특집

다운로더블 제한수신 시스템 기술

정 영 호, 정 준 영, 구 한 승, 조 용 성, 유 웅 식, 권 오 형(한국전자통신연구원)

Ⅰ. 서 론

유료방송의 불법시청을 막기 위한 제한수신 시스템(CAS; Conditional Access System)은 케이블방송 및 위성방송 등에 있어서 사업의 성패를 결정하는 매우 중요한 기술이다[1]. 케이블 방송에 도입된 초기 CAS는 임베디드 솔루션 형태로 구현되었기 때문에 방송 사업자가 가입자에게 단말을 직접 공급할 수 밖에 없었다. 또한 CAS갱신을 위해서는 가입자 단말을 교체해야 하는 상황이었으며, 이에 따른 사업자의 경제적 부담이 고스란히 소비자에게 전가될 수 밖에 없었다.

초기 CAS의 문제점을 해결하기 위해 단말과 제한수신 모듈을 분리하는 규격이 발표되었다[2-3]. 이를 통해 기존 단말의 사업자 대여 방식을 가입자가 직접 구매할 수 있는 소매 체제로 전환함으로써 특정 장비업체의 독과점 방지와 더불어 업체간 경쟁 유발을 통한 단말 가격 하락을 유도하고자 하였다. 그러나 단말에서 분리된 제한수신 모듈인 케이블카드 도입은 제작원가 상승과 추가 관리비용 발생, 그리고 단말 소매시장의 비활성화로 인해 기대만큼의 성과를 얻지 못하였다.

이와 같은 상황에서 북미 MSO(Multiple Service Operator)들을 중심으로 네트워크를 통해 제한수신 소프트웨어를 안전하게 다운로드 시킬 수 있는 다운로더블 제한수신시스템(DCAS; Downloadable CAS)에 대한 기술개발이 시작되었다[4-5]. 이는 단말에서 제한수신 모듈을 분리함으로써 케이블카드와 동일한 단말 표준화의 이점을 갖는 동시에 기존 케이블카드의 관리 비용을 줄일 수 있다는 장점을 가진다. 또한 케이블방송 사업자는 특정 CAS 업체 의존에서 탈피할 수 있으며, CAS의 결함이 발생하거나 업그레이드가 필요한 경우 즉시 대처할 수 있는 유연성을 확보할 수 있다. 이와 더불어 소비자는 단말 제조업체간의 가격 경쟁을 통한 다양한 고품질 단말들을 저렴하게 구매할 수 있는 기회를 가질 수 있다.

본 고에서는 국내외 케이블방송 분야에서 큰 화두로 떠오르고 있는 DCAS기술에 대해 다음과 같이 살펴보고자 한다. 먼저 Ⅱ장에서는 DCAS 시스템 요구사항에 대해 기술하고, Ⅲ장에서는 이를 만족시키기 위한 DCAS헤드엔드 및 호스트 관련 핵심기술을 소개한다. Ⅳ

