Downloadable 제한수신 기술

정영호* 권오형**

방송의 디지털화가 가속화 되면서 디지털 콘텐츠에 대한 접근과 보호에 대한 중요성이 증대되고 있으며, 특히 케이블 및 IPTV 와 같은 유료 방송 서비스를 제공하는 매체의 경우 제한수신시스템의 효과적 운용 여부에 따라 사업의 성패가 좌우될 것이다. 이러한 상황에서 기존 임베디드 CAS 및 CableCARD 에서 나타난 여러 가지 문제점들을 해결함은 물론 방송 사업자, 제조업체, 가입자의 새로운 요구 사항들을 수용할 수 있는 다운로더블(Downloadable) 제한수신 기술에 대한 연구가 최근 국내외에서 활발히 진행되고 있다. 본 고에서는 케이블 매체를 기반으로 개발중인 다운로더블 제한수신 기술에 대하여 소개하고, 이와 관련한 국내외 기술개발 동향 및 ITU-T 에서의 표준화 동향에 대하여 기술하고자 한다. ▨

목 차

* ETRI 디지털 CATV 시스템연구팀/책임연구원
** ETRI 디지털 CATV 시스템연구팀/팀장

Ⅰ. 서 론

유료 콘텐츠에 대한 시청자의 접근 제어를 위한 제한수신시스템(Conditional Access System: CAS)은[1] 초기 임베디드 CAS 형태로 제공되었으며, CAS 모듈이 STB 내에 내장되어 있는 관계로 보안에 대한 심각한 결함이 발견되거나 CAS 솔루션이 변경되면 STB 를 전면 교체해야만 하는 문제점이 있었다. 이에 따라 STB 가 특정 CAS 솔루션에 lock-in 되는 현상을 방지하고 CAS 모듈만의 교체가 가능한 대안 기술에 대한 개발 필요성이 대두되었다.

이를 위해 개발된 OpenCable 규격은 STB 에서 CAS 모듈을 분리할 수 있도록 관련 인터페이스를 규정하고 있으며[2],[3], STB 에서 분리된 CAS 모듈은 PCMCIA 카드 타입의 CableCARD 로 명명되었다. 방송 사업자는 STB 와 분리된 CableCARD 만

을 가입자에게 전달함으로써 유료방송 서비스 제공이 가능하게 되었다. 그러나 실제 서비스 운영 과정에서 CableCARD 의 발열로 인한 STB 의 오작동, CableCARD 추가에 따른 STB 가격의 상승 및 관리 비용의 증가, 그리고 수신기 소매 시장의 비활성화로 인해 예상했던 수준의 효과는 얻지 못하였다.

이와 같은 문제점들을 해결하기 위해 북미 MSO 들을 중심으로 양방향 케이블 네트워크를 통해 CAS 소프트웨어를 안전하게 가입자 STB 에 다운로드시킬 수 있는 다운로더블 제한수신 시스템(Downloadable CAS: DCAS) 기술에 대한 논의가 시작되었다[4],[5]. 이는 STB 에서 CAS 모듈을 분리함으로써 기존 CableCARD 와 동일한 표준화의 이점을 갖는 동시에 네트워크를 통해 다운로드 가능하게 함으로써 방송 사업자가 특정 CAS 혹은 STB 제조업체에 대한 의존으로부터 완전히 탈피할 수 있도록 해준다. 또한 CAS 의 보안상 결함이 발생하거나 신규 서비스 제공을 위한 업그레이드가 필요한 경우 즉시 대처할 수 있는 유연성을 확보할 수 있다. 최근 들어 STB 에서의 분리형 보안 모듈 장착이 의무화 되고 홈네트워크 기기간 콘텐츠 공유에 따른 DRM(Digital Rights Management), ASD(Authorized Service Domain) 등과 같은 보안 솔루션을 효과적으로 제공하기 위해 케이블 및 IPTV 를 비롯한 유료 방송매체에서의 DCAS 기술에 대한 연구 개발이 활발히 추진되고 있다.

본 고에서는 국내외 케이블 방송 분야에서 주목 받고 있는 DCAS 기술에 대하여 소개하고자 한다. 먼저 II 장에서는 DCAS 시스템 요구사항 및 이를 만족하기 위한 헤드엔드와 STB 의 구조 및 기술 특징에 대해 살펴보고, III 장에서는 현재 진행중인 국내외 기술개발 동향에 대해 기술한다. IV 장에서는 ITU-T SG 9 에서의 표준화 동향에 대하여 설명하고, 마지막으로 V 장에서 결론을 맺도록 한다.

