IPTV 접근제어 표준 및 서비스 기술

서 창 호 | 공주대학교 정보보호전공 부교수
박 종 열 | 한국전자통신연구원 유비쿼터스홈서비스연구팀 선임연구원
문 진 영 | 한국전자통신연구원 유비쿼터스홈서비스연구팀 연구원
백 의 현 | 한국전자통신연구원 유비쿼터스홈서비스연구팀 팀장

u-Home 표준화와 서비스 특집

1. 서론

정보기술에 있어서 인가되지 않은 노출이나 조작에 의한 정보의 유출이나 데이터 보호 및 사생활 보호를 위해 데이터 암호화, 실체 인증과 같은 암호학적인 메커니즘의 사용요구가 폭발적으로 증가하고 있다. 특히 위성을 이용한 디지털 방송의 다채널 시대에, 가입자는 개별화된 전문채널 서비스를 받을 수 있고, 한편 방송사업자는 기존 지상파에서 광고료 수입에만 의존하던 방송서비스 운영을 TV 방송에 가입자 개념을 추가하여 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하고, 전문 방송사업자들에 의한 전문 방송 프로그램의 제작을 가능케 하여 다양한 기능의 서비스를 제공할 수 있게 되었다. 즉, 다채널 방송시대의 방송사업자는 광고료 수입에만 의존하던 경영 방식을 탈피하여 가입자의 시청료에 의해 운영함으로써, 가입자는 전문화된 채널 및 개인별로 차별화된 보다 양질의 서비스를 받을 수 있는 장점들을 가지고 있다.

이러한 조건부 제한수신 서비스를 만족할 수 있는 시스템 즉, 제한수신시스템(CAS: Conditional Access System)이란, 송신기에서 스크램블된 신호를 수신측의 수신 인가를 받은 가입자만이 디스크램블하여 프로그램을 시청할 수 있도록 하는 시스템으로, 이 시스템이 갖추어야 하는 기본적인 요건은 프로그램 및 데이터에 스크램블링되고, 통신링크 상에서 보호되어야 하며, 인증을 위한 가입자 신분확인(Authentication) 기능과 접근제어(Access Control)기능을 갖추어야 한다.

또한 다양한 디지털방송 환경(DMB, 지상파방송, 위성방송, 케이블 TV, IPTV)에 적용이 용이한 iCOD 콘텐츠 응용을 위한 셋톱박스 기반의 동적 접근제어에 있어 요구되는 접근제어 표준 및 서비스 기술은 매우 중요하다고 볼 수 있다.

2. IPTV 서비스 동향

2.1 IPTV의 정의

IPTV는 현실적으로는 인터넷을 기반으로 하는 TV 서비스라는 기본 개념을 공통적으로 수용하고 있으며, 대부분 국가별, 사업자별로 VoD, 인터넷 TV, IPTV 등과 같은 개념이 혼용되어 쓰이고 있다.

한 편, IPTV는 'Internet Protocol TV', 'Interactive Personal TV, 'Intelligent Program Television TV' 라는 세 가지 특징을 갖는다[1]. 즉, IP를 기반으로 쌍방향서비스가 가능하고, point-to-point 전달방식으로 개인화된 채널을 볼 수 있으며 초고속 인터넷, VoIP와의 결합을 통해 TPS 번들서비스 제공이 가능하다.

위와 같은 점에서 찾아볼 수 있는 IPTV의 가장 큰 특징은 방송용 전파가 아닌 인터넷 프로토콜을 이용한 패킷방식으로 멀티미디어 콘텐츠를 제공하고 PC가 아닌 TV 단말기를 통해 다양한 서비스를 제공한다는 점이다. 이 같은 특징 때문에 미국에서는 IPTV, 유럽에서는 ADSL TV, 일본에서는 브로드밴드 방송이라고 정의한다[2].

