특집, 제한수신기술

다운로드형 제한수신 시스템 기술 동향

□ 김영모, 고병수 / 디지캡

I. 서 론

제한수신시스템은(CAS: Conditional Access System)은 방송사업자에게 유료방송 사업을 제공하는 핵심적인 기술이다. 최근 정부는 "유선방송국설비등에관한기술기준"에 대하여 디지털 케이블 방송과 IPTV의 기술기준에 대한 형평성을 고려해 제한수신 모듈(일명: CableCARD) 분리를 2010년 12월31일까지 유예토록 했다[1].

국내 "유선방송국설비등에관한기술기준"의 제25조(제한수신)는 "디지털유선방송송수신정합표준"을 따른다고 명시하고 있으며, "디지털유선방송송수신정합표준"에서는 OpenCable의 규격을 따른다고 명시하고 있다[2] [3]. OpenCable 규격에서는 가입자 정보를 별도의 CableCARD를 이용하여 STB(Set Top Box)로부터 분리/장착할 수 있도록 규정하여 방송사업자 변경 시 CableCARD의 교체만으로 기존 STB를 재사용할 수 있도록 명시하고 있다[4]. 하지만 2005년도에 CableCARD를 도입한 국내의 경우 방송사업자의 STB 임대서비스로 인하여 특정 사업자에게 종속되는 문제점과 CableCARD의 발열로 인한 STB 고장 그리고 CableCARD 사용으로 인한 STB 가격 상승 등의 문제점이 발생하고 있다. 이에 케이블 사업자들과 Klabs(한국케이블연구원) 등은 CableCARD 적용 의무화에 대한 정책 변경을 정부에 요구하였으며, 정부는 이 문제와 함께 여러 복합적인 이유로 인하여 CableCARD 분리를 2년간 유예하였다. 2년간 유예는 방송사업자들과 CAS 업체들에게 대안 마련을 위한 시간이라 할 수 있으며, 현재 사업자들은 Embeded 형태의 CAS와 소프트웨어 기반의 CAS 그리고 DCAS 기술을 대안으로 고려하고 있다[1]. 특히, DCAS 기술은 네트워크를 통하여 STB 내의 보안칩(SM: Secure Micro)에 사업자가 제공하는 CAS/DRM(Digital Right Management)/ASD(Authorized Service Domain)

Client 모듈을 다운로드하고, 설치하여 서비스하는 플랫폼 기술로서, 서비스 확장성과 CableCARD에 따른 비용절감, CAS 다운로드만으로 CAS를 변경할 수 있어 CAS의 종속성 탈피 그리고 현재의 기술기준을 개정하지 않고도 도입할 수 있다는 점에서 더욱 관심을 받고 있다.

또한, 정부의 국산 CAS 지원과 맞물려 DCAS 기술과 더불어 SimulCrypt 기술이 관심받고 있다. 현재 국내 방송시장에 적용된 CAS 기술은 NDS, Conax, Nagra, Irdeto 등의 외산업체들의 기술이 대부분이며, 위성 DMB와 IPTV 시장에서 일부 국산 업체의 기술이 적용되어 있어 CAS의 외산 의존성이 높다. 더구나, 초기 구축비용이 많이 소요되어 시스템 변경이 쉽지 않은 CAS의 특성은 CAS 기술의 외산 의존성을 더욱 높이고 있어 정부 및 방송업계의 대책마련이 시급한 상황이다. 하지만, 국산 CAS의 경우 기술 검증 문제와 함께 도입 시 기존의 STB을 모두 변경해야 하는 문제로 인하여 많은 고려가 이루어 졌으며, 고려결과 기존의 STB을 변경하지 않고, 신규 STB과 병행하여 CAS 서비스를 지원할 수 있게 해주는 SimulCrypt 기술이 관심을 받게 되었다.