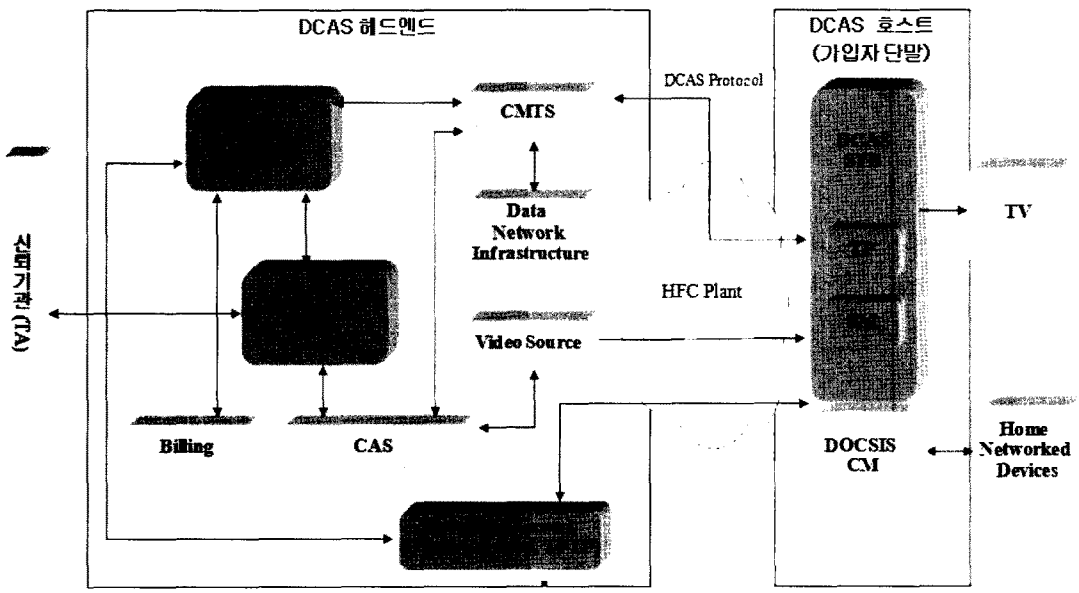
장에서는 현재 진행중인 국내외 기술개발 현황 및 표준화 관련 동향을 알아보고, 마지막으로 V 장에서 향후 전망에 대해 살펴보고자 한다.

II. DCAS 시스템 요구사항

DCAS시스템은 HFC망에서 DOCSIS네트워크를 통해 DCAS헤드엔드에서 DCAS호스트로 제한수신(CA)어플리케이션을 안전하게 전송하기 위한 시스템이다. 여기에 더하여 DCAS호스트는 케이블 방송 사업자 각각의 제한수신 시스템에 관계없이 표준화된 플랫폼의 제공을 목적으로 한다. 즉 DCAS시스템은 케이블 방송 사업자가 제한 수신 시스템을 변경하거나, 또는 가입자가 다른 케이블 사업자로 이동하여 서비스를 제공받으려 할 때, DCAS호스트의 하드웨어적인 변경 없이 해당 CA어플리케이션을 다운로드만 하면 되는 환경을 제공할 수 있다. 또한 DCAS시스템은 홈 네트워크 관련 ASD(Authorized Service Domain) 및 디지털 콘텐츠 보안 관련 DRM (Digital Right Management)어플리케이션의 다운로드도 지원한다.

그림 1은 DCAS 시스템의 구조를 나타내며, 크게 DCAS 헤드엔드와 DCAS 호스트로 구성된다. DCAS 헤드엔드는 키 관리(Key Management), CA 다운로드 프로토콜(Download Protocol) 및 전송 요구사항(Transport Requirements)을 관리하며, DCAS 호스트는 기존의 제한수신 방식들이 동작할 수 있는 후방 호환성을 제공하며 다수의 제한수신 방식을 지원하기 위한 멀티 디스크램블러 칩(TP; Transport Processor)과 CA 어플리케이션의 다운로드 및 구동을 위한 보안 칩(SM; Secure Micro)을 내장한다.

DCAS 헤드엔드에서 DCAS 호스트로 CA



〈그림 1〉 DCAS 시스템 구조

어플리케이션을 안전하게 전송하기 위해 DCAS 시스템은 안전하고 신뢰성 있는 구조로 설계되어야 한다. 이를 위해 DCAS 시스템이 만족해야 할 주요 요구사항은 다음과 같다.

