접근제어시스템간의 상호 운용성을 위한 기술 동향

Trends on Technologies for Interoperability of Various Conditional Access Systems

디지털 홈 특집

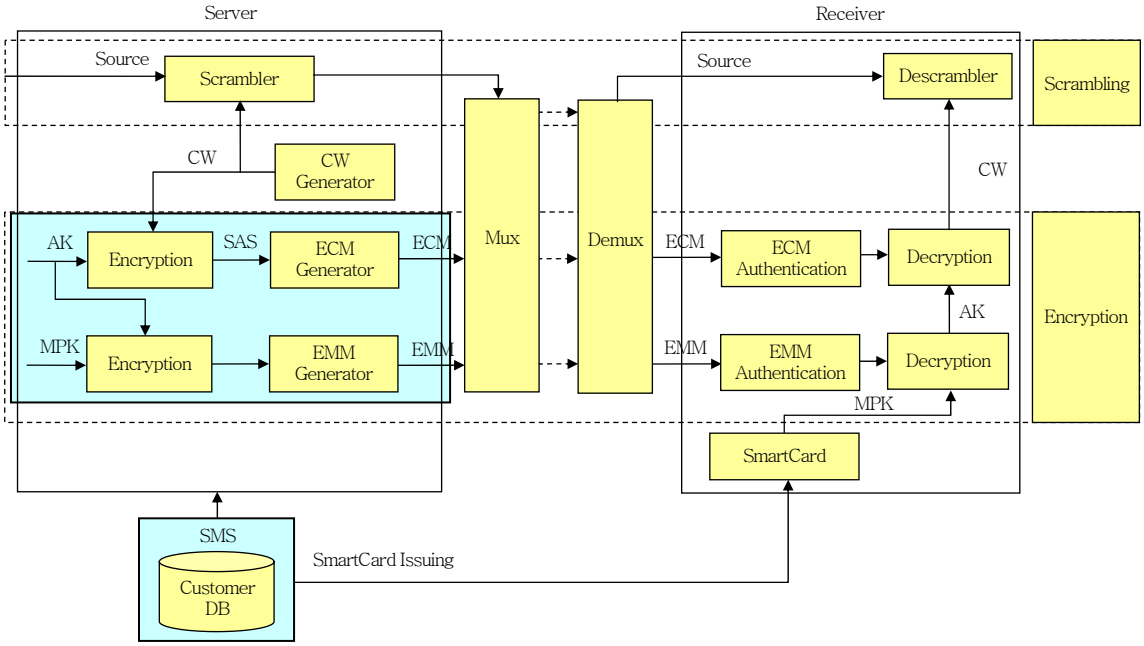
문진영 (J.Y. Moon) 유비쿼터스홈서비스연구팀 연구원
오봉진 (B.J. Oh) 유비쿼터스홈미들웨어연구팀 선임연구원
백의현 (E.H. Paik) 유비쿼터스홈서비스연구팀 팀장

목 차

허가받은 가입자만이 유료 방송 서비스를 수신할 수 있게 하는 접근제어시스템은 유료 콘텐츠를 이용한 비즈니스 모델을 실현하는 핵심 기술이 된다. 현재 접근제어시스템 시장은 업계 1, 2위를 다투는 NDS와 나그라비전의 시장 점유율 합이 70%를 넘는 독점적이고도 폐쇄적인 시장 구조를 유지하고 있다. 이는 접근제어시스템이 과금과 직결되기에 콘텐츠 사업자 및 셋톱박스 제조업체가 일단 하나의 접근제어시스템을 선택하고 나면 쉽게 다른 시스템으로 바꾸지 못하기 때문이다. 이로 인해, 가입자는 방송 서비스 사업자를 바꿀 때마다 새로운 셋톱박스로 교체해야 하는 불편함을 감수해야 한다. 이런 문제를 해결하고 시장에서 다양한 접근제어시스템들이 공존하며 자유롭게 경쟁하기 위해서 다양한 기술들이 표준으로 제안되고 있다. 본 고에서는 디지털 방송을 위한 접근제어기술에서 서로 다른 접근제어시스템간의 상호 운용성을 위한 기술 동향을 알아보도록 한다.