II Downloadable CAS 기술

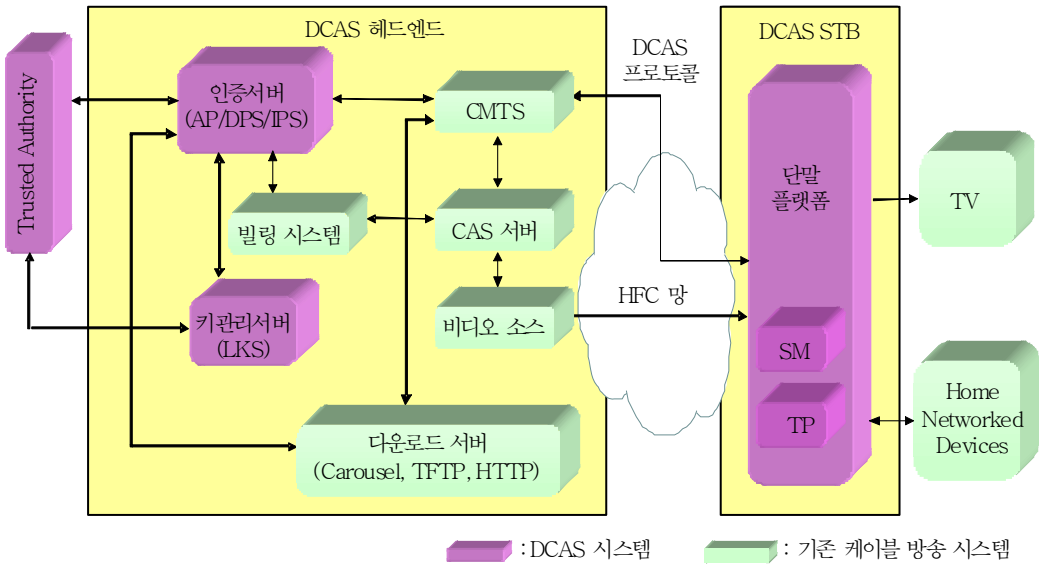
양방향 케이블 네트워크를 이용하여 제한수신 소프트웨어를 가입자 STB 에 안전하게 다운로드하기 위해 정의된 DCAS 시스템 요구사항은 다음과 같다.

먼저, DCAS 시스템은 제한수신 소프트웨어의 안전한 다운로드 및 사용되는 키에 대한 분배/검증, 그리고 안전한 키 갱신 방안을 제공해야 한다. 또한 콘텐츠 부호화 및 복호화를 위한 CAS/DRM/ASD 모듈의 키 관리를 지원해야 하며, STB 내 SM(Secure Micro)과 TP(Transport Processor) 간에 안전한 통신 채널을 확보해야 한다. DCAS 시스템은 동시에 다중 비디오 스트림에 대한 복호화 및 이에 대한 키 관리를 제공해야 하며, 가입자에게 신속한 서비스가 제공될 수

있도록 STB 의 초기 구동 조건을 설정해야 한다.

신뢰성과 확장 가능성 있는 DCAS 기반 구조를 위해 DCAS 헤드엔드는 네트워크에 접속하는 신규 STB 를 자동으로 감지해 낼 수 있음은 물론, 적절치 않은 제한수신 소프트웨어를 운용하는 SM 을 찾아낼 수 있어야 한다. AP 와 SM 간의 상호 인증을 기반으로 제한수신 소프트웨어의 다운로드를 진행해야 하며, STB 의 네트워크 간 이동을 감지하고 이전 네트워크에서의 가입자 관련 정보를 제거할 수 있어야 한다. DCAS 관련 보안 프로토콜은 향후 확장성을 고려하여 설계되어야 하며, DCAS 메시지들은 다른 전송 계층 프로토콜 내에 쉽게 포함되어 전송될 수 있어야 한다.

DCAS 시스템은 (그림 1)과 같이 기존 케이블 방송 시스템과 연동하며 운용되는 구조를 갖는다. 케이블 방송 사업자 도메인에 위치하지 않는 제 3 의 신뢰기관인 TA(Trusted Authority)는 인증 서버와 STB 내 SM 간의 상호 인증 및 암호화 키 공유에 도움을 준다. DCAS 헤드엔드는 AP (Authentication Proxy), DPS(DCAS Provisioning System) 및 IPS(Integrated Personalization Server)를 포함하는 인증 서버와 LKS(Local Key Server)인 키 관리 서버로 구성된다. 인증 서버는 빌링 시스템으로 STB 에 저장된 가입자의 구매 관련 정보를 전송할 수 있으며, 또한 제한수신 소프트웨어의 다운로드를 처리하기 위한 별도의 다운로드 서버를 구성할 수 있다. DCAS STB 는 제한수신 소프트웨어의 안전한 구동 및 해킹으로부터의 보호 기능을 수행하는 SM 과 스크램블된 방송 스트림의 디스크램블링 및 홈네트워크 디바이스로의 콘텐츠 전송 시 암호화를



(그림 1) DCAS 시스템 구조

수행하는 TP 를 포함한다.

1. DCAS 헤드엔드

DCAS 헤드엔드를 구성하는 인증 서버 및 키 관리 서버의 주요 기능은 다음과 같다.