- DCAS헤드엔드가 CA어플리케이션을 DCAS호스트의 SM으로 다운로드 할 때 헤드엔드는 SM이 적법한 가입자의 장치인지 확인할 수 있어야 하고, SM은 CA어플리케이션을 전송하는 헤드엔드가 케이블방송 사업자가 운용하는 합법적인 시스템인지 확인할 수 있어야 한다.
- 다운로드되는 CA어플리케이션의 보안을 위해 다운로드 프로토콜 상에서 데이터의 암호화, 데이터의 변조 유무에 대해 확인할 수 있어야 한다.
- CA어플리케이션의 변경 및 업데이트 시 시청자의 불편을 최소화 하여야 하며, DCAS헤드엔드는 다운로드된 CA어플리케이션이 DCAS호스트에 성공적으로 인스톨 되었는가에 대한 여부를 확인할 수 있어야 한다.
- DCAS프로토콜은 향후 필요에 의해 확장될 수 있는 구조로 설계되어야 하며, 네트워크 상에서 전송되는 메시지 수를 최소화하여 구현할 수 있어야 한다. 또한 DCAS메시지의 리플레이 공격을 저지하고 인증기관(TA; Trusted Authority)과의 키 체인(chain)을 통해 메시지를 인증할 수 있어야 한다.
- DCAS프로토콜 메시지는 명확하게 기술된 방식으로 전송하되 전송 계층에 독립적인 구조를 가질 수 있어야 한다.
- DCAS호스트 내에서도 SM과 TP간에 제한수신 관련 데이터(e.g. ECM, EMM)가 안전하게 이동할 수 있도록 보안이 유지되어야 한다.
- DCAS호스트는 동시에 다수 채널의 방송 스트림 디스크램블 및 이와 관련된 키에 대한 관리를 할 수 있어야 하며, 케이블방송 사업자가 선택한 제한수신 방식에 관계없이 CA어플리케이션이 구동될 수 있도록 표준화된 구조를 가져야 한다.

III. DCAS 주요 핵심기술

1. DCAS 헤드엔드

DCAS 헤드엔드는 그림 1에서 보는 바와 같이 4개의 서버로 구성되며, 각 구성요소에 대한 설명은 다음과 같다.

> Authentication Proxy (AP) : AP의 핵심 기능은 MSO의 헤드엔드 내에 위치하여 SM 클라이언트 이미지(CA, DRM, ASD어플리케이션)들을 안전하게 DCAS 호스트 내 SM으로 다운로드하기 위해 SM을 인증하고 SM과 AP간 보안 세션을 구성하는 것이다. SM과 보안 세션을 구성 할 때는 TA로부터 SM 인증을 위한 각종 인자 값들을 수신 할 뿐만 아니라 SM이 보내온 인증정보를 확인하는 기능도 수행한다. 즉, AP는 TA의 대리자 역할을 통해, MSO 네트워크에 연결된 SM들을 인증하는 서버를 의미한다.

> Local Key Server (LKS) : LKS는 케이블 운영자의 보안 정보를 보관 관리하는 기능을 수행한다. LKS는 별도의 서버로 헤드엔드에 위치할 수 도 있으며, AP의 논리적

구성요소로도 존재할 수도 있다. 만약, DCAS 보안 정보를 LKS에서 통합 관리하지 않는 시스템으로 구성할 경우 LKS는 별도의 서버로 구성되지 않을 수도 있다.

> Personalization Server (PS) : PS는 모든 SM 클라이언트 이미지들에 대한 배포, 다운로드, 관리 등을 수행하는 서버다. 따라서 PS는 CA, DRM, ASD 어플리케이션을 보관하고 이들을 Carousel, TFTP, HTTP를 통해 SM에게 전달하는 기능을 수행한다.

> DCAS Provisioning System (DPS) : DPS는 SM 클라이언트 이미지 다운로드를 위한 다운로드 정책 및 다운로드 스케줄링 정보를 생성 및 관리한다.