따라서 본 고에서는 최신 정부와 방송계에서 CableCARD 유예와 함께 CAS 국산화의 지원기술로 이슈화 되고 있는 DCAS기술과 SimulCrypt에 대하여 다음과 같이 살펴보고자 한다. Ⅱ에서는 DCAS 기술에 대한 소개와 현재 이슈화 되고 있는 SimulCrypt 기술을 소개한다. Ⅲ에서는 국내외 DCAS 기술에 대한 동향을 살펴보고, Ⅳ에서는 DCAS 기술에 대한 국내외 표준화 동향을 살펴본다. 마지막으로 Ⅴ에서 결론 및 향후 전망을 살펴보기로 한다.

Ⅱ. DCAS 기술 소개

본 장에서는 CableCARD 유예에 따라 CableCARD의 대안으로 고려되고 있는 CAS 기술을 살펴보고,

〈표 1〉 CableCARD 대안으로 제시되는 제한수신시스템 유형

CableCARD 유형		장 점	단 점
소프트웨어 기반의 CAS	보안수단 없음	– 개방구조 – 빠른 개발 가능 – 낮은 CAS 비용 – 낮은 업그레이드 비용	– 해킹위험에 취약 – 낮은 성능위험
	보안수단 구비	– 개방구조 – 빠른 개발 가능 – 낮은 CAS 비용 – 낮은 업그레이드 비용	– 낮은 성능위험 – 강화된 보안수단에 대한 보안성 검증필요
Embeded CAS		– 상대적으로 낮은 STB가격 – 빠른 개발 가능	– STB 모델 추가시 CAS 비용발생 – retail Market 불가 – STB에 대한 사용자 선택 불가능 – STB이 특정 CAS업체에 한정
DCAS		– 개방시스템 구조 – CAS 운영의 제어성 높임 – 서비스 확장성 높음(CAS 뿐만 아니라 DRM/ASD 기능도 추가 다운로드 설치 가능) – 다소 낮은 CAS 업그레이드 비용	– 추가적인 DCAS 서버 운영필요 – DCAS와 CAS 보안의 영역이 분리되어 해킹 발생시 책임소재를 판단하기 어려움

현재 대안기술로 가장 관심을 받고 있는 DCAS 기술과 DVB(Digital Video Broadcasting)에서 제안하는 SimulCrypt기술을 살펴보고자 한다. 다음 <표 1>은 현재 CableCARD의 대안으로 이슈화되고 있는 기술에 대한 장단점을 나타내는 표이다.

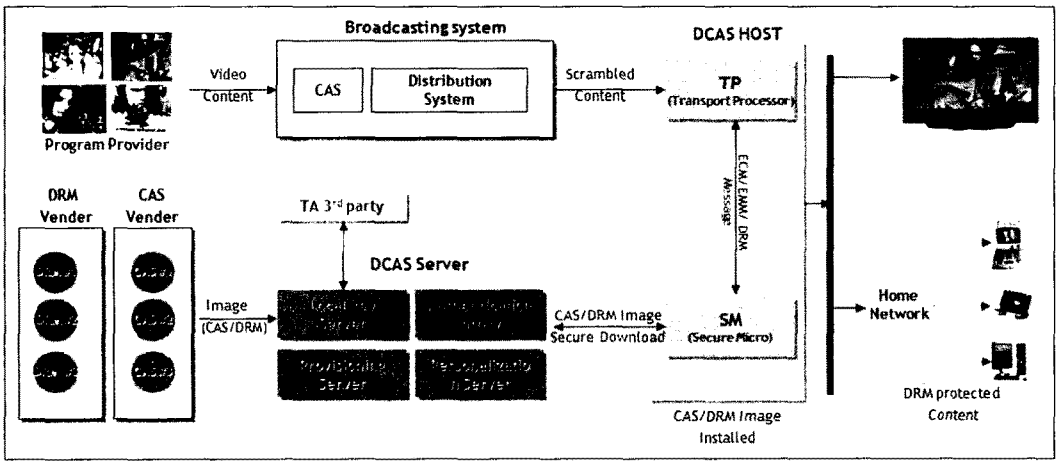
소프트웨어 기반의 CAS는 일반 OS에 탑재하는 형태로 보안수단이 없는 형태와 보안수단을 구비하는 형태로 적용할 수 있다. 일반적인 형태의 경우 보통의 마이크로프로세서에 CAS 모듈을 탑재하는 것으로 구현이 쉽고, 가격과 서비스 유연성 면에서 장점을 가지나 성능상의 문제와 보안에 취약한 단점이 있다. 이는 보안수단을 구비했다 할지라도, 보안수단에 대한 검증이 되지 않을 경우 소프트웨어 보안의 잠재적인 취약점을 항상 가지고 있는 것과 마찬가지다.

