다운로드 하기 위한 규격을 정의하고 있다. 인증과 무결성을 제공하기 위해 헤드엔드 및 디바이스에 포함되는 구성요소인 ISS/A(IPTV Security Solution/ Authentication)을 정의하고 있으며, 〔그림 8〕은 ISS/A가 소프트웨어 이미지를 서명하여 디바이스로 다운로드 하는 과정을 보여준다.

〔그림 8〕에서, 헤드엔드는 원본 소프트웨어 이미지를 인증기관을 통해 발급받은 인증서를 이용해 서명하



〔그림 8〕 ISS/A 서명 과정[13]



〔그림 9〕 ISS 보안 프로파일[13]

고, 무결성 제공을 위해 해쉬값을 첨부하여 수신 디바이스로 전송한다. 수신 디바이스는 신뢰기관을 통해 수신한 소프트웨어 이미지에 대해 인증서를 검증하여 헤드엔드를 인증하고, 무결성을 위해 계산된 해쉬값과 첨부된 해쉬값을 비교한다. 다이제스트 알고리즘으로 SHA-256을 권장하고 있으며, 서명 알고리즘은 SHA-256 with RSA를 권장하고 있다.

또한 ATIS-08000014에서는 〔그림 9〕와 같이 ISS 보안 프로파일을 정의한다. ISS 보안 프로파일은 ISS Profile 0 ~ ISS Profile 4까지 5개로 이루어져 있으며, IPTV 수신 디바이스를 구현하기 위한 보안 특성들을 각각 정의하고 있다.

· ATIS-0800015[14]

ATIS-0800014 규격과 관련되며, 계층적인 인증서 관리 구조를 위해 CVC CA(Code Verification Certificate CA), MVC CA(Message Verification Certificate CA), DEV CA(Device CA), SSE CA(Separable Security element CA), extCA(향후 정의될) 등을 정의하고 있다.

· ATIS-0800016[15]

인증서를 위한 포맷 형식을 정의한다. IIS/R(Root 인증서), IIS/CA(인증기관 인증서), IIS/C(디바이스 인증서) 인증서 형태를 정의하며, 각 인증서에 대해 공통의 필드와 확장 필드를 상세히 기술하고 있다.

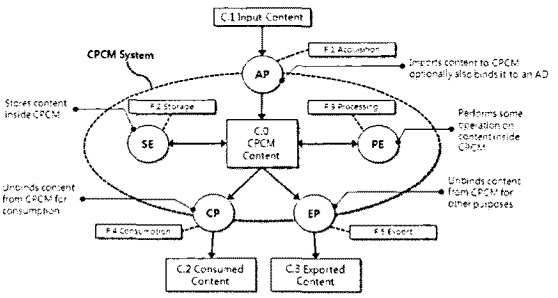
3.2.2 DVB CPCM

DVB CPCM(Copy Protection & Content Management)은 콘텐츠 보호 및 복제관리 기술 표준으로써, DVB 표준을 따르는 콘텐츠가 DVB CAS로 보호되는 범위를 넘어서 홈 네트워크 혹은 녹화기 등과 같은 개인 영역 네트워크(Personal Area Network, PAN)에 저장될 때에 콘텐츠의 보호와 관리를 위한 프레임워크를 제공한다. DVB CPCM은 콘텐츠의 사용을 최초 취득 단계에서부터 최종 소비 또는 CPCM 적용범위 밖으로의 출력 단계까지 공급자가 정한 그 콘텐츠 고유의 사용 규칙에 따라 관리되도록 규정하고 있다.

DVB CPCM에서 대상 매체의 보호 범위는 방송(케이블, 위성 등), 인터넷, 패키지화된 미디어(DVD 등), 모바일 서비스 등을 포함하며, 콘텐츠 보호 범위는 인가된 도메인 내의 네트워크 혹은 디바이스들을 포함한다. 또한 원격지에 있는 홈 네트워크 기반 사용 환경에서의 상호 운용성을 지원한다.