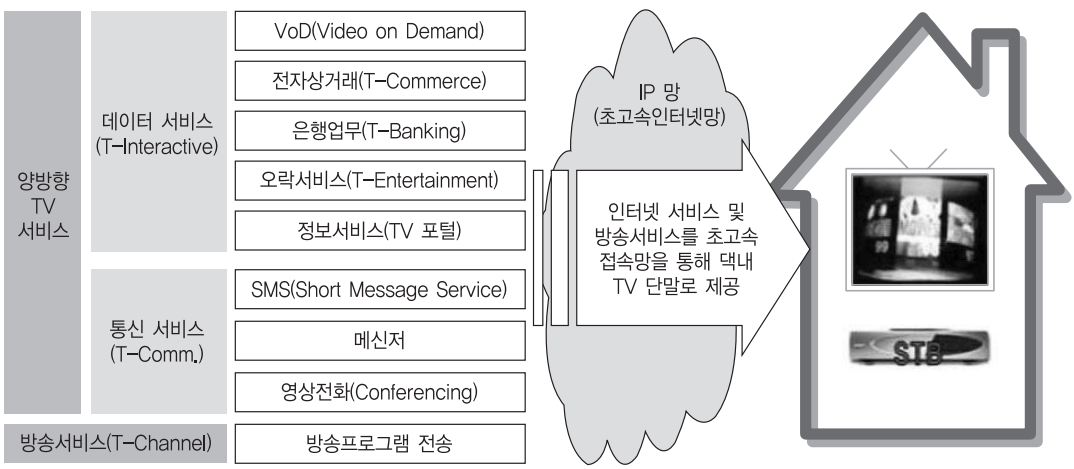
[그림 1]에서와 같이, IPTV는 기존에 PC 기반으로 인터넷서비스를 제공하는 통신기능과 다채널 TV 방송서비스를 제공하는 방송기능이 통합된 서비스 개념을 포괄할 뿐만 아니라, 동시에 VoD, EPG, T-커머스, 방송프로그램 연동형 데이터 서비스와 같은 새로운 양방향 콘텐츠를 제공하는 통신과 방송기능이 모두 녹아 있는 융합서비스인 것이다.

2.2 IPTV 표준화 기관 동향

IPTV 서비스는 초고속 인터넷 망의확산과 디지털화된 방송 프로그램 제작이라는 기술적 뒷받침, 그리고 통신과 방송의 융합이라는 새로운 패러다임 속에서 이미 전세계적인 추세로 받아들여지고 있다. 그리고 시장의 확대 및 활성화를 위해서 세계 각국의 주요 사업자들은 각 표준화 기관을 중심으로 표준 제정에 힘쓰고 있다. 따라서 본 장에서는 IPTV 서비스를 위한 표준화 기관 동향에 대해 알아본다.

2.2.1 DVB

1993년부터 정식으로 시작된 DVB 프로젝트는 디지털TV와 데이터 서비스의 범세계적 전송을 위한 국제 표준을 만들기 위해 35개 국 이상의 270개 방송사, 제조업자, 전송망 사업자, 소프트웨어 개발자, 입법부로 구성된 산업 주도형 컨소시엄이다. 현재 DVB 프로젝트는 유럽, 아시아, 호주, 북미 등에서 디지털 TV를 전달하기 위한 일반적이면서 다양한 종류의 표준들을 만들고 있



[그림 1] IPTV 서비스 개념

다. 이미 전세계 1억 DVB 수신자들이 지상파, 위성파, 케이블 TV 및 MHP와 같은 DVB 스펙을 사용한 서비스를 이용하고 있다[3].

가장 활발히 진행 중인 분야는 2005년 3월에 Pro-MPEG 포럼에서 제안하고 있는 방송 데이터의 IP 데이터 프로그램으로의 전달방법, 특히 패킷 손실을 줄이기 위해 IP 레벨의 FEC에 대한 새로운 스킴으로, 이를 통해 방송 데이터의 패킷 손실을 해결하려고 하는 것이 중요한 이슈로 대두되고 있다. 또한, DLNA와 연계하여 홈 네트워크 내에서 서비스 품질(QoS), 복제방지를 위한 기술 등에 관한 사항도 중요한 논의사항으로 자리잡고 있다[4].

2.2.2 ATSC

ATSC는 HDTV 방송 표준을 위한 기술적인 표준을 수립하기 위해 1982년에 창립된 비영리 국제표준화 단체이다. 오늘날 아날로그 방송의 3~5배 고감도 영상을 제공할 수 있다. 미국 내에서 이미 서비스를 시작한 디지털방송에서 이미 정식으로 채택되었으며, 미국, 캐나다, 한국, 대만, 아르헨티나 등에서 ATSC 디지털 TV 표준을 지상파 방송을 위해 채택하였다. 2005년 9월, ATSC는 데이터방송 표준으로 US케이블 산업계의 OCAP과 ATSC의 DASE를 통합하고 케이블, 위성, 지상파의 양방향(interactive)TV를 지원하도록 디자인된 ACAP 표준을 제안하였다. ACAP은 콘텐츠 제작자, 방송사, 케이블 사업자, 그리고 가전업체에게 상호 운영 가능한 서비스와 제품을 위해 필요한 세부 기술을 제공하여 소비자에게 향상된 양방향 서비스를 제공할 수 있게 해준다. 양방향 애플리케이션을 위한 미들웨어 스펙으로써 ACAP은 콘텐츠 제작자와 애플리케이션 개발자들이 만든 프로그램과 데이터가 모든 브랜드 및 모든 모델의 수신기에서 동일하게 수신되어 실행됨을 보장한다. ACAP 표준을 이용한 데이터방송은 우리나라가 세계 최초로 상용화에 성공하였고, 2004년 6월 말부터 지상파 시험 방송을 시작하였다[5].