I. 서론

접근제어시스템(CAS)은 유료 TV 시스템에서 자격을 가진 가입자만이 해당 채널을 시청할 수 있도록 하는 콘텐츠 보안 솔루션이다. (그림 1)과 같이, 일반적인 접근제어시스템의 구성요소와 기능은 다음과 같다[1]. 자격 없는 수신자의 접근을 막기 위해 헤드엔드에서는 스크램블링한 콘텐츠를 전송한다. 수신기에서 스크램블된 콘텐츠는 셋톱박스의 접근제어 모듈에서 디스크램블링 과정을 통해 복구된다. 대부분의 접근제어시스템에서는 스크램블링 키와 디스크램블링 키로 동일한 키를 사용하는데, 이를 제어 단어(CW)라고 한다. 수신기에서 디스크램블링을 위해 서버의 스크램블러가 사용한 제어 단어를 전송하는데, 보안을 위해 인증 키(AK)를 이용하여 제어단어를 암호화한 뒤에 자격 제어 메시지(ECM)를 통해 전송한다. 인증 키는 다시 가입자 비밀 키(MPK)를 사용해서 암호화한 뒤에 자격 관리 메시지(EMM)를 통해 전송한다. 고객 정보를 관리하는 가입자 관리 시스템(SMS)에서 접근제어 관련 정보만을 가지고 가입자의 가입 및 탈퇴에 따라 자격 관리 메시지와 자격 제어 메시지를 생성하여 신규 가입자가 가입한 방송 채널을 수신하거나 탈퇴한 가입자가 더 이상 방송을 수신하지 못하도록 하는 기능을 가입자 인증 시스템(SAS)에서 제공한다. 가입자 비밀 키는 스마트카드 안에 내장되어 가입자 관리 시스템을 통해 가입자에게 배포된다. 수신기에서 자격 제어 메시지와 자격 관리 메시지를 받으면 메시지 확인 과정을 거친 뒤에 서버에서 수행한 역순으로 복호화 과정을 수행한다. 먼저 스마트카드 안에 내장된 가입자 비밀 키를 가지고 인증 키를 복호화 한다. 그런 다음 복호화된 인증 키를 가지고 제어 단어를 복호화하여 디스크램블링에 사용한다. 여기서 제어 단어와 가입자 비밀 키 사이에는 필요에 따라서 하나 이상의 키를 둘 수 있는데, 이는 시스템 효율 및 접근제어시스템이 지원하는 비즈니스 모델에 따라 서로 다르게 구성될 수 있다[2]. 이와 같이, 접근제어시스템은 크게 동영상 및 데이터 콘텐츠에 대한 스크램블링 과정과 제어 단어 및 구성 키들의 암호화 및 복호화 과정으로 구성된다. 대개 가입자 댁내의 셋톱박스에 수신 접근제어 모듈이 임베디드 시스템으로 탑재되어 방송 서비스의 수신을 제어한다.



(그림 1) 개념적인 CAS 구성도

접근제어시스템은 유료 채널에 대한 제한 수신을 가능하게 하여 유료 채널을 이용한 비즈니스 모델이 수익을 창출할 수 있게 해주는 핵심 기술이 된다. 따라서 방송 사업자는 접근제어시스템의 도입에 신중할 수 밖에 없다. 그러나 일단 한 제품을 도입하고 나면 쉽게 다른 접근제어시스템으로 바꾸지 못한다. 세계 유료 방송 시장에서 접근제어시스템 1, 2위 업체인 영국의 NDS와 스위스의 나그라비전의 시장 점유율의 합이 70%라는 점은 접근제어시스템 시장이 얼마나 독점적이고 폐쇄적인지를 잘 보여준다. 독점적 시장에 의한 피해는 콘텐츠 제공자인 방송 사업자뿐만 아니라 이를 이용하는 가입자에게까지 미친다. 가령 가입자가 케이블 TV 사업자를 바꾸면 기존의 셋톱박스를 더 이상 쓰지 못하고 새로 구매하거나 임대해야 한다.

디지털 방송 표준화 단체에서는 특정 접근제어시스템 제품에 대한 의존도를 줄이고, 다양한 제품이 시장에서 공존하며 자유롭게 경쟁할 수 있도록 상호 운용성을 고려한 접근제어시스템 모델을 제안하고 있다. 따라서, 본 고에서는 접근제어시스템간의 상호 운용성 제공을 위해 표준화 단체에서 제안한 접근제어 기술들을 살펴보기로 한다. Ⅱ장에서는 먼저 대표적인 디지털 방송 표준화 단체인 DVB에서 제안한, 접근제어시스템간의 상호 운용성을 고려한 두 시나리오인 Simulcrypt와 Multicrypt를 알아본 다음, 미국 오픈케이블에서 케이블 방송 수신을 위해 가입자 셋톱박스 내에 접근제어 모듈을 올린 케이블카드에 대해 살펴보고, Ⅲ장에서는 NGNA 프로젝트에서 제안하는 소프트웨어 다운로드가 가능한 접근제어시스템에 대해 알아보기로 한다. 그리고 마지막 Ⅳ장에서는 결론을 맺는다.