Embeded CAS는 STB 내의 SoC를 통해 CAS 모듈을 탑재하는 기술로서 상대적으로 낮은 STB가격과 빠른 개발시간의 장점이 있으나 STB 모델 추가 시 CAS 비용발생과 특정업체의 CAS에 종속이 될 수 있는 단점이 있다.

마지막으로 DCAS는 네트워크를 통하여 STB 내의 보안칩에 사업자가 제공하는 CAS/DRM/ASD Client 모듈을 다운로드하고, 설치하여 서비스 하는 플랫폼 기술로서, 개방형 구조, 서비스 확장성과, CableCARD에 따른 비용절감, CAS의 종속성을 탈피, 그리고 "유선방송국설비등에관한기술기준"을 개정하지 않고도 도입할 수 있는 장점이 있으나, 추가적인 DCAS Server 운영이 필요하며, DCAS와 CAS의 보안영역이 분리되어 해킹발생시 책임소재를 판단하기 어려운 단점이 있다.

1. DCAS 기술

DCAS 기술은 STB에 CAS가 미리 설치되어 있는 것이 아니라 STB가 사업자 네트워크 연결시 DCAS Server로부터 CAS 이미지를 안전하게 DCAS HOST의 SM에 다운로드하여 설치한 후 스크램블된 방송을 디스크램블하여 시청할 수 있도록 하는 기술로서, 다운로드 받은 CAS, DRM, ASD 등의 콘텐츠 보호 모듈이 잘 구동되어 서비스 될 수 있도록 지원하는 플랫폼 기술이라 할 수 있다. <그림 1>은



<그림 1> DCAS 시스템 구성도

DCAS 시스템 구성도이다. DCAS 시스템은 크게 DCAS Server, DCAS HOST 그리고 3rd party에서 SM(Secure Micro), TP(Transport Processor) 인증서를 관리하는 TA로 구성될 수 있다.

1) DCAS Server

DCAS Server는 다음과 같이 4개의 주요 콤포넌트들로 구성된다.

- AP(Authentication proxy)는 사업자의 헤드엔드(Head-End) 내에 위치하며 SM Client 이미지(CAS/DRM/ASD Clinet)를 SM에 다운로드 하기 위하여 SM을 인증하고, 이미지 다운로드를 위한 정보를 전송하는 DCAS Server의 Proxy 역할을 담당한다.
- DPS(DCAS Provisioning System)는 사업자의 이미지 등록과 정책정보등록에 의하여 이미지 다운로드에 대한 MSO의 정책 및 스케줄링 정보를 생성하고 관리하는 역할을 한다.
- PS(Personalization Server)는 DPS의 정책에 따라 SM에 다운로드 되어질 이미지를 선택하고, 개인화하여 배포하는 서버로서, SM Client 이미지를 생성하고, DPS의 정책에 따라 다운로드서버(Carousel, TFTP, HTTP 등)에 전달하는 기능을 담당한다.
- LKS(Local Key Server)는 사업자의 네트워크에 속한 모든 SM, TP에 대한 인증정보를 TA를 통하여 전송받고, 이미지 암호화키를 관리한다.

2) DCAS HOST

DCAS Host는 DCAS 서비스를 지원하는 단말로 케이블 망에서 제공하는 방송신호 및 데이터 신호를 수신하는 기능을 지닌 단말로서, SM, TP구조를 갖는다.