ATSC는 한국에서 2001년 ATSC 서비스를 시작한 이후, 2005년 현재 80%의 점유율을 가지고 있는 것으로 예측하고 있다. 스카이라이프㈜에서 ATSC의 표준에 따라 서비스하고 있고, 지상파 및 위성DMB도 이를 따를 것으로 예상된다. 이외에도 비영리적인 기구인 ETSI, 케이블랩스, OSGi 얼라이언스와 미국이 주도하는 ATIS IIF, 그리고 ITU SG13 회의에서 신규 표준화 아이템으로 채택된 ITU-T 등에서 표준화 활동을 활발하게 진행하고 있다.

3. IPTV 접근제어 서비스 기술

3.1 구현 형태에 따른 제한수신시스템의 유형

CAS 응용은 가입자 수신 단말에 위치해 제한수신용 키 관리 및 자격 제어를 담당하는 기능 모듈을 의미하며 크게 6가지로 구분한다.

첫번째 CAS 응용 구현 유형은 일반 OS에 클라이언트 형태로 CAS 응용을 구현하는 것으로, 이 방식에서는 키 관리와 자격관리 프로그램을 단순히 일반적인 형태의 마이크로프로세서에 탑재한다. 하지만, 이 방식은 역엔지니어링 공격에 매우 취약하다.

두번째 유형은 보안이 강화된 소프트웨어 형태로 CAS 응용을 구현하는 것으로써, 이때 CAS 응용은 프로그램 내 키 관리와 자격관리 부분이 해커에 의해 역엔지니어링 공격을 당하는 것을 방지하기 위한 보안 메커니즘을 포함하게 된다. 또한, 이 방식은 양방향 네트워크를 통해 CAS 응용에 대한 인증을 실시함으로써 응용 복제(cloning)와 같은 공격을 막을 수 있다.

세번째 유형은 셋톱박스 내 SoC칩에 CAS 응용을 구현하는 것으로, 셋톱박스에서 사용되는 일반적인 SoC를 디자인할 때 부가적으로 키 관리와 자격관리 기능을 추가하여 구현하게 된다. 칩 자체는 스마트카드에서 사용된 칩 수준의 보안을 제공하지는 않지만, 소프트웨어만으로 구현된 것보다는 안전하다.

네번째 유형은 셋톱박스에 내장된 형태의 소프트웨어와 독립된 모듈인 스마트카드를 함께 사용해 CAS 응용을 구현하는 것으로, 이 유형에서 소프트웨어는 스마트카드가 생성한 CW(Code Word)를 보호하고 스마트카드로 향하는 메시지 흐름을 제어하는 역할을 수행한다. 하지만, 셋톱박스 내 소프트웨어는 해커에 의한 역엔지

니어링 공격에 취약하기 때문에 제어단어를 안전하게 보호할 수는 없다.

다섯번 째 유형은 셋톱박스에 내장된 보안 칩과 스마트카드를 함께 사용해 CA 응용을 구현하는 것으로, 셋톱박스에 내장된 보안 칩은 스마트카드와 셋톱박스 사이에 보안 채널을 형성한다. 그리고, 스마트카드는 암호화된 제어단어를 셋톱박스로 출력하고, 셋톱박스는 내장된 보안 칩을 사용해 암호화된 제어 단어를 복호화 한다. 이 방식에서는 키나 자격정보와 같이 매우 중요한 정보가 스마트카드에 저장되기 때문에 셋톱박스 내 보안칩의 보안수준은 높지 않아도 된다.