2. DCAS 프로토콜

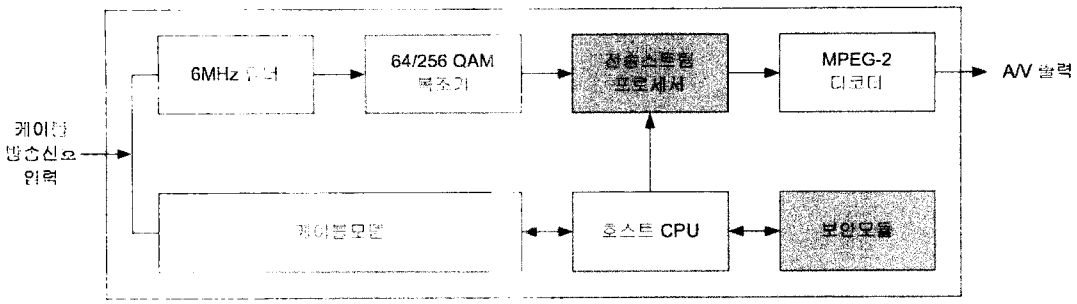
DCAS프로토콜을 통해 SM클라이언트 이미지는 헤드엔드 내의 AP로부터 DCAS호스트 내의 SM으로 안전하게 다운로딩 된다. DCAS 프로토콜의 핵심은 AP와 SM간의 상호 인증을 통해 SM클라이언트 이미지를 다운로드 받으려는 SM이 TA로부터 인증된 SM인지 아닌지 여부를 판단한 후, 인증 받은 SM일 경우 AP와 SM간 보안 세션을 형성하고 이를 통해 SM 클라이언트 이미지들을 다운로드 하는 데 있다. DCAS프로토콜은 AP가 TA와 SM간의 인증 정보를 교환하는 과정을 포함한다. 이와 같이 TA를 기반으로 AP와 SM간 상호 인증하는 인증 모델을 '3자 인증 모델 (three-way authentication model)' 이라고 부른다. DCAS 프로토콜의 4가지 중요 기능을 정리하면 다음과 같다.

- SM과 AP간 상호 인증을 수행한다.
- AP을 통해 SM을 MSO 망에 등록 시키는 기능을 수행한다.
- 필요에 따라 키를 갱신하는 기능을 수행한다.
- SM클라이언트 이미지를 SM내에 다운로딩 하는 기능을 수행한다.

DCAS 프로토콜의 각 메시지들은 가변 길이의 페이로드(payload)를 가지며, 메시지 인증을 위해 서명되어 전달된다. 이때 모든 메시지는 헤더에 NONCE를 포함하여 재전송 공격에 대비한다. 또한 망에 접속하는 모든 DCAS 호스트에게 현재 MSO망에서 운영하고 있는 SM클라이언트 이미지 종류 및 버전 정보 등을 알릴 수 있어야 한다. 이를 위해 AP는 SM 클라이언트 이미지 관련 정보를 담은 메시지를 브로드캐스팅하며, 이 메시지를 수신한 DCAS호스트는 SM클라이언트 이미지에 대한 다운로드 여부를 결정한다.

AP와 SM은 SM클라이언트 이미지를 안전하게 전달될 수 있도록 암호화 키를 이용하며, 이를 위해 DCAS프로토콜은 상호 인증 및 키 교환 기능을 포함하고 있다. 또한 SM클라이언트 이미지 다운로드 세션을 암호화기 위한 키의 갱신이 필요할 경우, 이를 동적으로 처리할 수 있는 키 갱신(rekeying) 기능도 포함한다.

AP가 DCAS 프로토콜을 통해 SM을 인증할 때 TA로부터 수신한 SM 인증 정보를 사용한다. 이 SM인증 정보와 별도로 TA로부터 AP와 SM간 형성되는 보안 세션에 사용될 암호화 키에 대한 생성인자 정보도 수신한다. 따라서 DCAS프로토콜은 앞서 언급한 바와 같이 TA가 AP와 SM간의 상호 인증 절차에 간접적으로 참여하는 '3자 인증 모델' 형태를 가진다.