● 용 어 해 설 ●

NGNA: 컴캐스트케이블, 타임워너케이블, 콕스 커뮤니케이션 등의 미국 대표 MSO들이 주축이 되어 기존의 케이블 TV 망을 통해 디지털케이블방송, 유무선 전화, 초고속 인터넷, 홈네트워크 등 각종 융합서비스를 제공하는 인터넷 망 기반 네트워크를 구축하는 프로젝트이다. 광동축혼합망인 기존의 케이블 TV 망에 대규모 투자없이 광대역 IP 망 인프라를 구축하고 아날로그 케이블 TV의 디지털 전환을 넘어 향후 통신영역에서 가능한 모든 사업 진출을 목표로 하고 있다.

Ⅱ. 상호 운용성 있는 접근제어 시스템

본 장에서는 대표적인 디지털 방송 표준화 단체 DVB에서 서로 다른 접근제어시스템들이 시장에서 공존하며 자유롭게 경쟁할 수 있는 상호 운용성 있는 접근제어시스템을 위해 제안한 두 가지 시나리오 Simulcrypt와 Multicrypt에 대해서 알아보고, 미국 케이블 산업에 대한 기술적 연구를 계획하고 자금을 지원하는 케이블랩스에서 추진중인 오픈케이블(Open Cable) 표준에서 제안한 교체 가능한 하드웨어 장치인 케이블카드를 이용한 접근제어시스템 기술에 대해서 알아본다.

1. DVB의 Simulcrypt

DVB에서는 1993년 이래로 디지털 방송을 위한 접근제어 기술의 표준화 활동을 진행하고 있다. DVB 프로젝트에서는 DVB 시스템에서 접근제어 요소들에 지적재산권이 있을 수 있음을 받아 들이면서도, 시장에서 여러 다른 접근제어시스템들이 공존하며 사용될 수 있어야 한다는 데 초점을 두었다. 이를 위해서 헤드엔드에서 콘텐츠를 하나의 동일한 알고리듬으로 스크램블링 하되, 접근제어와 관련된 자격 관리 메시지와 자격 제어 메시지는 접근제어시스템별로 각자의 방법으로 페이로드를 채워 전송할 수

● 용 어 해 설 ●

오픈케이블(OpenCable): 미국에서 케이블 TV 산업을 위한 차세대 디지털 가전을 정의하기 위해 케이블랩스(CableLabs)에 의해 개발중인 하드웨어 및 소프트웨어 스펙들의 집합이다. 디지털 케이블 TV를 위한 하드웨어 및 소프트웨어 공통 표준을 만들어, 어느 한 소프트웨어가 디지털 TV를 지배하는 것을 배제하면서 라이선스를 받은 장치 제조업체간의 경쟁을 촉진하는 것을 목적으로 한다.

있도록 하였다. 이것이 DVB Simulcrypt[3]의 기본 개념으로, 이를 실현하기 위해서 공통된 스크램블링 알고리듬인 CSA[4]를 제안하였다.

1994년에 DVB 컨소시엄에서 채택된 CSA의 상세 내용은 NDA를 맺은 스크램블러 제조업자에게만 공개되어 하드웨어로 구현하도록 규정하고 있다. 따라서 접근제어시스템 업체별로 서로 다른 접근제어 모듈을 두더라도 각 접근제어 모듈에서 제어 단어를 획득하고 나면 제품에 상관없이 DVB CSA를 지원하는 디스크램블러를 가지고 콘텐츠를 디스크램블링 할 수 있다.

Simulcrypt는 기존 수신기를 수정 없이 그대로 사용할 수 있다는 장점이 있으나, 서버에서 접근제어시스템별로 각기 다른 자격 관리 메시지와 자격 제어 메시지를 생성하여야 하므로, 하나의 접근제어시스템에서 하나의 자격 관리 메시지와 자격 제어 메시지를 생성하여 전송할 때와 비교해서 사용 대역폭이 크게 증가하고 컴퓨팅 부담이 커진다는 단점이 있다.