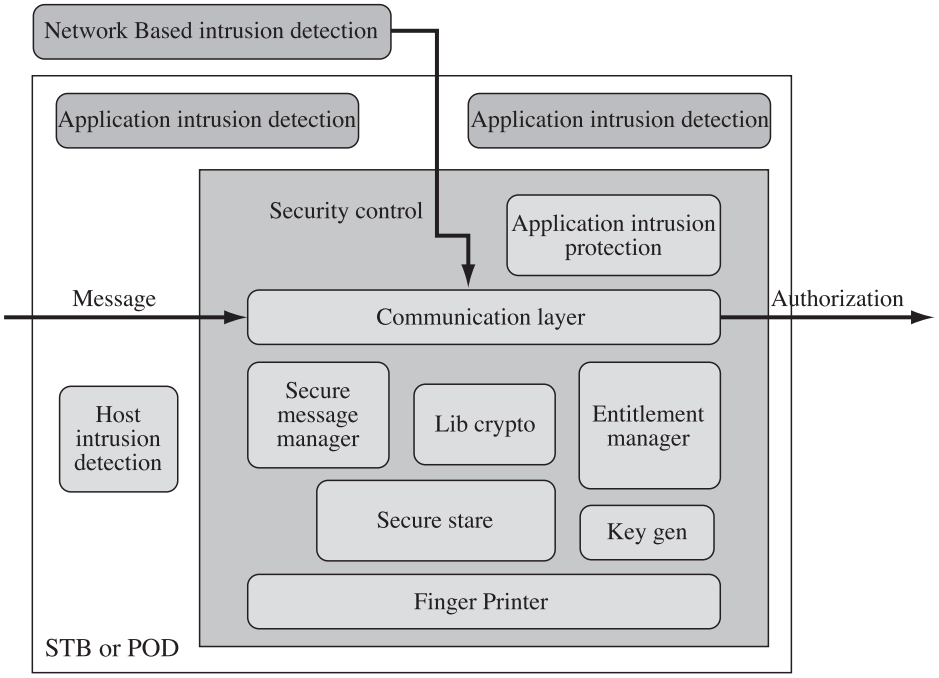
마지막으로, 셋톱박스에 보안 칩만을 내장해 CAS 응용을 구현하는 것으로, 이 유형에서는 셋톱박스 마더보드에 보안칩을 내장한다. 칩이 키나 자격정보와 같이 중요한 정보를 저장해야 하기 때문에, 다섯번 째 유형에 사용된 보안 칩보다는 높은 레벨의 물리적 보안이 요구된다. 하지만, 이 유형은 단방향 네트워크 상에서 보안의 결합으로 인해 키 관리 및 자격관리 알고리듬 갱신이 요구될 때 셋톱박스 자체를 교환해야 한다. 따라서, 스마트카드를 사용한 방식보다 유연한 운용을 할 수 없다.

3.2 소프트웨어 기반 제한수신시스템

제한수신시스템의 유형은 스마트카드를 배제한 소프트웨어 기반의 제한수신시스템이다. 소프트웨어 기반의 제한수신시스템이 관심을 끄는 첫번째 이유는 스마트카드 또는 OpenCable의 Cable CARD 등과 같은 하드웨어 기반의 제한수신 모듈을 사용했을 경우 모듈에 대한 발급 및 갱신 비용이 방송사업자들에게 큰 부담으로 작용한다는 것이다.

특히, OpenCable 방식에서 요구하는 PCMCIA 형태의 Cable CARD는 스마트카드보다 많은 운영 비용을 요구한다. 두번째 이유는 예전의 단방향 방송 네트워크가 양방향 네트워크로 변하는 점을 들 수 있다. 단방향 네트워크에서의 제한수신시스템은 사용자와 동일시 되는 스마트카드 또는 Cable CARD가 없으면 실체 인증이 불가능하였다.

하지만, IPTV와 같이 양방향 방송이 점차 가시화 되고 있는 현재는 스마트카드와 같은 하드웨어를 통한 실체인증이 반드시 필요하지 않게 되었다. 이러한 이유들



[그림 2] 소프트웨어 기반 제한수신시스템(Cyber VSC 구성 모듈)

때문에 양방향 네트워크 상에서 소프트웨어 기반 제한수신시스템이 시장에 소개되고 있는 것이다. 특히, 소프트웨어 기반 제한수신시스템은 200,000~300,000명의 가입자 수를 갖는 소규모 네트워크에서는 매우 유리한 위치를 차지할 것으로 예상되고 있다. [그림 2]에서 보듯이, 소프트웨어 기반의 제한수신시스템이 운용비용 절감이라는 측면에서 큰 매력을 가지고 있지만, 보안 측면에서는 아직까지 하드웨어 기반의 제한수신시스템이 우세하다. 왜냐하면, 단순히 플래쉬 메모리에 CAS 응용 코드를 저장하는 소프트웨어 방식은 보안 칩을 사용한 스마트카드 보다 역엔지니어링과 같은 물리적 공격에 매우 취약하기 때문이다.