〔표 5〕 DVB-CPCM 규격

파트	규격명
1	CPCM Abbreviations, Definitions and Terms
2	CPCM Reference Model
3	CPCM Usage State Information
4	CPCM System Specification
5	CPCM Security Toolbox
6	CPCM Security Test Vectors
7	CPCM Authorised Domain Management
8	CPCM Authorised Domain Management scenarios
9	CPCM System Adaptation Layers
10	CPCM Acquisition, Consumption and Export Mappings
11	CPCM Content Management Scenarios
12	CPCM Implementation Guidelines
13	CPCM Compliance Framework
14	CPCM Extensions



〔그림 10〕 CPCM 콘텐츠 및 개체들의 기능적 모델[16]

〔그림 10〕은 CPCM 환경에서 방송콘텐츠의 흐름 및 CPCM 콘텐츠와 CPCM 시스템 개체들의 기능적 모델을 나타낸다. AP(Acquisition Point)는 CPCM 시스템 혹은 AD(Authorized Domain)로 유입되는 콘텐츠를 획득하여 CPCM 콘텐츠로 변환하는 역할을 수행한다. 변환된 CPCM 콘텐츠는 SE(Storage Entity)와 PE(Processing Entity)를 통해 CPCM 디바이스 상에서 저장되거나 처리된다. 그리고 CP (Consumption Point)와 EP(Export Point)에서는 소비되거나 외부로 유통되는 CPCM 콘텐츠를 재 변환하는 역할을 수행한다.

현재까지 DVB CPCM 규격은 〔표 5〕와 같이 14개의 파트들로 구성되어 있으며, 향후 DVB 규격의 방송시스템을 채택한 국가 및 사업자는 IPTV 콘텐츠를 보호하기 위해 DVB CPCM 기술을 도입할 것으로 예상된다.

3.2.3 OIPF CSP

OIPF(Open IPtv Forum)는 개방형 기술 표준화를 통해 IPTV 기술의 보급을 가속화하고 시장을 활성화하자는 취지로 산업체들이 모여 2007년에 설립된 단체이다. OIPF는 기존 IPTV 관련 기술들을 수용하면서 각 업체의 장비 간 호환성 문제를 해소하는데 초점을 맞추고 있다. 현재의 IPTV 기술 표준화가 단말, 네트워크, 서비스 등 각 계층별로 진행되어 온 반면, OIPF는 Open IPTV Common UNI 인터페이스를 통해 end-to-end 관점에서의 일괄된 규격 및 Managed Network와 Open Network 양쪽 모두를 위한 표준의 개발을 목표로 하고 있다.

OIPF의 표준 규격은 현재 7개의 Volume을 포함하는 Release 1이 완성되었으며, 새로운 서비스와 특징들을 위해 추가적인 요구사항 등을 포함하는 Release 2 규격이 개발 중에 있다.

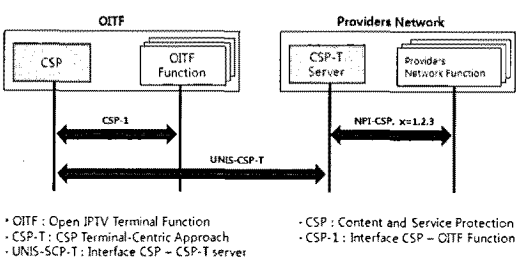
OIPF 규격 중 보안관련 규격은 Release1의 Volume7(Authentication, Content Protection and Service Protection)[17]에 정의되어 있다. Volume7은 2009년 1월에 v1.0이 제정되어, 2009년 10월에 v1.1로 개정된 상태이다.

OIPF는 CSP(Content and Service Protection)를 위해 터미널 중심 방법(Terminal -Centric)과 게이트웨이 중심(Gateway-Centric) 방법을 정의했다.