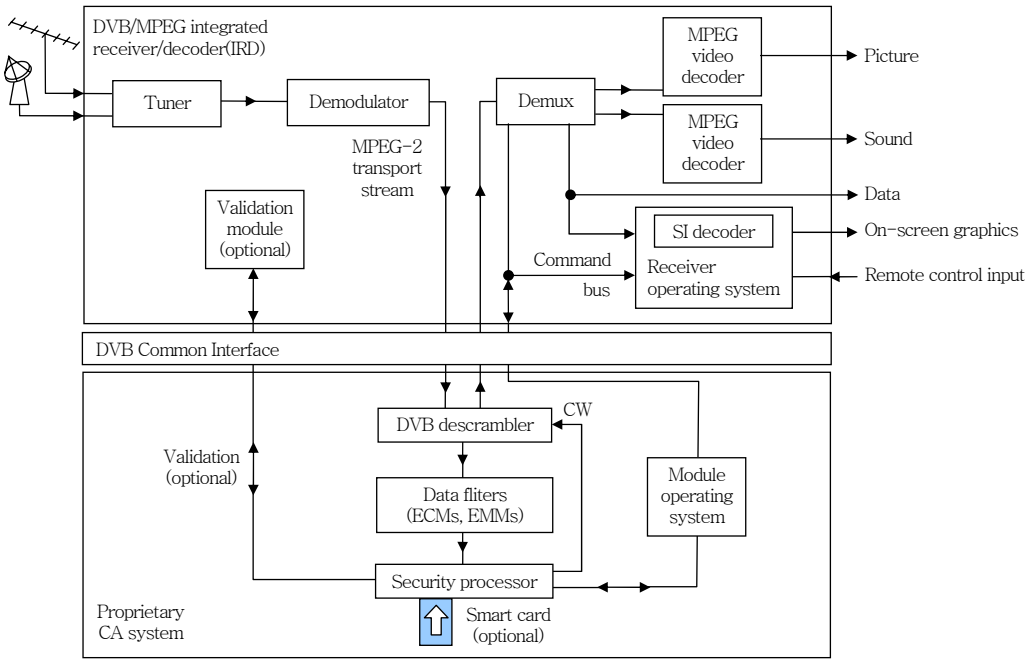
Simulcrypt 스펙은 Simulcrypt 그룹의 활동으로 2개의 ETSI 표준 문서[5],[6]로 정리되고, 2001년 1월에 결성된 SimExt 그룹에서 이전 스펙을 보완하여 다시 2개의 ETSI 표준 문서[7],[8]로 추가 정리했다.

서로 다른 접근제어시스템의 공존을 고려한 Simulcrypt는 ATSC의 접근제어시스템[9]에서 스크램블링 알고리듬을 제외하고 그대로 채택되었다. 스크램블링 알고리듬만 ATSC에서 제안한 ATSC CSA를 사용하도록 하고 있다.

2. DVB의 Multicrypt

상호 운용성을 위해 제안된 또 다른 시나리오는 하나의 수신기에서 하나 이상의 접근제어시스템을 수용하도록 규정한 Multicrypt이다. 이를 위해 시그널이 셋톱박스 내부에서 서로 다른 접근제어 모듈을 순차적으로 통과하도록 한다.

이를 위해서 1997년에 DVB에서는 수신기에서 접근제어 모듈을 분리하기 위해, 지적재산권을 가진 접근제어 모듈과 호스트(MPEG 디코더와 튜너) 사이에 위치한 입출력 인터페이스인 CI[10]를 제안하였다.

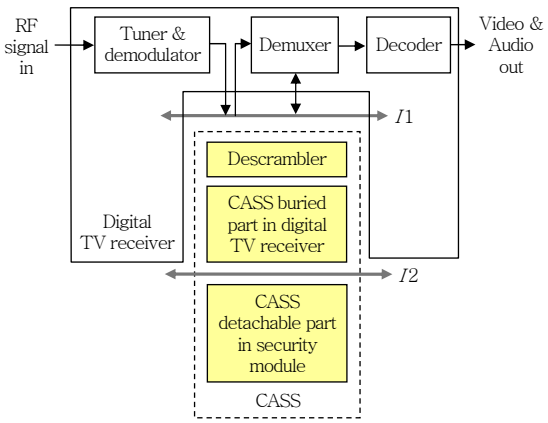


(그림 2) DVB Common Interface를 포함하는 수신기 구조도

접근제어 모듈은 사용자 개인 정보인 가입자 비밀 키와 자격 제어 메시지 및 자격 관리 메시지 처리부, 제어 단어를 추출하기까지의 단계적인 키 복호화 처리부, DVB 디스크램블러로 구성된다. 이 부분은 각 접근제어시스템 업체별로 자사의 지적재산권에 있는 구성 요소로 만들도록 하되 DVB CI를 따르는 경우 특정 제품에 상관없이 연동이 용이하다. Multicrypt에서 스마트카드의 사용 여부는 선택적이다. DVB CI를 사용하는 수신기의 구조는 (그림 2)와 같다[1].

DVB CI에서는 디스크램블링 기능까지 독립적인 접근제어 모듈로 분리한 인터페이스를 제시하는데, 접근제어 모듈의 입력과 출력은 MPEG TS 레벨이다. 이 방식은 (그림 3)의 I1 인터페이스와 같은 방식이다[11]. 2001년에 제안된 오픈케이블의 케이블카드 인터페이스와 1999년 제안된 NRSS-B, 1998년에 제안된 DAVIC CA0들이 DVB CI와 같은 방식으로 I1에 위치한 인터페이스들이다. 이 방식의 경우 수신기와 접근제어 모듈간에 많은 양의 데이터가 송수신되므로 스마트카드 보다는 빠른 데이터 전송속도를 제공하는 PCMCIA 카드를 사용한다.