하지만, 소프트웨어 기반의 제한수신시스템을 주장하는 측은 소프트웨어 기반의 제한수신시스템 솔루션이 하드웨어 기반의 제한수신시스템보다 훨씬 빠르게 CA 응용을 갱신할 수 있기 때문에 보안적인 측면에서 문제될 것이 없다고 말한다. 왜냐하면, 제한수신시스템에 치명적 보안 결함이 발생했을 때 소프트웨어 기반의 제한수신시스템은 단순히 새로운 CA 응용을 다운로드하면 되기 때문이다.

3.3 상호 운용 접근제어 시스템

DVB(Digital Video Broadcasting)에서 IPTV에 대한 표준화는 DVB-IP(CM-IPTV, TM-IPI)와 TM-TAM Module의 MHP-IPTV Workin Group에서 주도하고 있으며, 단계1과 단계2로 나뉘어서 진행되고 있다.

대표적인 디지털방송 표준화 단체 DVB에서 서로 다른 접근제어 시스템들이 시장에서 공존하며 자유롭게 경쟁할 수 있는 상호운용성 있는 접근제어 시스템을 위해 제안한 두 가지 시나리오 Simulcrypt와 Multicrypt가 있으며, 미국 케이블 산업에 대한 기술적 연구를 계획하고 자금을 지원하는 케이블랩스에서 추진중인 오픈케이블(Open Cable) 표준에서 제안한 교체가능한 하드웨어 장치인 케이블카드를 이용한 접근제어 시스템 기술이 있다.

3.3.1 DVB의 Simulcrypt

DVB에서는 1993년 이래로 디지털방송을 위한 접근제어 기술의 표준화 활동을 진행하고 있다. DVB 프로젝트에서는 DVB 시스템에서 접근제어 요소들에 지적재산권이 있을 수 있음을 받아들이면서도, 시장에서 여러 다른 접근제어 시스템들이 공존하며 사용될 수 있어야 한다는 데 초점을 두었다. 이를 위해서 헤드엔드에서 콘텐츠를 하나의 동일한 알고리듬으로 스크램블링 하되, 접근제어와 관련된 자격관리 메시지와 자격제어 메시지는 접근제어 시스템별로 각자의 방법으로 페이로드를 채워 전송할 수 있도록 하였다. 이것이 DVB Simulcrypt[6]의 기본 개념으로, 이를 실현하기 위해서 공통된 스크램블링 알고리듬인 CSA(Common Security Algorithm)[7]를 제안하였다.