〈그림 2〉 DCAS 호스트의 구조

DCAS 프로토콜은 단일 또는 복수개의 SM 클라이언트 이미지들을 한 세션 내에서 다운로딩 하는 것을 지원한다. SM은 다운로딩의 상태를 AP에게 보고하는 과정과 SM이 AP를 이동했을 때 기존 유료방송 구매 정보를 SM에서 AP로 전달하는 과정도 DCAS프로토콜은 지원한다.

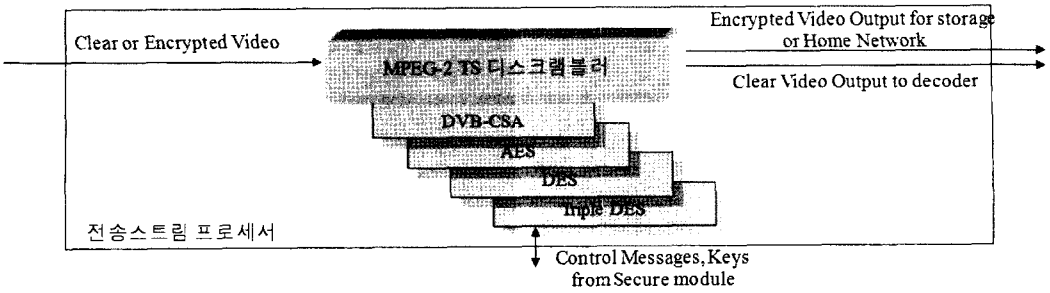
3. DCAS 호스트

DCAS호스트는 DCAS를 지원하는 케이블방송 시스템에서 제공되는 방송 신호 및 데이터 신호를 수신하는 기능을 지닌 가입자 단말장치로, 기존의 OpenCable방식의 가입자 단말장치와 달리, 가입자 단말장치를 인증하고 CAS, DRM, ASD등의 클라이언트 이미지들을 안전하게 저장하고 구동하는 보안모듈인 SM과 복수의 CA시스템을 지원할 수 있도록 다수의 디스크램블러를 지원하는 전송스트림 프로세서인 TP를 내장하고 있다. 이를 통해, DCAS호스트는 유선을 통한 다운로드 방식으로 자유롭게 제한수신 시스템을 변경할 수 있다. 그림 2는 DCAS 호스트의 개략적인 구조를 보여준다.

DCAS호스트는 보안모듈과 전송스트림 프로세서, 방송신호를 수신하고 재생하는 튜너, 복조기, MPEG-2디코더 및 데이터 송수신을 위한 내장형 케이블모뎀으로 구성된다. 방송신호의 처리 과정을 살펴보면, DCAS호스트로 입력된 방송용 A/V신호는 튜너와 복조기를 거쳐 MPEG-2 TS(Transport Stream) 형태로 전송스트림 프로세서로 출력되고, 전송스트림 프로세서는 해당 TS의 스크램블 여부를 판단하여 이를 처리한다. 전송스트림 프로세서의 출력은 디코더를 거쳐 TV신호로 출력된다. 또한, EPG(Electronic Program Guide), SI(System Information),CA(Conditional Access) 메시지 등의 방송 관련 부가정보들은 DSG (DOCSIS Set-top Gateway) 규격에 따라 케이블모뎀을 통해 DCAS호스트의 CPU로 입력되어 DCAS호스트 내부의 각 기능 모듈로 전달되어 처리된다.

가. 전송스트림 프로세서

전송스트림 프로세서는 DCAS 호스트에 내장되어 DCAS호스트로 입력되는 방송신호의 스크램블 여부와 가입자의 시청권한에 따라 해당 신호를 디스크램블 하는 기능을 담당한다. 전송스트림 프로세서의 디스크램블러는 여러 CA시스템을 지원할 수 있도록 AES