DAVIC CA1은 I2에 위치한 인터페이스이다. 그런데 DAVIC CA1은 인터페이스뿐만 아니라 어떤 데이터 객체를 사용할지 그리고 데이터 객체들을 저장하는 데 어떤 스마트카드 파일 시스템을 사용해야



(그림 3) 디지털 TV 수신기와 CA 모듈간의 인터페이스의 가능한 두 위치

하는지 등의 구체적인 구현 조항을 기술하고 있기에 스마트카드에서 구현에 관련된 세부사항을 밝히길 꺼려하는 접근제어시스템 업체들 사이에서 널리 사용되지 못하고 있다[11].

Multicrypt의 장점은 셋톱박스의 기능 설계를 간소화 시켰다는 것이다. 셋톱박스가 더 이상 스크램블링과 접근제어 모듈을 포함할 필요가 없이 DVB Multicrypt를 따르는 CI에 맞추어 설계하면 CI에 맞추어 제작된 어느 접근제어시스템이든지 셋톱박스에 연동할 수 있다. 그리고 접근제어시스템의 업그레이드가 용이해서, 접근제어시스템의 업데이트가 필요하면 가입자 댁내의 셋톱박스는 그대로 두고도 접근제어 모듈만 업그레이드하면 된다.

3. 오픈케이블의 케이블카드

미국에서는 1996년 12월, 방송통신융합법인 텔레콤 액트(Telecom Act)를 통과시켜 접근제어 모듈이 분리된 셋톱박스를 규정하고, 1998년 9월 셋톱박스와 접근제어 모듈의 분리를 명시하였다. 수신기 업체의 독점을 막기 위해서 케이블랩스에서 오픈케이블 접근제어 표준을 제정하였다. 케이블카드 인터페이스 스펙을 포함하는 오픈케이블에서 발표한 접근제어 표준에는 Simulcrypt와 같은 헤드엔드 장비와 공통 스크램블링 알고리듬에 대한 표준은 없다. 케이블카드에서 스크램블링에 대한 모든 책임을 지도록 규정하고 있다. 케이블카드란 POD 모듈의 트레이드 마크화된 용어로, 접근제어시스템 제품별로 각자의 접근제어 모듈로 구현되어 호스트에 삽입된다. 소비자가 케이블 TV 사업자의 시스템에 종속된 셋톱박스를 구매 또는 임대하는 것이 아니라 케이블카드를 지원하는 셋톱박스를 구입한 뒤 해당 케이블 사업자의 케이블카드만 꽂으면 된다. 그리고, 업그레이드를 위해서 케이블카드만 교체하면 된다.

미국에서는 2005년 1월, 셋톱박스와 접근제어 모듈간의 분리를 의무화 하였으나 케이블 TV 방송사와 연방통신위원회간의 대립으로 분리 의무시점을 2006년 7월로 연기하고, 2005년 4월에 다시

2007년 7월 이후로 연기하였다. 케이블 카드의 도입이 셋톱박스의 원가를 높일 뿐만 아니라, 도입된 시스템에서 발열문제로 셋톱박스 성능이 저하되고, 잦은 고장으로 AS 요청이 많아지는 등의 문제점으로 인해 케이블카드를 의무적으로 도입하도록 규정하기 어려운 상황이다.

Ⅲ. 다운로드 가능한 접근제어 시스템

케이블카드와 같은 하드웨어 기반의 접근제어시스템의 한계를 극복하고자 새롭게 제시되고 있는 것이 소프트웨어 다운로딩 방식의 접근제어시스템이다. 현재 디지털 가입자 망(DSL)을 이용한 IP 망이나 DAVIC 또는 DOCSIS 기반의 리턴 패스를 가지는 양방향 케이블망에서는 다운로드 및 업로드가 모두 가능하다. 이런 전송망의 양방향성을 이용해서 수신기에 접근제어 모듈을 다운로드하고, 사용자 인증을 위한 키 교환관련 필요한 데이터를 업로드 및 다운로드 하는 소프트웨어 다운로딩 방식의 접근제어 기술이 대두되고 있다.

미국에서는 디지털 케이블 망에서 접근제어시스템을 다운로드 하는 DCAS가 등장하였다. 미국 복수 유선사업자들은 연방통신위원회가 규정하고 있는 분리 의무화를 케이블카드를 교체하는 셋톱박스뿐만 아니라 소프트웨어 다운로딩 방식의 DCAS까지 포함하도록 요구하고 있다. 이미 2006년 1월에 CES에서 LG전자가 컴캐스트, 나그라비전과 공동으로 DCAS를 첫 공개 시연한 것을 시작으로, 4월 NCTA 2006 내셔널쇼에서 모토롤라와 사이언티픽 애틀랜다 등 미국 셋톱박스 업체와 삼성전자 등이 DCAS 방식의 셋톱박스를 전시했다.