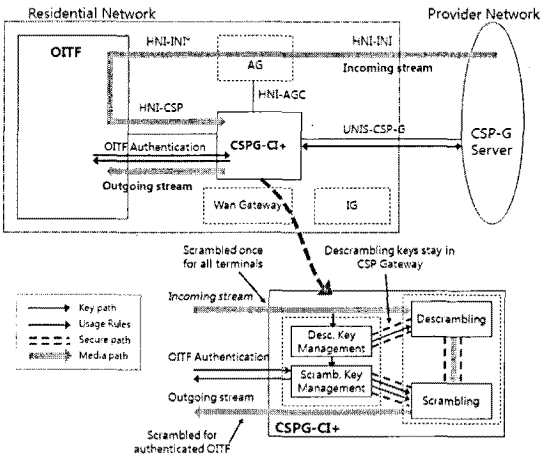
터미널 중심은 DRM 기술인 Marlin에 기반하고 있으며, 파일 보호를 위해 OMA 파일 포맷(PDCF, DCF)과 Marlin IPMP 파일 포맷을 사용한다. 또한 MPEG2-TS의 보호를 위해 AES 또는 DVB-CSA 암호화를 지원한다. 다음 〔그림 11〕은 터미널 중심 방법에서 SCP를 위한 메시지들의 흐름을 나타낸다.

〔그림 11〕에서, OITF(Open IPTV Terminal Function)의 CSP 기능 개체와 서비스제공자 네트워크의 CSP-T Server 기능 개체는 UNIS-CSP-T (Interface CSP - CSP-T server) 인터페이스를 통해 메시지들을 교환한다. 이들 메시지의 종류에는 Marlin의 등록, Marlin의 해제, Marlin의 라이센스 획득 등이 있다.

게이트웨이 중심은 CSPG(CSP Gateway)와 OITF 사이의 안전한 인증 채널에 기반 한다. CSP 게이트웨이 기능 개체는 Marlin 기반 SCP 솔루션에 대한 대안으로 가능한 프레임워크를 제공한다. 〔그림 12〕는 CI+(Common Interface Plus)에 기반을 두는 게이트웨이 중심 방법을 나타낸다. 홈 네트워크(Residential Network) 내의



〔그림 11〕 터미널 중심법 개요[17]



〔그림 12〕 게이트웨이 중심법 개요[17]

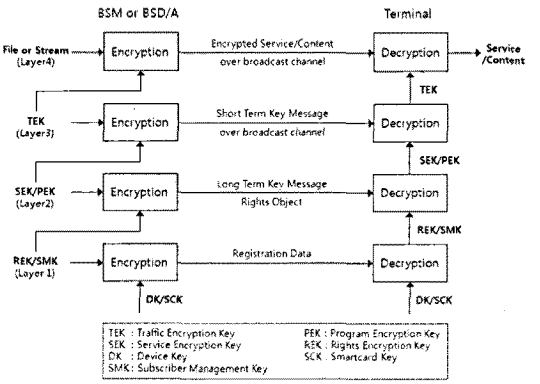
CSP 게이트웨이 기능 개체와 서비스 제공자 네트워크상의 CSP-G 서버 기능 개체는 UNIS-CSP-G 인터페이스를 통해 SCP에 관련된 메시지들을 교환한다. CSPG와 OITF 사이의 HNI-CSP 인터페이스는 SCP 기법으로부터의 변환을 위해서 OITF가 인증을 통해 CSPG로 접근하는 것을 허용한다. 그리고 HNI-AGC 인터페이스는 CSPG와 AG (Application Gateway)와의 연결을 제공한다.

OIPF는 종단 단말장치에서 콘텐츠 보호를 위해 Marlin 기술을 선택할 수 있을 뿐만 아니라(터미널 중심), 서비스 제공자에 의해 선택된 독점적인 보호기술들을 그 대안으로 수용할 수 있도록 하고 있다(게이트웨이 중심).

3.2.4 OMA BCAST

OMA BCAST(Mobile Broadcast Service)는 단말 응용 계층 표준화 단체인 OMA(Open Mobile Alliance)에서 휴대 방송 응용 계층의 단일 기술을 만들기 위해 시작된 표준으로써, 이동통신 영역에서의 Mobile IPTV 서비스에 관련하여 가장 대표적인 기술이다. OMA BCAST는 DVB-H와 같은 방송시스템에서부터, 3GPP MBMS, 3GPP2 BCMCS와 같은 휴대폰시스템, 그리고 모바일 유니캐스트 스트리밍 시스템에 적용될 수 있다.