〈그림 3〉 전송스트림 프로세서의 구조

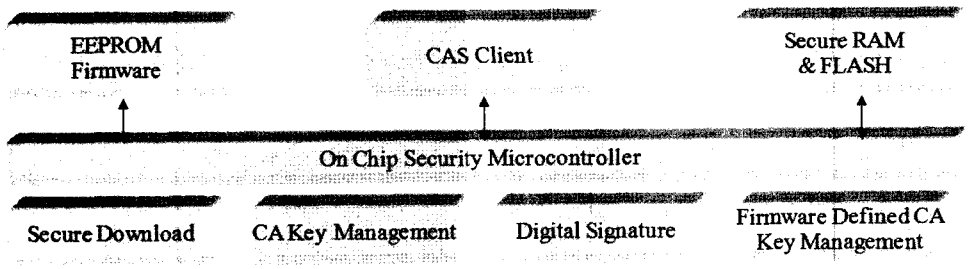
(Advanced Encryption Standard)-128, DES(Data Encryption Standard), 3-DES, CSA(Common Scrambling Algorithm) 등의 알고리즘을 내장하고 있으며, 방송 서비스 사업자가 원하는 특정 CA 시스템을 자유롭게 선택할 수 있도록 재설정 가능한 구조를 가지고 있다. 그림 3은 전송스트림 프로세서의 개략적인 구조를 보여준다.

전송스트림 프로세서는 보안모듈에서 구동되는 CA클라이언트로부터 디스크램블에 필요한 키 정보 등을 입력 받고, 이를 이용하여 스크램블된 프로그램을 디스크램블 한다. 또한, DCAS호스트가 수신한 방송 프로그램을 DCAS호스트 내의 하드디스크에 저장하거나, DCAS호스트에 연결되어 있는 외부의 방송 수신장치에 전송하는 경우, 해당 방송 프로그램을 보호하기 위해 이를 다시 재 암호화 하는 기능도 포함하고 있다. 이 밖에도 DCAS 호스트 인증에 사용되는 전송스트림 프로세서의 고유 ID와 인증서를 보안상 안전하게 저장하고 관리하는 기능도 포함하고 있다.

나. 보안 모듈

보안 모듈은 DCAS호스트에 내장되는 보안칩으로, DCAS헤드엔드와 가입자 장치에 대한 상호인증과 DCAS프로토콜 및 CA클라이언트 다운로드 등을 지원하는 보안모듈용 펌웨어 및 다운로드 받은 클라이언트 프로그램을 보안상 안전하게 저장하고 구동할 수 있는 환경을 제공한다. 그림 4는 보안모듈의 개략적인 구조를 보여준다.

보안모듈은 DCAS헤드엔드와의 상호인증 및 데이터 전송 과정에서 필요한 여러 암호화



〈그림 4〉 보안모듈의 구조

기능, 예를 들면, 인증, 기밀성 보장, 무결성 검증 등을 위한 여러 암호화 알고리즘을 지원하게 된다. 또한, 보안모듈의 구동을 위해 필요한 펌웨어 및 클라이언트 프로그램을 외부의 공격으로부터 보호하기 위한 보안 메모리, 템퍼 저항 등의 하드웨어 적인 여러 보안 장치들을 포함하고 있다.

IV. DCAS 기술개발 및 표준화 현황

Comcast를 비롯한 미국 주요 MSO들은 DCAS 기술 개발을 위하여 2004년 중반에Next Generation Network Architecture(NGNA) joint venture 회사를 설립하고 DCAS 프로젝트 시작하였다. 2005년 7월에 미국 케이블 사업자 단체인 NCTA가 FCC에 DCAS 기술에 대한 기능 시연을 하였고, 같은 해 11월에는 2008년 7월까지 DCAS 기술의 전국적인 roll-out에 대한 계획을 FCC에 제출하였다. 이를 수용한 FCC는 케이블용 STB에 있어, CAS 내장형 STB사용을 금지하고, 케이블 사업자에게 의존하는 CAS기능과 STB본체를 분리하게 하는 네비게이션 장치 법안(Navigation Device Rule)을 2년 동안의 유예 기간을 거쳐 2007년 7월부터 시행 중에 있다[6-7]. 이에 STB에서 CAS기능을 분리하기 위한 방법으로 CableCARD 및 DCAS 기술 등이 존재하나, DCAS는 아직 상용화되지 않은 이유로 현재로서는 CableCARD가 시장에 보급되고 있는 상황이다.