- TP는 암호화 모듈/디스클램블링 모듈로서 여러 개의 디스크램블링 알고리즘들을 처리할 수 있는 유연한 복호화 엔진(Flexible Decryption Engine)을 구비해야 한다[8].
- SM은 DCAS HOST에 내장되는 보안칩으로, DCAS Server와 통신하여 SM Client 이미지(CAS/DRM/ASD 모듈)를 다운로드 받으며, 다운로드 받은 SM Client 이미지를 설치하고, TP와 통신하여 설치된 콘텐츠 보호서비스를 제공한다.

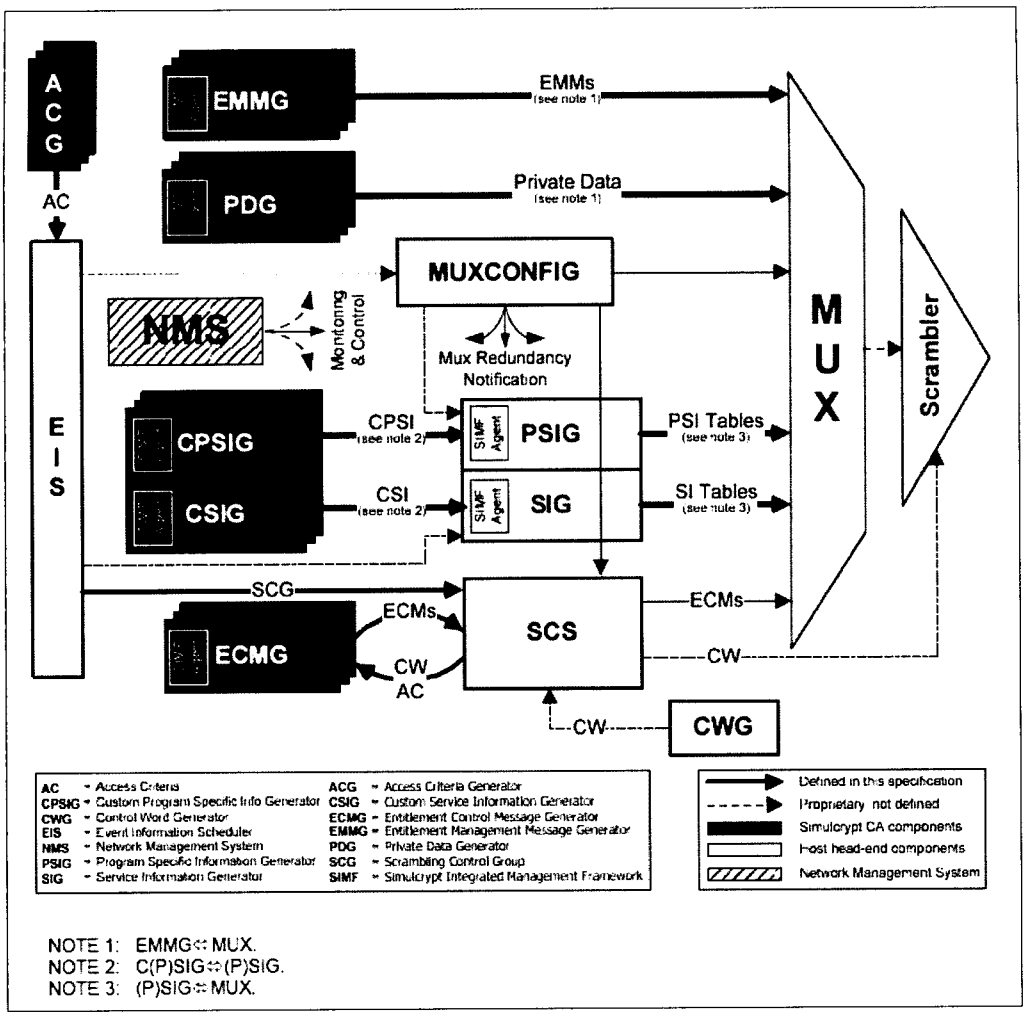
3) TA(trusted Authority)

TA(Trusted Authority) 시스템은 SM의 소매시장을 위하여 DCAS 시스템에서 3rd Party 구성요소로 설계되었으며, DCAS HOST를 위한 SM, TP의 인증서를 발행하고, DCAS HOST의 신규 등록과 지역 이동에 관련하여 인증을 하거나, LKS의 인증정보 요청 시 인증정보를 전달한다.