서비스와 콘텐츠 보호를 위해, OMA BCAST는 USIM 등과 같이 대칭키를 기반으로 하는 Smartcard



〔그림 13〕 OMA BCAST SCP - 4계층 모델[18]

Profile과 OMA DRM 2.0에 의한 공개키 기반의 DRM Profile에 대해 각각 계층적인 키 관리 구조를 정의 하고 있다. 다음 〔그림 13〕은 SmartCard Profile에서 4계층 모델을 통한 서비스 및 콘텐츠 보호 구조를 나타낸다.

OMA BCAST 규격은 2009년 2월에 Release 1이 완성되었고, 보다 다양한 서비스를 수용하기 위해 Release 1.1 표준을 진행 중에 있다.

3.3 ITU-T 표준화 동향

2006년 ITU-T에서는 FG-IPTV를 통해 IPTV 보안의 표준초안이 마련됐으며, 현재는 SG17 Q.6에서 IPTV 보안 표준개발을 진행하고 있다. 특히, IPTV 보안 관련 권고안들은 한국인이 에디터를 맡고 있어, 한국의 주도로 표준개발 작업이 진행되고 있는

〔표 6〕 IPTV 보안 관련 권고안 개발 현황

권고번호	권고명
X.1191 (2009년 2월 승인)	Functional requirements and architecture for IPTV security aspects
X.iptvsec-2	Functional requirements and mechanisms for secure transcod able scheme of IPTV
X.iptvsec-3	Key management framework for secure IPTV communications
X.iptvsec-4	Algorithm selection scheme for SCP descrambling
X.iptvsec-5	SCP interoperability scheme

중이다.

〔표 6〕은 ITU-T의 IPTV 보안 권고안 개발 현황을 나타낸다. 참고로 ITU-T 에서는 CAS, DRM 등과 같은 보호 기술들을 총칭하여 SCP (Service and Content Protection)라 칭한다.

· X.1191 (IPTV SCP를 위한 요구사항 및 보안 구조)[1]

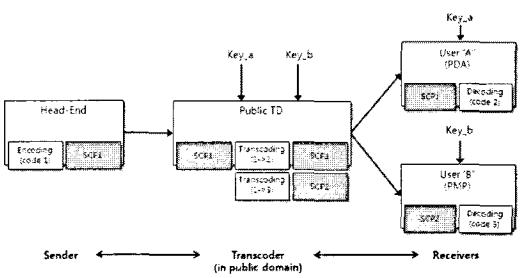
이 권고안은 IPTV 보안을 위한 기본 지침이 될 권고안으로써 IPTV SCP를 위한 요구사항 및 보안 구조를 정의한다. IPTV 보안에 대한 요구사항으로 그 대상을 콘텐츠 보안, 서비스 보안, 네트워크 보안, 터미널 보안 그리고 가입자 보안 등으로 분리하여 정의하였고, IPTV 보안에 대한 보안구조로는 일반적인 보안구조를 바탕으로 콘텐츠 보호 구조와 서비스 보호 구조로 정의하여 각각 구조에서 요구되는 보안기능 및 구성요소들의 기능을 정의하였다. 여기에서 말하는 콘텐츠 보호란 콘텐츠 소유자에 의해 허용된 권한으로 획득된 콘텐츠를 사용할 수 있게 보장하는 기술이며, 서비스 보호는 적법한 사용자에게 자격이 있는 서비스와 서비스 내에 포함되어 있는 콘텐츠를 획득하도록 하는 기술을 뜻한다.

X.1191 권고안은 2008년 9월 전통채택과정(Traditional Approval Protection)으로 승인되었으며, 2009년 2월 SG17 회의에서 최종 채택되었다.

· X.iptvsec-2 (IPTV 트랜스코더블 보안 기법)

본 권고초안은 2008년 4월에 신설되었으며, IPTV 서비스에서 다양한 단말들에게 안전한 IPTV 서비스 제공을 보장하기 위한 내용을 담고 있다.