1. 국내 기술개발 현황

국내에서의 DCAS 기술개발은 2007년 3월 ETRI를 주관연구기관으로 KLabs, 코어트러스트, 디지털스트림테크놀로지, 코어크로스 등이 참여하는 "Downloadable제한수신 시스템 기술 개발" 사업을 시작으로 본격적으로 추진되고 있다. 2007년 이전에도 삼성전자, LG전자 등이 PolyCipher와의 협력 하에 미국에서 진행 중인 DCAS프로젝트에 참여해온 것으로 알려졌으나, 기술 개발에 관한 내용들이 외부에 전혀 알려지지 않고 있다.

현재 ETRI에서 진행 중인 Downloadable제한수신 시스템 개발은 케이블 방송용 DCAS 헤드엔드 서버 개발, DCAS용 가입자 단말 개발, DCAS프로토콜 개발, 테스트베드 구축 및 DCAS 기술과 관련한 국내/외 표준화를 목표로 하고 있다. 올해 6월, 부산에서 열린 KCTA 전시회에서는 ETRI, KLabs 컨소시엄, 삼성전자, 알티캐스트 등이 개발 중인 DCAS시스템 또는 STB제품들을 전시하였으며, 국내에서도 DCAS관련 기술 및 제품 개발이 활발히 진행되고 있다.

2. 국외 기술개발 현황

미국의 주요 MSO인 Comcast, Time Warner Cable, Cox Communications는 2004년에 PolyCipher사를 설립한 후, 이를 중심으로 DCAS 관련 기술 개발을 추진하여 왔다. 미국 내 DCAS관련 기술 개발은 PolyCipher 및 Comcast가 주도적으로 진행하였으며, 현재 검증 시스템 수준의 시스템 개발은 완료된 것으로 파악되며, 최근 Motorola, Scientific Atlanta, NDS등이 상용화를 위한 기술개발에 추가로 참여하였다. 한편, 2007년 BBT(Beyond Broadband Technology LLC) 사는 PolyCipher사의 DCAS를 지원하는 저가형 STB를 개발하

였다고 발표하였으며, Widevine사도 PolyCipher에서 개발한 DCAS와는 다른 DCAS솔루션을 개발하였다고 발표하였다. DCAS기술은 2008년 중반 혹은 늦어도 2009년 중에 미국 내 상용화가 완료될 것으로 예상되어 왔었으나, 현재로서는 상용화 및 도입 시기의 지연은 불가피해 보인다[8-9].

3. 국내/외 표준화 현황

국내 DCAS 표준화는 케이블 방송 사업자 표준화를 담당하는 KLabs를 중심으로 케이블 방송 사업자 및 ETRI를 포함한 관련 기술개발 기관 등이 참여하여 2008년 10월부터 본격적으로 시작될 예정이며, 이를 위한 표준화 범위 및 일정 등에 관한 사전 논의가 진행 중에 있다. 국내 케이블 방송 사업자 및 관련 기술 개발 기관들의 지대한 관심과 노력으로 금년 말까지 주요 내용에 대한 표준 초안 작성이 이루어질 것으로 예상된다.

미국의 경우, PolyCipher등을 중심으로 DCAS프로토콜, 단말 및 보안 칩 관련 기술 규격의 개발을 완료한 것으로 파악되고 있으나, 이들 규격들에 대한 일반 공개는 이루어지지 않고 있다. 다만, 미국 CableLabs를 통해 DCAS 관련 기술 규격 중 일부인 DCAS Host 관련 기술 규격 초안들을 "DCAS Host License Agreement"를 체결한 업체에 한해 공개하고 있으나, 이외의 기술 규격들은 전혀 공개하고 있지 않다. 따라서, CableLabs을 통한 표준화 움직임은 아직까지 논의 조차도 이루어지지 않고 있으며, PolyCipher를 중심으로 개발된 기술 규격들이 향후 일정 부분 DCAS 표준 규격으로 채택될 가능성이 있을 것으로 예상된다.