- 복수의 제한수신 소프트웨어의 안전한 다운로드
- SM 에 대한 개별화된 제한수신 소프트웨어 전송
- SM 에 기록된 과금에 필요한 구매 정보 획득 및 관리
- 다운로드를 포함한 서비스 정책 정보 배포 및 관리
- 제한수신 소프트웨어의 SM 내 다운로드 상태 관리
- 높은 보안성 및 효율성을 지닌 DCAS 프로토콜 운용 및 세션 관리
- DCAS 네트워크 운용 관련 키에 대한 이력 관리

AP 는 DSG(DOCSIS Set-top Gateway) 채널 내 CA 터널을 통해 DCAS 프로토콜을 기반으로 SM 과의 상호 인증을 수행하며, 인증이 완료된 SM 관련 정보는 DCAS 서비스 정책을 관리하는 DPS 로 전송한다. 이때 적용되는 DCAS 프로토콜은 AP 와 SM 간 상호 인증 및 암호화 키 공유, 그리고 암호화된 제한수신 소프트웨어의 다운로드를 위한 DCAS 메시지 및 일련의 처리 절차를 규정한다. SM 과의 상호 인증 및 암호화 키 공유에 필요한 정보는 신뢰기관인 TA 로부터 수신하고, 이를 이용하여 생성된 암호화 키는 다운로드될 제한수신 소프트웨어의 암호화를 수행하는 IPS 에게 전달한다.

DPS 는 DCAS 서비스 운용 및 관리에 필요한 정책 정보를 각 서버들에게 전달함으로써 효율적인 네트워크 운용을 보장하며, SM 으로부터 전송받은 IPPV(Impulse Pay-Per-View) 관련 콘텐츠 구매 정보를 빌링 시스템으로 전송하여 가입자에 대한 과금 정보로 활용한다. 앞서 언급한 AP 로부터 전달받은 인증된 SM 관련 정보를 이용하여 케이블 네트워크에 접속한 복제 SM 을 검출하거나 SM 의 적절치 못한 제한수신 소프트웨어의 운용을 감지하여 이를 개선하는데 활용한다. 또한 가입자의 이사 등에 의한 STB 의 AP 네트워크 이동을 효과적으로 감지하여 이전 AP 네트워크에서 전송되는 CAS 관련 정보 전송을 중단함으로써 네트워크 이용 효율을 높일 수 있다.

IPS 는 AP 로부터 수신한 암호화 키를 이용하여 다운로드될 제한수신 소프트웨어를 암호화하고 DPS 로부터 지시받은 전송 메커니즘(Carousel, TFTP, HTTP 등)에 따라 다운로드 절차를 진행한다. 모든 SM 에 공통적으로 적용될 수 있는 다운로드 객체에 대해서는 캐루셀(Carousel)

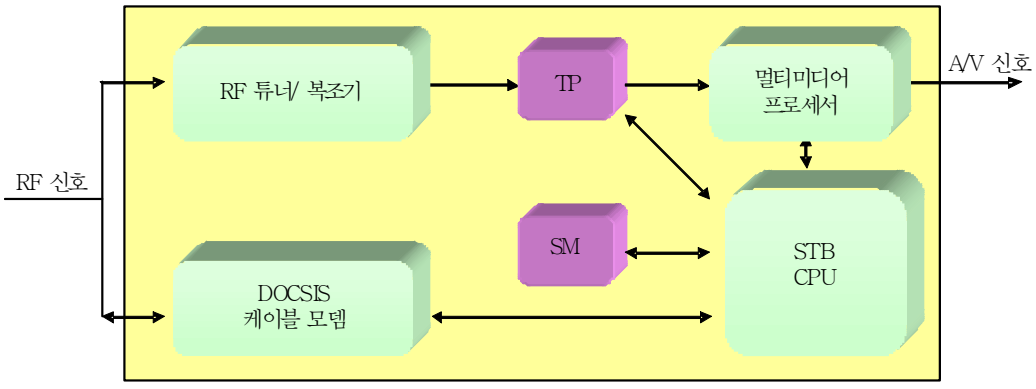
형태의 전송 메커니즘이 효과적이다. 만일 전송 메커니즘이 TFTP 로 선택되었다면, IPS 는 TFTP 서버에 암호화된 제한수신 소프트웨어를 업로드하고 관련 다운로드에 필요한 정보 즉, 서버 IP 주소, 접속 포트 번호, 다운로드 객체명 등을 AP 를 통해 SM 으로 전송한다.

LKS 는 DCAS 시스템에서 운용되는 모든 키 및 ID 관련 정보, 생성된 암호화 키 등을 DB 에 저장하고 이에 대한 이력 관리를 수행한다. 또한 재난 상황이 발생하여 다른 서버의 키 및 ID 등의 키 관련 정보가 손실되었을 경우 이에 대한 복구를 도와 준다. 케이블 방송 사업자의 운용 방법에 따라 신뢰기관인 TA 에서 수행되는 SM/TP 유효성 검증 및 SM 과 AP 간 암호화 키 공유를 위한 시드(seed)값 제공 등의 기능을 수행할 수도 있다.

2. DCAS STB

(그림 2)와 같이 DCAS STB 는 기존 OpenCable 방식의 STB 와는 달리 다운로드된 제한수신 소프트웨어의 안전한 저장 및 운용에 필요한 SM 과 다수의 디스크램블러 엔진을 포함하는 TP 를 새롭게 내장하고 있으며, 그 외에 STB CPU, DOCSIS 케이블 모뎀, RF 튜너/복조기, 멀티미디어 프로세서 등으로 구성된다.