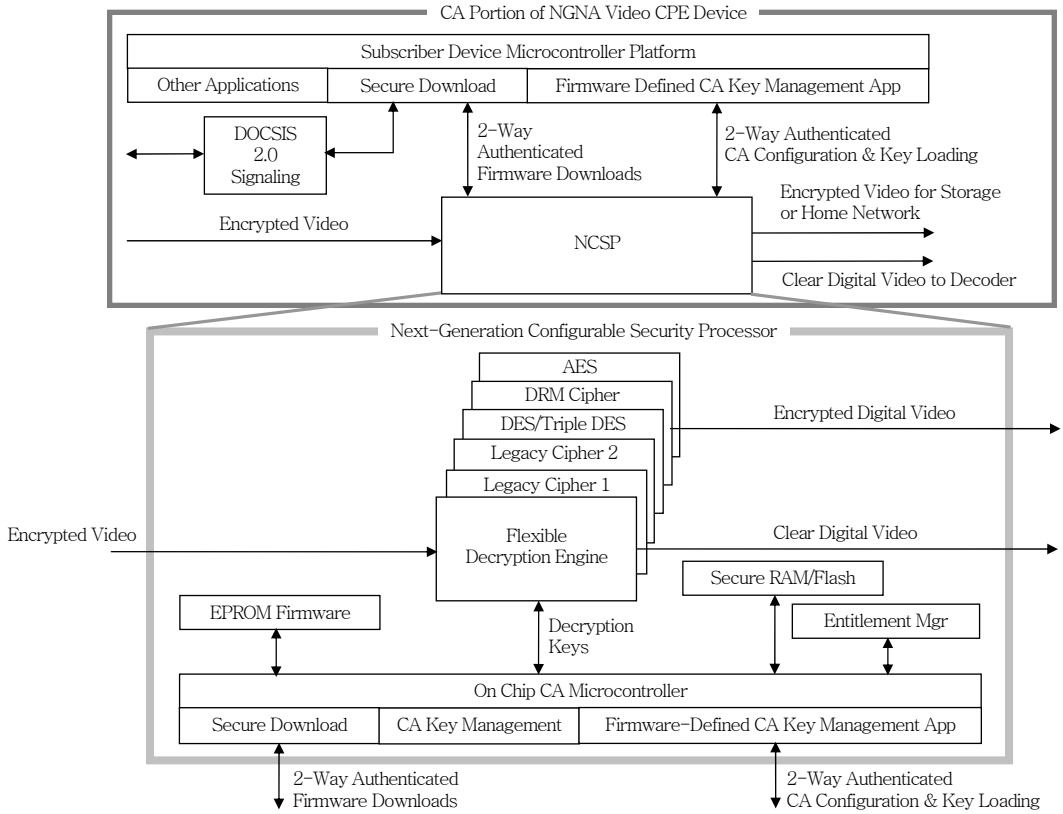
본 절에서는 미국 3대 복수 유선 사업자인 컴캐스트, 콕스 커뮤티케이션 그리고 타임워너 케이블이 주축이 되어 현재 케이블 TV 망인 광동축혼합망(HFC) 인프라에 추가적인 비용 투자 없이, 제품 혁신과 가격 절감을 유도하는 통합 멀티미디어 구조의 구현을 목표로 하는 NGNA 프로젝트[12]에서 새롭게 제안하고 있는 소프트웨어 다운로딩 방식을 도입한 NGNA 보안 모델에 대하여 살펴 보도록 한다.

1. NGNA 보안 모델

NGNA의 보안 모델은 크게 하드웨어 기반이나 원격으로 재구성 가능한 콘텐트와 키 암호화/복호화 시스템, 소프트웨어 기반 접근제어 모듈의 다운로딩으로 재정의할 수 있는 키 관리 시스템 그리고 부분적으로 소프트웨어 기반 접근제어 모듈 다운로딩으로 업데이트 가능한 인증 시스템의 3가지 서브 시스템으로 구성된다. 기존 디지털 방송의 보안 모델과 뚜렷한 차이점은 하드웨어 기반 시스템을 원격으로 재구성할 수 있고, 소프트웨어 기반 시스템도 다운로드에 의해 접근제어시스템의 일부를 업데이트 할 수 있다는 점이다.