2. SimulCrypt 기술

CAS에 대한 개방적인 국제 표준을 제시하기 위하여 STB의 사용과 배포에 관심을 둔 DVB는 특히, 유료방송 서비스 시장이 특정 CAS 사업자에 의해 독점되는 것을 방지하는 것을 목표로 하였으며, 이를 위해 SimuCrypt 기술과 MultiCrypt 기술을 제안하였다.

SimulCrypt 기술은 여러 CAS 공급자를 수용하기 위하여 STB에서 디스크램블링과 암호화 처리를 담당하는 부분을 모듈로 분리한 방식이다. 이는 모듈에서 동작하는 디스크램블링과 암호화 기능을 분리하여 디스크램블링 방식을 Common Scrambling 알



<그림 2> DVB SimulCrypt System Architecture

고리즘인 DVB-CSA(Common Scrambling Algorithm)을 사용하도록 하고, 암호화 방법은 각 CAS 마다 다르게 사용하도록 하여 STB이 서로 다른 CAS를 갖는 보안모듈을 수용할 수 있도록 하였다. <그림 2>는 DVB SimulCrypt System Architecture이다[6].

제어단어(CW: Control Word)의 생성은 한 곳에서 이루어지며 SimulCrypt Synchroniser를 통해 제어단어 생성주기마다 TCP/IP 통신을 통해 Scambler에 제어단어를 전송하고, CAS로 제어단어를 전송한다. 이에 따라 CAS는 SimulCrypt Synchroniser를 통해 여러 개의 CAS로부터 생성되는 ECM을 재다중화기로 전송할 수 있으며 SMS는 가입자 별로 ECM을 해석하기 위한 EMM을 생성하여 재다중화기로 전송할 수 있도록 하였다.

Common Scrambling 기술에 대한 표준의 내용은

스크램블링 알고리즘, CA와 관련된 메시지가 MPEG2-TS 패킷에서의 다중화 되는 방법 그리고 제어단어를 생성하고 스크램블러로 전송하기 위한 메커니즘 등에 관련된 것이다.

이와 관련하여 MPEG 시스템 ISO/IEC 13818-1에 CAS로부터 생성되는 메시지에 대하여 Table ID 값에 대한 정의를 추가하였고, 모듈에서 다수의 CAS를 구별하기 위해서 CA_descriptor를 정의하는 방법을 규정하였다. 다음 <표 2>는 MPEG TS CA_descriptor이다.

<표 2> MPEG TS의 CA_descriptor

Syntax	NO. of bits	Mnemonic
CA_descriptor(){		
descriptor_tag	8	uimnbf
descriptor_length	8	uimnbf
CA_system_ID	16	uimnbf
reserved	3	bslbf
CA_PID	13	uimnbf
for(i=0;i<N;i++){		
private_data_byte	8	uimnbf
}		
}		

각 필드를 설명하면 다음과 같다.

- descriptor_tag: 0x09의 값을 가지며 descriptor가 CA_descriptor임을 표시
- descriptor_length: descriptor의 바이트 수를 표시
- CA_system_ID: 각 CAS을 구별하기 위해 사용하는 식별자로서, 관련된 ECM이나 EMM의 CAS 타입을 말함
- CA_PID: CA_system_ID에 의해서 지정된 CAS의 ECM이나 EMM정보를 포함하는 TS packet의 PID를 가리키는 것으로, CA_PID는 EMM과 같이 시스템 전반의 관리에 사용되는 CAS용 메시지를 지시하는데 사용되는 구별자
- Reserved: 확장성을 위해 미래에 사용될 수 있는 값으로 모든 비트가 '1'로 정해져 있음
- private_data_byte: 각 CAS에서 정의하여 사용할 수 있는 필드