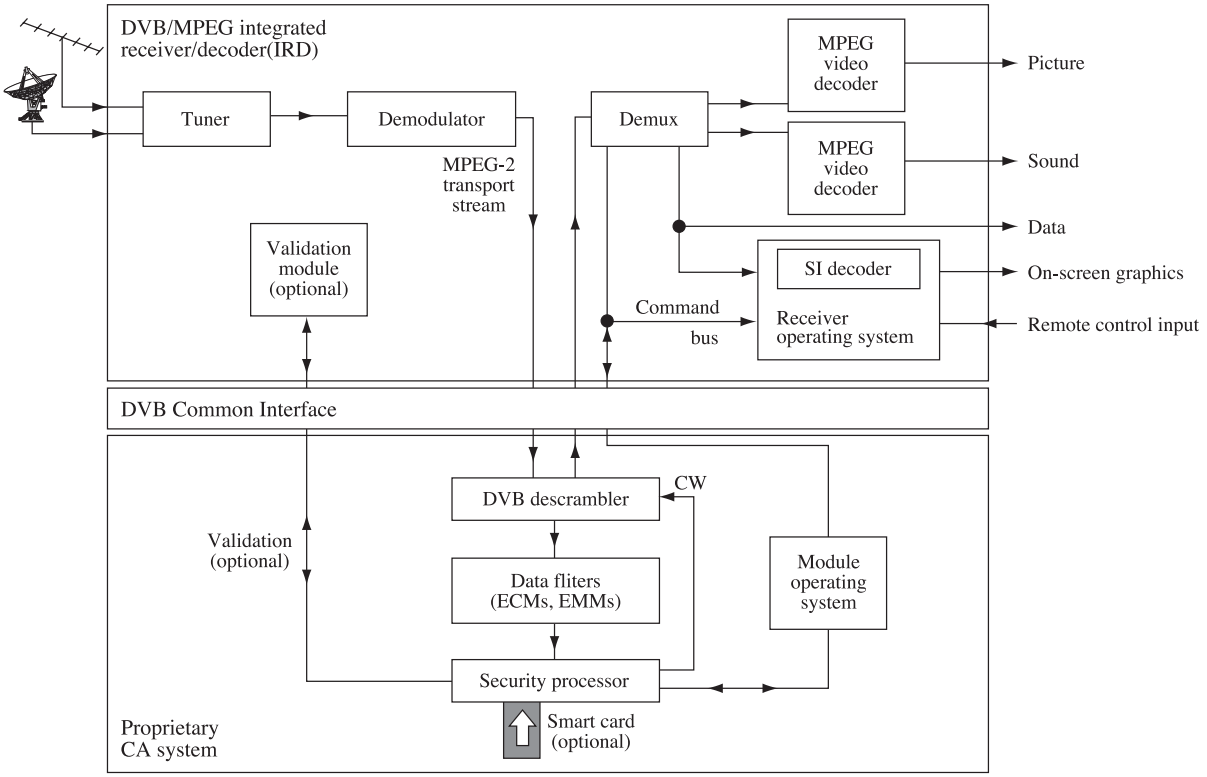
최근 Simulcrypt 스펙은 Simulcrypt 그룹의 활동으로 2개의 ETSI 표준 문서[8], [9]로 정리되고, 2001년 1월에 결성된 SimExt 그룹에서 이전 스펙을 보완하여 다시 2개의 ETSI 표준 문서[10], [11]로 추가 정리했으며, 서로 다른 접근제어 시스템의 공존을 고려한 Simulcrypt는 ATSC의 접근제어 시스템[12]에서 스크램블링 알고리듬을 제외하고 그대로 채택되고 있으며, 다만 스크램블링 알고리듬만 ATSC에서 제안한 ATSC CSA를 사용하도록 하고 있다.

3.3.2 DVB의 Multicrypt

상호운용성을 위해 제안된 또 다른 시나리오는 하나의 수신기에서 하나 이상의 접근제어 시스템을 수용하도록 규정한 Multicrypt으로써, 1997년에 수신기에서 접근제어 모듈을 분리하기 위해, 지적재산권을 가진 접근제어 모듈과 호스트 사이에 위치한 입출력 인터페이스인 CI(common Interface)[13]를 제안하였다.

Multicrypt에서 스마트카드의 사용여부는 선택적이며, DVB CI를 사용하는 수신기의 구조는 [그림 3]과 같다].

접근제어 모듈은 사용자 개인 정보인 가입자 비밀키와 자격제어 메시지 및 자격관리 메시지 처리부, 제어단어를 추출하기까지의 단계적인 키 복호화 처리부, DVB 디스크램블러로 구성된다. 이 부분은 각 접근제어 시스템 업체별로 자사의 지적재산권에 있는 구성 요소



[그림 3] DVB Common Interface를 포함하는 수신기 구조도

로 만들도록 하되 DVB CI를 따르는 경우 특정 제품에 상관없이 연동이 용이하다.