위의 서브 시스템들은 새로운 접근제어 알고리듬뿐만 아니라 보편적으로 사용되는 레거시 접근제어 알고리듬을 포함하여 이미 정의된 여러 개의 스크램블링 알고리듬을 지원하는 복호화 엔진을 원격으로 재구성하거나, 접근제어 키 교환 메커니즘을 소프트웨어로 정의하는 초기 다운로딩이나 업데이트하는 방식으로 케이블 운영자를 지원할 수 있다. 비디오 서비스의 보안을 책임지는 NCSP는 (그림 4)와 같이, DES, 3-DES, CSA 그리고 AES와 같은 다양한 암호화 알고리듬을 지원하는 복호화 엔진이 있어 암호화된 전송 스트림을 복호화 시킨다[12].

NGNA 플랜은 복수 유선 사업자가 지적재산권이 있는 접근제어시스템뿐만 아니라 새로 표준화되는 접근제어시스템을 사용할 수 있게 하여, 케이블 운영자를 위한 다수의 접근제어 모듈 중에서 선택 가능하도록 지원한다. 접근제어 기술의 선택은 헤드엔드 쪽의 영향을 받기 때문에 NCSP에 들어가 있는 접근제어시스템은 하나의 접근제어 모듈에서 다른 접근제어 모듈로의 전환이 가능해야 한다. 그리고, 케이블카드 인터페이스를 가지는 가입자 장치는 케이블카드가 인스톨되어 있지 않으면 NCSP가 디폴



(그림 4) NGNA 보안 참조 모델

트가 된다. 이와 같이 케이블카드를 고려하는 것은 미국 정부의 분리 의무화 정책을 최대한 존중하는 NGNA 기본 방침을 보여준다.

2. NGNA 보안 모듈 업데이트

알고리듬 특정 부분, 키 교환, 키 관리 그리고 암호 프로토콜은 NCSP에 소프트웨어 또는 업데이트 가능한 펌웨어로 구현된다. 콘텐츠 보안 요소의 소프트웨어 업데이트는 하드웨어 업데이트보다 저렴하고 업데이트가 용이하기 때문에 차세대 네트워크에서 일반화 되리라 예상된다. 그러나 하드웨어 보안 요소도 고품질 콘텐츠를 위한 효율적인 보안 시스템을 위한 필수 요소라고 보기에, 암호 함수가 범용 프로세스에서 수행되는 소프트웨어 단독의 접근제어 모듈은 지원하지 않을 예정이다. 소프트웨어와 특화된 하드웨어는 서로 상호보완적이며, 소프트웨어 또는 하드웨어 전용보다 좀더 안전하다는 콘텐츠 보안 시스템 업계 전반의 인식을 반영한 것이다.

그리고, NGNA 보안 모듈 업데이트는 사용자 인터페이스와 디바이스 오퍼레이션 그리고 애플리케이션 지원을 제어하는 범용 제어 펌웨어, NCSP와 통신하고 관리하는 내부 펌웨어, NCSP에 하드웨어 엔진과 (또는) 접근제어 키 관리 펌웨어를 재구성하는 보안 메시지의 세 가지 타입의 펌웨어 보안 다운로드를 지원한다. 이 보안 다운로드는 보안 채널에 대해서 가입자 비디오 디바이스로의 전송을 위해 암호화된다. 모든 보안 다운로드 경로는 양방향 인증 교환을 필요로 하고, 블록 사이에 물리적으로 접근할 수 있는 시그널 경로는 암호화한다는 것을 가정한다.

비록 소프트웨어 업데이트가 좀 더 비용면에서 경제적이고 구현하기도 쉬우나, NCSP에서의 키 관리와 전송 스트림 복호화를 위해서는 어느 정도의

하드웨어 업데이트가 필요하다. 전송 스트림의 대역폭을 지원할 수 있는 분리 가능한 하드웨어를 사용하는 여러 방식으로 키를 관리하고 전송 스트림을 복호화하는 하드웨어를 업데이트 할 수 있다. 예를 들어, 멀티스트림 케이블카드 인터페이스를 지원하는 NGNA 디바이스에 케이블카드를 삽입함으로써 하드웨어를 완전히 업데이트 할 수 있다.