SM 은 DCAS 프로토콜을 기반으로 상호 인증을 통해 DCAS 헤드엔드 서버와 안전한 통신 채널을 형성하고 이를 통해 다운로드 받은 제한수신 소프트웨어를 안전하게 저장하고 구동할 수 있는 환경을 제공해 준다. 이를 위해 SM 은 DCAS 헤드엔드 서버와의 상호 인증 및 암호화 키 공유 처리 등을 위한 암호화 알고리즘을 지원한다. 또한 SM 내 운용중인 부트로더 및 제한수신 소프트웨어를 외부의 물리적 해킹으로부터 보호하기 위한 여러 가지 보안 기능들을 포함한다 [6].



(그림 2) DCAS STB 구조

TP 는 수신된 방송 신호의 스크램블링 여부와 가입자의 시청권한에 따라 해당 신호를 디스크램블링 하는 기능을 담당하며, 여러 CAS 사업자의 제한수신 시스템을 지원할 수 있도록 복수의 디스크램블링 알고리즘을 내장하고 있다. TP 는 SM 에서 운용되는 제한수신 소프트웨어로부터 수신한 제어 단어(Control Word: CW)를 이용하여 디스크램블링을 수행하며, DCAS STB 에 연결된 홈네트워크 디바이스로 전송되는 콘텐츠에 대한 보호를 위해 암호화 알고리즘도 포함하고 있다.

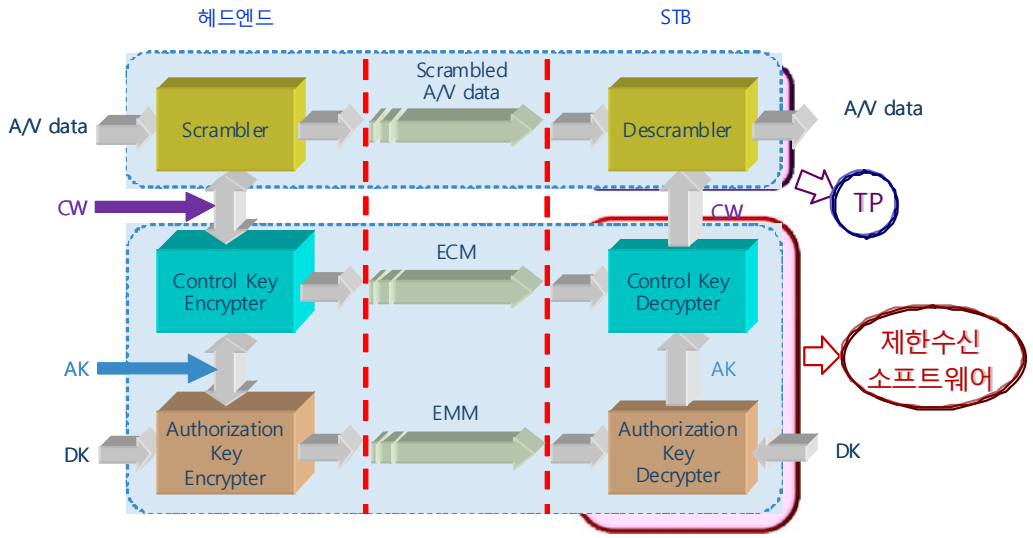
DCAS STB 의 동작 과정을 살펴보면, 먼저 SM 은 DCAS 헤드엔드 서버로부터 주기적으로 전송되는 제한수신 소프트웨어에 대한 버전 관련 정보와 SM 에 저장되어 있는 정보를 비교하여 제한수신 소프트웨어의 다운로드 여부를 결정한다. 만일 다운로드가 필요하다면, DCAS STB 는 DOCSIS 모뎀을 이용한 양방향 통신 채널을 통해 DCAS 프로토콜을 기반으로 상호 인증 및 암호화 키 공유 과정을 수행하여 제한수신 소프트웨어를 안전하게 다운로드하고, 이후 DCAS STB 에 전원이 인가될 때마다 제한수신 소프트웨어를 SM 내 메모리에 로딩하여 구동한다. 케이블 네트워크를 통해 수신된 방송 신호는 RF 튜너 및 복조기를 통해 베이스밴드 신호 변환 및 복조 과정을 거쳐 스크램블링된 A/V 데이터로 변환되고, TP 에서는 적절한 디스크램블링 엔진을 이용하여 이를 MPEG-2 TS 신호로 변환하여 출력한다. 이때 디스크램블링에 필요한 CW 및 암호화 알고리즘 정보는 SM 에서 실행중인 제한수신 소프트웨어로부터 STB CPU 를 통해 전달받는다. 멀티미디어 프로세서는 수신된 MPEG-2 TS 신호를 MPEG 디코더를 이용하여 A/V 신호로 변환하여 출력한다.

3. CAS 와 DCAS 구성요소 비교

(그림 3)과 같이 일반적인 헤드엔드 및 STB 에서의 CAS 처리 과정은 3 단계로 구성된다[1].