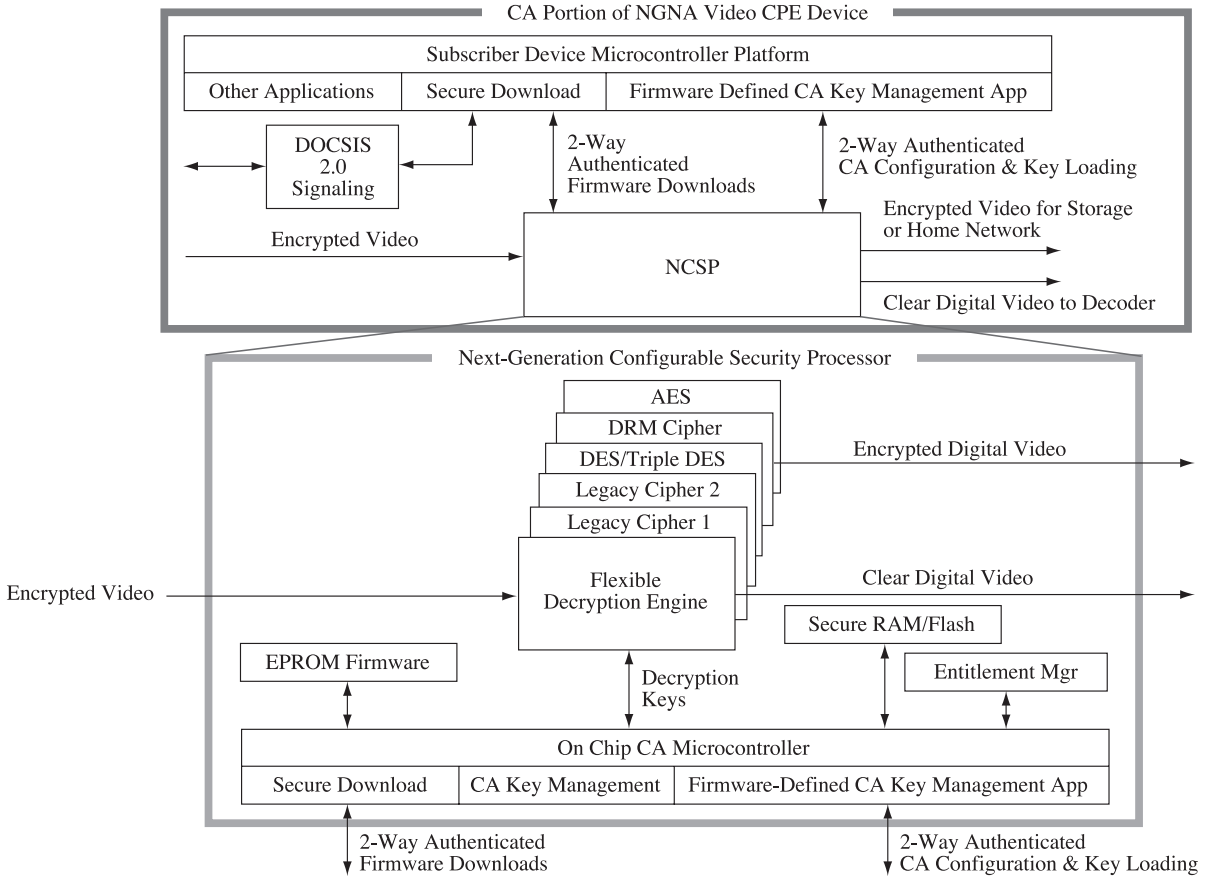
3.3.3 오픈케이블의 케이블카드

미국에서는 1996년 12월, 방송통신융합법인 텔레콤 액트(Telecom Act)를 통과시켜 접근제어 모듈이 분리된 셋톱박스를 규정하고, 1998년 9월 셋톱박스와 접근제어 모듈의 분리를 명시하였다. 2005년 1월, 셋톱박스와 접근제어 모듈간의 분리를 의무화 하였으나 케이블 TV 방송사와 연방통신위원회간의 대립으로 분리 의무 시점을 2006년 7월로 연기하고, 다시 2007년 7월 이후로 연기하였다. 케이블카드의 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.

3.4 다운로드가 가능한 접근제어 시스템

케이블카드와 같은 하드웨어 기반의 접근제어 시스템의 한계를 극복하고자 새롭게 제시되고 있는 것이 소프트웨어 다운로딩 방식의 접근제어 시스템이다. 현재 디지털 가입자망(DSL)을 이용한 IP망이나 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 교환 관련 필요한 데이터를 업로드 및 다운로드 하는 소프트웨어 다운로딩 방식의 접근제어 기술이 대두되고 있다.

미국에서는 디지털케이블망에서 접근제어 시스템을



[그림 4] NGNA 보안 참조 모델

다운로드 하는 DCAS(Download Conditional Access System)가 등장하였다. 미국 복수 유선사업자들은 연방통신위원회가 규정하고 있는 분리 의무화를 케이블카드를 교체하는 셋톱박스 뿐만 아니라 소프트웨어 다운로딩 방식의 DCAS까지 포함하도록 요구하고 있다. 미국 3대 복수 유선 사업자인 컴캐스트, 콕스 커뮤티케이션 그리고 타임워너 케이블이 주축이 되어 현재 케이블 TV망인 광동축 혼합망(HFC) 인프라에 추가적인 비용투자 없이, 제품혁신과 가격절감을 유도하는 통합 멀티미디어 구조의 구현을 목표로 하는 NGNA(Next Generation Network Architecture) 프로젝트[14]에서 새롭게 제안하고 있는 소프트웨어 다운로딩 방식을 도입한 NGNA 보안 모델이 있다. [그림 4]에서와 같이, NGNA 보안 참조 모델은 복수 유선사업자가 지적재산권이 있는 접근제어 시스템뿐만 아니라 새로 표준화되는 접근제어 시스템을 사용할 수 있게 하여, 케이블 운영자를 위한 다수의 접근제어 모듈 중에서 선택 가능하도록 지원한다. 접근제어 기술의 선택은 헤드엔드 쪽의 영향을 받기 때문에 NCSP(NGNA Configurable Security processor)에 들어가 있는 접근제어 시스템은 하나의 접근제어 모듈에서 다른 접근제어 모듈로의 전환이 가능해야 한다. 그리고, 케이블카드 인터페이스를 가지는 가입자 장치는 케이블카드가 인스톨되어 있지 않으면 NCSP가 디폴트가 된다. 특히 기존 디지털방송의 보안 모델과 뚜렷한 차이점은 하드웨어 기반 시스템을 원격으로 재구성할 수 있고, 소프트웨어 기반 시스템도 다운로드에 의해 접근제어 시스템의 일부를 업데이트 할 수 있다는 점이다.