〔그림 14〕는 현재 개발 중인 트랜스코더블 기법의 개념을 보여준다. 그림에서, 트랜스코더는 SCP1에 대한 별도의 과정 없이 code 1을 code 2로 트랜스코딩하여 PDA로 전송해 주고 있다.

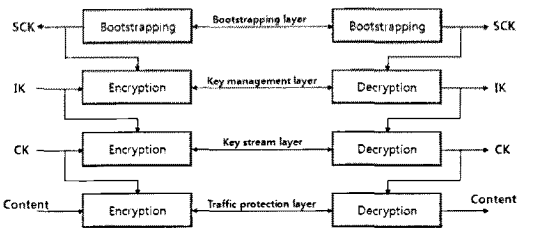


〔그림 14〕 IPTV 트랜스코더블 기법 (X.iptvsec-2)

이처럼 X.iptvsec-2에서는 다양한 단말의 다양한 해상도(resolution)를 지원하면서 네트워크 중간 노드에서 복잡한 복호화 및 재암호화 과정 없이 서비스 제공자와 유무선 단말 간에 종단간(end-to-end) 보안을 유지할 수 있는 트랜스코더블(Transcodable) 기법을 개발 중에 있다.

· X.iptvsec-3 (IPTV 서비스 키관리 프레임워크)

본 권고초안은 2008년 5월 IPTV-GSI 회의에서 신설되었으며, 안전한 IPTV 서비스를 제공하기 위해 필수적으로 요구되는 키 관리 요소 기술을 개발하고 있다.

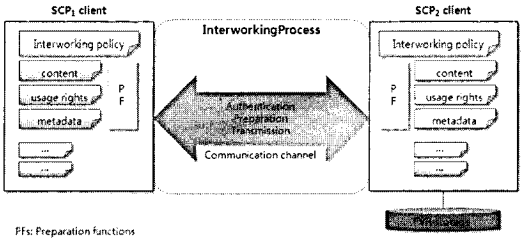


〔그림 15〕 계층적 키 관리 기법 (X.iptvsec-3)

〔그림 15〕는 유니캐스트, 멀티캐스트, 다운로더블 SCP 등의 다양한 IPTV 서비스를 위한 키 관리의 4계층 구조를 보여준다. 이외에도 본 권고초안에서는 프로토콜 및 메시지 포맷/관련 파라미터 등에 대해서도 기술하고 있다. 최근 X.iptvsec-3 권고초안은 5번째 수정안이 반영되는 등 활발한 개발 작업을 진행 중에 있다.

· X.iptvsec-4 (SCP 디스크램블링을 위한 알고리즘 선택)

2008년 1월 IPTV-GSI 회의에서 신설되었으며, 하나의 IPTV 단말에서 여러 IPTV 서비스제공자로부터 오는 암호화 콘텐츠를 동시에 수신할 수 있게 공통 복호화 부분을 정의하는 기술을 담고 있다. 즉, 서로 다른 SCP 기법을 사용하는 여러 IPTV 서비스제공자로부터 수신되는 채널 별 콘텐츠를 복호화 하기 위한 암호 알고리즘을 단말이 선택 가능하게 할 수 있게 하는 것을 말한다.



〔그림 16〕 SCP 상호운용 기술 (X.iptvsec-5)

· X.iptvsec-5 (SCP 상호운용 기법)

이 드래프트 권고안은 CAS-DRM 등과 같이 여러 다른 콘텐츠 보호 시스템을 서로 연결시키기 위해, 다양한 SCP 간에 상호 연동을 위한 기법과 상호연동 프레임워크를 개발하는데 목적을 둔다.

〔그림 16〕에서, SCP1과 SCP2의 상호운용은 표준의 형태로 변환된 content, usage rights, metadata 등을 이용해 이루어 질 수 있다.

Ⅳ. 결론

IPTV 보안 기술은 접근제어 기술에서부터 인증 및 키 관리 기술, 권리 제어 기술, 암호화 기술, 기술 간의 상호운용 및 연동 기술 등 다양한 기술들이 접목되어 이루어진다.