헤드엔드에서는 첫째, CW 를 이용하여 A/V 데이터를 스크램블링하는 단계, 둘째, 스크램블링에 사용되는 CW 를 인증키(Authorization Key: AK)로 암호화하고 이를 자격 제어 메시지(Entitlement Control Message: ECM)에 포함하여 전송하는 단계, 마지막으로 인증키를 분배키(DK: Distribution Key)로 이용하여 암호화하고 이를 자격 관리 메시지(Entitlement Management Message: EMM)에 포함하여 전송하는 단계로 구성된다.

STB 에서는 헤드엔드에서의 역 처리 과정을 통해 먼저 수신된 EMM 메시지를 헤드엔드와 동일한 DK 로 복호화하여 AK 를 추출하고, 추출된 AK 로 수신된 ECM 메시지를 복호화하여 CW 를 획득한다. 획득된 CW 를 이용하여 수신된 스크램블링된 A/V 데이터를 디스크램블링하여 원래의 A/V 데이터를 얻는다.



(그림 3) CAS 와 DCAS 구성 요소 비교

CableCARD 의 경우, 앞서 설명한 수신기에서의 CAS 처리 기능인 EMM/ECM 파싱을 통한 CW 추출 및 디스크램블링을 모두 포함하고 있다. 그러나 DCAS 에서는 EMM 과 ECM 파싱을 통해 각각 AK 및 CW 키를 추출하는 기능은 제한수신 소프트웨어에 포함되어 STB 내 SM 에서 처리되며, SM 으로부터 전달받은 CW 를 이용하여 스크램블된 A/V 데이터를 디스크램블링하는 기능은 TP 에서 처리된다.

III 국내외 기술개발 동향

1. 국내

2000 년대 중반 이후로 DCAS 기술에 대한 관심이 고조되면서 ETRI 를 주관 연구기관으로 하여 코어 트러스트, DST, 코아 크로스 등이 공동 참여한 'Downloadable 제한수신 시스템 개발' 과제가 시작되었으며, 이를 계기로 국내에서의 DCAS 기술 개발이 본격화 되었다. ETRI 와 더불어 LG CNS 및 Alticast 도 각각 개발 컨소시엄을 구성함으로써 상호 경쟁 및 협력을 통한 DCAS 기술 개발을 촉진하였다. 현재 DCAS STB 내 실장되는 SM 이외에도 STB 의 메인 프로세서를 이용하는 소프트웨어 기반 SM 과 스마트 카드 타입의 SM 등과 같은 다양한 형태의 DCAS 솔루션에 대한 개발이 진행중에 있다.

국내에서는 처음으로 KCTA 2008 전시회를 통해 ETRI 를 비롯한 양 컨소시엄에서 개발중

인 DCAS 솔루션과 더불어 삼성전자, LG 전자 등이 개발한 DCAS STB 에 대한 시연이 진행되었으며, 그 이듬해 ETRI 는 대전에서 개최된 KCTA 2009 전시회에서 한층 기술적 완성도가 높아진 DCAS 솔루션을 전시하였다[7].

최근 케이블 방송 사업자인 C&M 은 DCAS 에 대한 BMT(Bench Mark Test)를 실시하여 DCAS/CAS/STB 분야별로 우선 협상 대상자를 선정하고, 연내 현장 시험을 통해 DCAS 상용화를 진행할 예정에 있다고 밝혔다[8]. 이와 더불어 2008 년 10 월부터 DCAS 표준 제정 실무위원회를 중심으로 DCAS 개발업체, 케이블 방송 사업자, CAS 벤더, STB 제조업체, 학계 등이 참여하여 DCAS 송수신 정합 표준 및 보안 프로토콜 등을 포함한 세부 기술 규격에 대한 표준화를 진행중에 있다.

2. 국외

NGNA 프로젝트를 통해 시작된 DCAS 기술 개발은 북미 MSO 인 Comcast, Time Warner Cable, Cox Communications 이 공동 투자하여 설립한 PolyCipher 를 중심으로 본격화 되었다. FCC 는 네비게이션 장치 법안(Navigation Device Rule)에 대한 2 년 간의 유예 조치를 거쳐 2007 년 7 월부터 보안 모듈 분리 의무화 조치를 시행함에 따라 DCAS 기술에 대한 관심은 매우 고조되었다[9],[10].

PolyCipher 는 EmbedIC 및 Envieta 등을 통해 관련 시스템 및 규격 개발을 진행하였으나, 북미 시장에서의 DCAS 도입에 대한 불확실성 등으로 인해 원하는 성과를 얻지 못했다[11], [12]. 결국 2009 년 6 월, PolyCipher 는 DCAS 프로젝트를 CableLabs 로 이관하고 문을 닫았으며, 북미 케이블 주요 장비업체인 Motorola 및 SA 를 인수한 Cisco 등이 신규 참여하여 DCAS 기술에 대한 개선 작업이 진행중에 있다[13]. 이와 더불어 2007 년 BBT(Beyond Broadband Technology LLC)는 저가형 DCAS STB 를, Widevine 사는 PolyCipher 와 다른 방식의 DCAS 솔루션을 개발했다고 발표하였다[14]. 현재까지 DCAS STB 관련 일부 규격만이 CableLabs 을 통해 CLP-SP(CableLabs Private-Specification) 형태로 유료로 제공되고 있으나, 주요 DCAS 관련 규격에 대한 초안 작업은 대부분 마무리되었을 것으로 보여진다.