4. 결론

본 고에서는 IPTV 표준 및 여러 접근제어 시스템간의 서비스 기술에 대하여 기술하였다. 현재 새로운 이슈가 되고 있는 IP망에서의 IPTV 서비스에서의 접근제어 시스템에 대한 표준화 활동이 ITU-T 등에서 활발히 진행 중이다. 또한 케이블 망의 디지털화 및 양방향화가 DCAS를 도입시켰듯이 IP망에서는 IP망의 고유한 특성 및 망 내의 보안시스템을 활용하여 하드웨어 의존도를 최소화시키고, 업데이트가 용이한 소프트웨어 다운로딩을 활성화한 접근제어 표준의 등장이 예상된다.

처음에 임베디드 시스템 형식으로 셋톱박스에 내장되었던 접근제어 시스템은 DVB의 Simulcrypt를 통해 헤드엔드에서의 상호운용성 개념을 도입하고, DVB의 CI를 통해 수신기에서 호스트와 접근제어 모듈을 분리하여 DVB CI를 따라 설계한 셋톱박스에는 CI를 따르는 어느 접근제어 시스템도 쉽게 연동될 수 있게 해주었다. 그리고 케이블TV에서는 케이블카드를 도입하여 가입자가 케이블TV 방송사를 변경할 경우 케이블 셋톱박스를 바꾸는 것이 아니라 케이블카드만 교체하면 되도록 하였다. 그러나 교체가능한 스마트카드 기반의 접근제어 시스템이 하드웨어적으로 문제가 많은 것으로 밝혀졌고, 방송망이 디지털화되고 양방향화된 현상황에서 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 접근제어 시스템이 하드웨어를 배제한다는 것은 아니다. 오히려 기존의 하드웨어와 소프트웨어를 동시에 사용하여 하드웨어의 안정성과 소프트웨어의 업데이트 용이성이라는 장점을 모두 살리도록 하고 있다. 현재 순수 소프트웨어 기반 접근제어 시스템 제품이 등장하고 있으나, 전통적 접근제어 시스템에서 하드웨어 장치의 보안에 대한 신뢰가 커서, 소프트웨어만을 사용한 접근제어 시스템의 표준화는 논의되지 않고 있는 상황이다.

[참고문헌]

[1] 권호영, 'IPTV의 동향과 전략,' 커뮤니케이션북스, 2004. p.24.

[2] 권호영, 'IPTV의 동향과 전략,' 커뮤니케이션북스, 2004. p.19.

[3] http://www.dvb.org

[4] http://www.etsi.org

[5] http://www.atsc.org/

[6] ETSI TS 103 197 v1.4.1, Digital Video Broadcasting(DVB) Head-end implementation of DVB Simulcrypt, Dec. 2004.

[7] ETSI Technical Report 289: Support for use of scrambling and Conditional Access within digital broadcasting system, 1996.

[8] ETSI TS 101 197 V1.2.1, DVB Simulcrypt; Part 1: Head-end architecture and synchronization, 2002.

[9] ETSI TS 103 197 V1.2.1, Head-end Implementation of Simulcrypt, 2002.

[10] ETSI TR 102 035 V1.1.1, Implementation Guidelines of the DVB Simulcrypt Standard, Apr. 2002.

[11] 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.

[12] ATSC Standard, Conditional Access System for Terrestrial Broadcast, Revision A, 2004.

[13] Common Interface Specification for Conditional Access and other digital video broadcasting applications, EN50221, 1997.

[14] NGNA LLC, "NGNA Plan: Integrated Multimedia Architecture," 26 July 2004.

TTA