이와 같은 기술들에 대한 표준화 작업은 국가별, 지역별, 그리고 관련 산업체 중심의 포럼 등을 통해 활발하게 추진되고 있다. 유럽 중심의 DVB 표준과, 미국 중심의 ATIS 표준, 그리고 산업체 중심의 OIPF 표준이 대표적이며, ITU-T에서는 이들 표준들에 대한 글로벌 표준화를 목표로 IPTV 보안 관련 권고안 작업을 진행 중에 있다.

본 고에서는 현재 ITU-T SG17 Q.6에서 진행되고 있는 IPTV 보안 관련 권고안을 비롯하여, 국내외 표준화 단체의 IPTV 보안 기술 표준화 동향에 대해 살펴보았다.

현재 진행되고 있는 IPTV 보안 관련 표준화 작업이 유선망에서의 보안 기술에 집중하고 있기 때문에, 향후 IPTV 2.0 서비스의 표준화를 위해 모바일 IPTV 환경에서 적용 가능한 다양한 IPTV 보안 기술의 연구가 선행 되어야 할 것이다.

참 고 문 헌

〔1〕 ITU-T, Functional requirements and architecture for IPTV security aspects, X.1191, 02/2009

〔2〕 EBU Project Group B/CA, Functional model of a conditional access system, EBU Technical Review, Winter 1995

〔3〕 KBS 방송기술연구, DTV 콘텐츠 저작권 보호 기술 및 동향, 2007

〔4〕 황용호, 최문영, IPTV를 위한 다운로드 가능한 CAS 기술, TTA Journal No.126, 11·12/2009

〔5〕 TTA Standard, IPTV 용 교환 가능한 CAS (iCAS), TTAK.KO-08.0023, 2010-03-26

〔6〕 TTA Standard, Non-NGN 기반 Mobile IPTV 요구사항, TTAK.KO-08.0021, 2009-06-18

〔7〕 박수홍, Non-NGN 기반 모바일 IPTV 요구사항, TTA Journal No.125, 9·10/2009

〔8〕 TTA Standard, IPTV 보안 요구사항 및 구조, TTAE.IT-X1191, 2009-12-22

〔9〕 TTA Standard, 스케일러블 비디오 코딩 암/복호화 지침, TTAK.KO-12.0122, 2009-12-22

〔10〕 TTA Standard, CAS와 DRM 간의 상호연동을 위한 인터페이스, TTAK.KO-12.0099, 2008-12-19

〔11〕 TTA Standard, IPTV 서비스 보호를 위한 SEED/ARIA 스크램블링 알고리즘, TTAK.KO-12.0123, 2009-12-22

〔12〕 ATIS Standard, IIF Default Scrambling Algorithm(IDSA), ATIS-0800006, January 2007

〔13〕 ATIS Standard, Secure Download and Messaging, ATIS-0800014, March 2008

〔14〕 ATIS Standard, Certificate Trust Management Hierarchy, ATIS-0800015, August 4, 2008

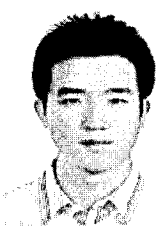
〔15〕 ATIS Standard, Standard PKI Certificate Format, ATIS-0800016, August 4, 2008

〔16〕 DVB-CPCM Part 2, CPCM Reference Model, ETSI TS 102 825-2 V1.1.1, 2008-07

[17] OIPF, Volume7 - Authentication, Content Protection and Service Protection V1.1, Release 1 Specification, 2009-10-08
[18] OMA, Service and Content Protection for Mibile Broadcast Services, OMA-TS-BCAST_SvcCntProtection-V1_0-20090212-A, 12 Feb 2009

〈著者紹介〉

최 현 우 (Hyun-Woo Choi)
학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> IPTV 보안, 스마트그리드 보안, USN 보안, 역추적



정 영 곤 (Young-Gon Jung)
학생회원
2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 스마트그리드 보안, IPTV 보안, 역추적

염 흥 열 (Heung-Youl Youm)
종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