V. 향후 전망

그 동안 북미 MSO들은 CableCARD의 대안으로 DCAS 도입을 적극적으로 검토하여 왔다. 그러나, 2007년 6월 FCC가 케이블 업계의 보안 모듈 분리 의무화 유예 요청을 거부함에 따라, 현재로서는 CableCARD를 적용한 STB 보급에 많이 치중하고 있다. 이로 인해 현재 북미에서의 DCAS 기술 도입 움직임은 다소 추진력이 떨어진 상황으로 아직 구체적인 상용화 시기는 거론되지 않고 있으며, 2009년 이전에는 DCAS상용화가 힘들 것으로 예상되고 있다.

국내의 경우, 북미의 상황과는 일부 다르게, CableCARD 분리 의무 유예에 대한 검토가 진행됨에 따라 DCAS 기술 상용화에 대한 관심이 높아지고 있다. 이와 함께, 현재 ETRI 및 케이블 방송 관련 기관을 중심으로 진행중인 DCAS 기술개발 및 표준화가 원활히 진행될 경우 2010년 하반기에는 상용화가 가능할것으로 예상된다

참고문헌

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

[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] Federal Communications Commission FCC 07-127, Page 2
[7] http://www.multichannel.com/article/CA6480827.html?q=Download+Incomplete
[8] http://www.cedmagazine.com/Article-night-polycipher-shift.aspx
[9] Federal Communications Commission FCC 08-88, Page 6

저자소개

정 준 영

1999년 2월 영남대학교 전자공학 학사
2001년 2월 한국정보통신대학교(ICU) 공학석사
2001년 2월-현재 한국전자통신연구원 방송시스템연구부 재직
2003년 7월-2004년 6월 Cable Television Laboratories, Inc. (미국, 덴버) Visiting Engineer

주관심 분야 : 디지털 케이블 방송/통신, 제한수신 시스템

저자소개

정 영 호

1988년 2월 전북대학교 전자공학과 학사
1992년 2월 전북대학교 전자공학과 석사
2006년 8월 충남대학교 전자공학과 박사
1994년 3월-현재 한국전자통신연구원 선임연구원

주관심 분야 : DCAS, Network Security, DCATV

구 한 승

1992년 3월-1999년 2월 충남대학교 전자공학과 학사
1999년 3월-2001년 2월 충남대학교 전자공학과 대학원 석사
2005년 3월-2008년 8월 충남대학교 전자공학과 대학원 박사

2001년 2월-현재 한국전자통신연구원(ETRI) 선임연구원

주관심 분야 : 방송 및 통신 보안 시스템

저자소개

조 용 성

1998년 2월 전북대학교 공과대학 전자공학 학사
2001년 2월 전북대학교 일반대학원 전자공학 석사
2001년 2월-현재 한국전자통신연구원 선임연구원

주관심 분야 : DCATV, 정보보호

유 웅 식

1997년 8월 충남대학교 컴퓨터공학과 졸업
2000년 2월 충남대학교 컴퓨터공학과 석사
2000년 4월-현재 한국전자통신연구원 선임연구원
2005년 12월-2006년 12월 CableLabs Visiting Engineer

주관심 분야 : DOCSIS 시스템, IPTV, DCAS 시스템

저자소개

권 오 형

1981년 2월 서강대학교 전자공학과 학사
1983년 2월 서강대학교 전자공학과 석사
2004년 7월 서강대학교 전자공학과 박사
1983년 3월-현재 한국전자통신연구원 디지털CATV 시스템연구팀 팀장

주관심 분야 : DCATV, DCAS, IPTV, CAS