IV ITU-T 표준화 동향

ITU-T 산하 SG 9 은 TV 와 오디오 프로그램 방송을 위한 통신 시스템과 양방향 비디오 서비스, 전화 및 데이터 서비스들을 제공하기 위한 인터넷을 포함한 케이블 네트워크와 관련된 분

야를 주로 다룬다. 최근 케이블 네트워크에서의 음성/데이터/비디오 IP 응용(IPCablecom), 양방향 케이블 TV 서비스, 고속 데이터 서비스 및 IP 기반 TV 내용 등을 다룬 J 시리즈 권고안이 제정되었으며, 또한 유니버설 통합 수신기 혹은 홈네트워킹을 위한 STB 의 역할을 하는 차세대 케이블 모뎀 분야의 권고안을 완료하였다.

WTSA-08 회의를 통해 결정된 2009 년부터 2012 년까지 SG 9 에서 검토되어야 할 Question 들은 <표 1>과 같다. 각 Question 별로 세부 내용을 설명한 관련 기고문에서 DCAS 관련 논의 필요성이나 이에 대한 세부 검토 내용을 확인할 수는 없었다[15]. 그러나 Q 3/9 에서는 CAS, DRM 및 ASD 관련 내용을 검토하며, 세부 논의 대상으로 이와 관련한 안전한 스크램블링 절차 및 암호화 알고리즘, 키 및 자격정보의 갱신주기, 가입자 그룹핑 및 관련 키에 대한 규격 등을 포함하고 있으므로 향후 Q 3/9 를 중심으로 DCAS 관련 표준화에 대한 논의가 이루어질 수 있을 것으로 보인다.

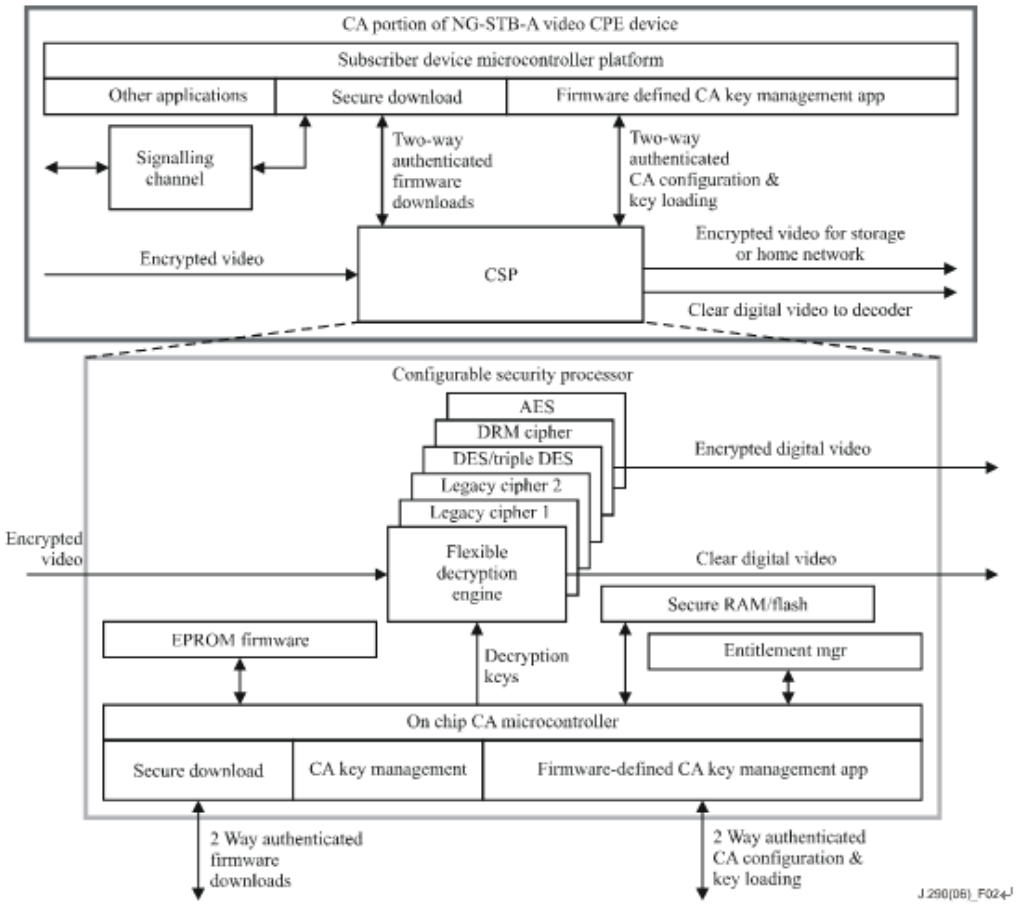
지난해 및 올해 상반기까지 ITU-T SG 9 에 제출된 기고문을 검토해 본 결과, DCAS 관련