Ⅳ. 결론

본 고에서는 여러 접근제어시스템간의 상호 운용성을 위한 기술 및 표준화 현황을 알아 보았다. 처음에 임베디드 시스템 형식으로 셋톱박스에 내장되었던 접근제어시스템은 DVB의 Simulcrypt를 통해 헤드엔드에서의 상호 운용성 개념을 도입하고, DVB의 CI를 통해 수신기에서 호스트와 접근제어 모듈을 분리하여 DVB CI를 따라 설계한 셋톱박스에는 CI를 따르는 어느 접근제어시스템도 쉽게 연동될 수 있게 해 주었다. 그리고 케이블 TV에서는 케이블카드를 도입하여 가입자가 케이블 TV 방송사를 변경할 경우 케이블 셋톱박스를 바꾸는 것이 아니라 케이블카드만 교체하면 되도록 하였다. 그러나 교체 가능한 스마트카드 기반의 접근제어시스템이 하드웨어적으로 문제가 많은 것으로 밝혀졌고, 방송망이 디지털화되고 양방향화된 현 상황에서 업데이트가 훨씬 용이한 소프트웨어 다운로딩 방식이 대두되고 있다. 미국 케이블업계에서는 케이블카드 대신에 소프트웨어 다운로드 가능한 DCAS를 통해 셋톱박스 내의 호스트와 접근제어 모듈을 분리하는 추세이다. 그러나, NGNA 프로젝트에서 제안하는 소프트웨어 다운로딩 방식의 접근제어시스템이 하드웨어를 배제한다는 것은 아니다. 오히려 기존의 하드웨어와 소프트웨어를 동시에 사용하여 하드웨어의 안정성과 소프트웨어의 업데이트 용이성이라는 장점을 모두 살리도록 하고 있다. 현재 순수 소프트웨어 기반 접근제어시스템 제품이 등장하고 있으나, 전통적 접근제어시스템에서 하드웨어 장치의 보안에 대한 신뢰가 커서, 소프트웨어만을 사용한 접근제어시스템의 표준화는 논의되지 않고 있다.

현재 새로운 이슈가 되고 있는 IP 망에서의 IPTV 서비스에서의 접근제어시스템에 대한 표준화 활동이 ITU-T 등에서 활발히 진행중이다. 케이블 망의 디지털화 및 양방향화가 DCAS를 도입시켰듯이 IP 망에서는 IP 망의 고유한 특성 및 망 내의 보안 시스템을 활용하여 하드웨어 의존도를 최소화시키고 업데이트가 용이한 소프트웨어 다운로딩을 활성화한 접근제어 표준의 등장이 예상된다.

약 어 정 리

3-DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AK	Authentication Key
ATSC	Advanced Television System Committee
CAS	Conditional Access System
CI	Common Interface
CSA	Common Scrambling Algorithm
CW	Control Word
DAVIC	Digital Audio Video Council
DES	Data Encryption Standard
DOCSIS	Data Over Cable Service Interface Specifications
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
EBU	European Broadcasting Union
ECM	Entitlement Control Message
EMM	Entitlement Management Message
HFC	Hybrid Fiber Coax
IP	Internet Protocol
IPTV	Internet Protocol Television
ITU-T	ITU Telecommunication Standardization Sector
ITU	International Telecommunications Union
MPK	Master Private Key
NCSP	NGNA Configurable Security Processor
NCTA	National Cable Television Association
NDA	Non-Disclosure Agreement
NGNA	Next Generation Network Architecture
NRSS	National Renewable Security Standard
PCMCIA	Personal Computer Memory Card International Association

POD Point Of Deployment
SAS Subscriber Authorization System
SMS Subscriber Management System

참 고 문 헌

[1] EBU Project Group B/CA, Functional model of a conditional access system, EBU Technical Review, Winter 1995.
[2] F.K. Tu, C.S. Laih, and H.H. Tung, "On Key Distribution Management for Conditional Access System on Pay-TV System," *IEEE Trans. On Consumer Electronics*, Vol.45, Feb. 1999, pp.151-158.
[3] ETSI TS 103 197 v1.4.1, Digital Video Broadcasting(DVB) Head-end implementation of DVB Simulcrypt, Dec. 2004.
[4] ETSI Technical Report 289: Support for use of scrambling and Conditional Access within digital broadcasting system, 1996.
[5] ETSI TS 101 197 V1.2.1, DVB Simulcrypt; Part 1: Head-end architecture and synchronization, 2002. 2.
[6] ETSI TS 103 197 V1.2.1, Head-end Implementation of Simulcrypt, 2002. 2.
[7] ETSI TR 102 035 V1.1.1, Implementation Guidelines of the DVB Simulcrypt Standard, Apr. 2002.
[8] ETSI TS 103 197 V1.3.1, A new version of the Simulcrypt standard including a revision of the architecture model and the specification of two new interfaces, 2003. 1.
[9] ATSC Standard, Conditional Access System for Terrestrial Broadcast, Revision A, 2004.
[10] Common Interface Specification for Conditional Access and other digital video broadcasting applications, EN50221, 1997.
[11] Xie Qiang, Zheng Shi-bao, and Yu Xiao-jing, "A Smart card Conditional Access Interface Scheme for Conditional Access Subsystem Separation in Digital TV Broadcasting," 2006.
[12] NGNA LLC, "NGNA Plan: Integrated Multimedia Architecture," 26 July 2004.