<표 1> ITU-T SG 9 의 Question 목록

구분	Question Title
Q 1/9	Transmission of television and sound programme signal for contribution, primary distribution and secondary distribution
Q 2/9	Measurement and control of the Quality of Service(QoS) for television transmission on contribution and distribution networks
Q 3/9	Methods and practices for conditional access, protection against unauthorized copying and against unauthorized redistribution('redistribution control' for digital cable television distribution to the home)
Q 4/9	Application programming interfaces (API) for advanced content distribution services within the scope of Study Group 9
Q 5/9	Functional requirements for a universal integrated receiver or set-top box for the reception of advanced content distribution services
Q 6/9	Digital programme delivery controls for multiplexing, switching and insertion in compressed bit streams, possibly encapsulated in TS or IP packets
Q 8/9	Voice and video IP applications over cable television networks
Q 9/9	The extension of network-based content distribution services over broadband in Home Networks
Q 10/9	Requirements and methods to delivery sound and television programmes and other multimedia services over IP networks for advanced service platforms
Q 11/9	Transmission of multichannel analogue and/or digital television signals over optical access networks
Q 12/9	Objective and subjective methods for evaluating perceptual audiovisual quality in multimedia services within the terms of Study Group 9
Q 13/9	Transmission of Large Screen Digital Imagery programmes for contribution and distribution purposes

기고 내용은 없었으며 주로 IPCablecom 네트워크를 통한 통신 서비스, FTV(Free view point TV)를 위한 전송시스템 및 데이터 포맷, 양방향 서비스를 위한 전송 플랫폼의 기능적 요구사항, DCATV 를 위한 비디오 화질 측정 기법 등에 관한 기고문이 주류를 이루었다[16].

2006 년 11 월에 제정된 J.290 권고는 Q 5/9 에 해당하는 차세대 STB 의 핵심 구조 기능을 기술하고 있으며[17], STB 구조는 VoD, HDTV, Home 네트워크, 미래 IP 멀티미디어 서비스의 성장을 지원할 수 있는 유연성 및 성능을 가진 경제적인 플랫폼이 되도록 요구하고 있다. 이를 위해 차세대 STB 는 SM 과 TP 를 포함하는 CSP(Configurable Security Processor)를 통해 원격으로 다운로드되어 구성되거나 갱신될 수 있는 소프트웨어 기반의 CA 구현, 다수의 CA 지원, 그리고 보안 카드 장치의 사용을 통해 물리적 보안을 지원할 수 있는 것을 특징으로 정의하



<자료>: ITU-T Rec. J.290, "Next generation set-top box core architecture," Nov. 2006.

(그림 4) CSP 기능 구성도

고 있다. (그림 4)는 STB 내 CSP 의 기능 구성도를 보여주고 있으며, CSP 내 unique ID 를 private seed ID 로 하여 헤드엔드로부터 보안 명령에 따라 새로운 값으로 변환하고 이를 이용하여 새로운 암호화 키 값을 생성하는 과정을 private serialization 이라 명명하고 있다[17].

CSP 하드웨어 구성 요소는 다음 4 가지 방식의 TS 암호화/복호화를 지원하기 위한 기술들이 적용할 것으로 기술하고 있다.

- Triple-DES(Data Encryption Standard): ECB, CBC 모드 지원
- DVB-CSA(Common Scrambling Algorithm)
- AES(Advanced Encryption Standard)
- ARIB 에서 정의된 B-CAS

그 외에도 RSA 전자서명을 통한 인증, 키 암호화 키, unique ID, tamper resistance, 키 관리, 복제 보호에 대한 가이드 라인을 포함하고 있다.

2008 년 6 월에 제정된 J.293 권고는 RF 기반 및 IP 기반 네트워크를 통해 다양한 콘텐츠 분배 방식을 지원하기 위한 STB 의 3 개 카테고리를 정의하며, 권고 J.290, J.291, J.292 에서 정의된 STB 구성요소 및 인터페이스에 대해서도 규정하고 있다[17]-[20]. 보안 처리와 관련하여 제한수신 모듈은 아래의 과정을 포함하는 SAC(Security Authentication Channel) 형성을 지원하도록 요구하고 있으며, DCAS 와 같이 네트워크를 통해 보안 시스템의 갱신이 가능하도록 권고하고 있다[20].

☞ SAC 형성

- 서버 인증: STB 는 challenge/response 메커니즘으로 서버를 인증
- 단말 인증: 서버는 상기 인증에 대한 응답으로 challenge/response 메커니즘으로 STB 를 인증
- 세션키 생성: 인가된 세션키는 위의 인증 프로세스를 통해 STB 와 서버가 획득하며, SAC 을 통해 전달되는 메시지의 암호화를 위해 사용

앞서 살펴본 바와 같이 ITU-T SG 9 에서는 최근 DCAS 표준화와 관련된 논의는 진행되고 있지는 않으나, 기존 차세대 STB 관련 권고들에서 DCAS 를 수용하도록 하는 보안 관련 기능 요구사항을 규정하고 있음을 확인할 수 있었다. 향후 ITU-T SG 9 에서의 DCAS 표준화는 CAS/DRM 관련 주제를 포함하고 있는 Q 3/9 관련 미팅에서 논의될 수 있을 것으로 여겨지며, 기존 권고에서 규정하고 있는 DCAS 내용과의 harmonization 을 고려하여 표준화가 진행되어야 할 것으로 보인다.

V. 결 론

기존 CAS 솔루션이 지닌 여러 가지 문제점들을 해결하기 위해 제안된 DCAS 기술은 유료 서비스를 제공하고 있는 케이블 방송 매체를 비롯한 IPTV, 이동통신, DMB 등에서 적용될 수 있는 경제적 파급 효과가 매우 큰 기술 중 하나이다.

북미에서 시작된 DCAS 관련 기술 개발은 투여된 비용과 노력만큼의 큰 진척을 보이지 못하고, 이를 주도했던 PolyCipher 의 해체 및 CableLabs 으로의 관련 프로젝트 이관이라는 새로운 국면을 맞고 있다. 그러나 국내에서는 2010 년 말까지 보안 모듈 분리 의무화가 유예되었음에도 불구하고 기존 임베디드 CAS 솔루션으로 회귀하지 않고 케이블 방송 사업자, DCAS 솔루션 개발업체, STB 제조업체, CAS 벤더 등의 도전적이고 적극적인 관련 기술 개발 및 부단한 노력을 통해 금년 연말부터 일부 케이블 방송 사업자가 DCAS 시스템을 도입하여 운용할 예정에 있다.

2010 년부터 본격적인 DCAS 기술에 대한 상용화가 시작되면, 케이블 방송 사업자는 특정 CAS 솔루션 및 장비업체에 대한 lock-in 현상으로부터 벗어남은 물론 CableCARD 교체 및 관리에 사용되는 비용을 상당 부분 절감할 것으로 기대된다. 또한 STB 와 홈네트워크 기기간의 콘텐츠 공유에 따른 새로운 비즈니스 영역에 신속하고 효과적으로 대처할 수 있다. 장비업체는 CAS 종속성 제거에 따른 장비간 호환성을 확보할 수 있으며, 또한 기존 lock-in 된 CAS 관련 시장의 장벽을 없앰으로써 자사의 기술 및 가격 경쟁력을 기반으로 시장 점유율 확대를 꾀할 수 있는 장점이 있다. 가입자는 이사에 따른 번거로운 변경 처리 및 CAS 솔루션 교체로 인한 불편함을 해소할 수 있으며, 케이블 방송 사업간 호환성이 보장된 다양한 사양의 STB 를 선택할 수 있을 것으로 예상된다.

<참 고 문 헌>

[1] EBU Project Group B/CA, “Functional Model of a Conditional Access System,” EBU Technical Review, Winter 1995, pp.64-77.

[2] OpenCable Specification, CableCARD Interface 2.0 Specification, Cable Television Laboratories, Inc., Jan. 2008.

[3] OpenCable Specification, CableCARD Copy Protection 2.0 Specification, Cable Television Laboratories, Inc., June 2007.

[4] Tom Lookabaugh & James Fahrny, “Openness and secrecy in security systems: PolyCipher downloadable conditional access,” The Cable Show conference, May 2007.

[5] Gary Traver and James Capps, “The unique challenges faced by cable systems serving smaller

markets as they expand to meet conditional access and OCAP requirements," The Cable Show conference, May 2007.
[6] NIST FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001.
[7] http://www.etnews.co.kr/news/detail.html?id=200904090012
[8] http://www.etnews.co.kr/news/detail.html?id=200908260102
[9] Federal Communications Commission FCC 07-127, p.2.
[10] http://www.multichannel.com/article/CA6480827.html?q=Download+ Incomplete
[11] http://www.cedmagazine.com/Article-night-polycipher-shift.aspx
[12] Federal Communications Commission FCC 08-88, p.6.
[13] http://www.multichannel.com/article/294897-CableLabs_Takes_Over_DCAS_Project_From_Poly Cipher.php
[14] http://www.multichannel.com/article/130496-Download_Incomplete.php
[15] ITU-T WTSA-08, "Questions assigned to Study Group 9," Nov. 2008.
[16] ITU, http://www.itu.int/ITU-T/studygroups/com09/index.asp
[17] ITU-T Rec. J.290, "Next generation set-top box core architecture," Nov. 2006.
[18] ITU-T Rec. J.291, "Next generation set-top box cable architecture," Nov. 2006.
[19] ITU-T Rec. J.292, "Next generation set-top box media-independent architecture," Nov. 2006.
[20] ITU-T Rec. J.293, "Component definition and interface specification for the next generation set-top box," June 2008.

* 본 내용은 필자의 주관적인 의견이며 NIPA의 공식적인 입장이 아님을 밝힙니다.