III. DCAS 기술 동향

1. 국외 DCAS 기술 동향

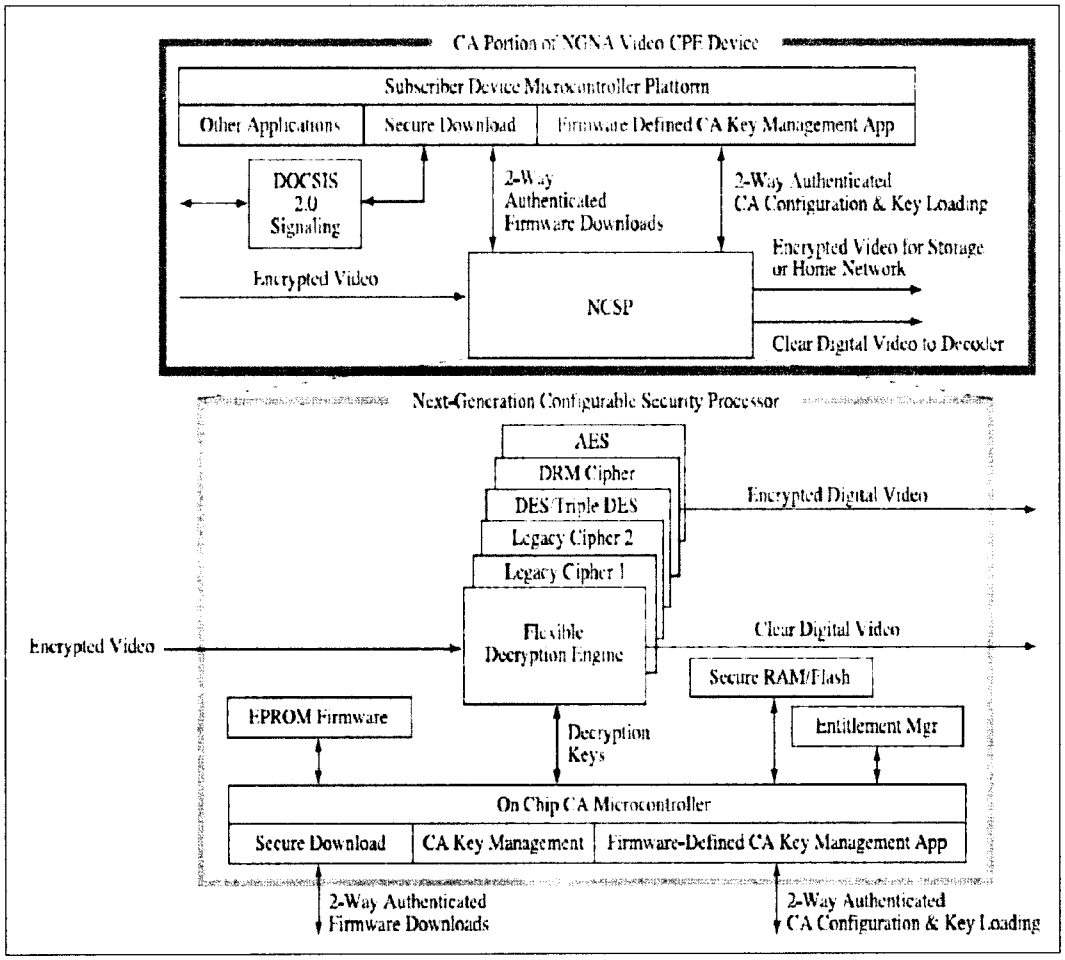
국외에서는 미국내 주요 케이블사업자인 Comcast, Time Warner Cable, Cox가 2004년부터 NGNA (Next Generation Next Architecture) 프로젝트를 통신사업자의 FTTH 구축 계획에 맞서 추진해 온 것으로 그 핵심 기술 개발의 일환으로 PolyCipher라는 조인트 벤처회사를 설립하여 규격작업을 하고 있다. PolyCipher 설립 초기에는 모토로라, SA, NDS, NagraVision, 삼성, LG, Vidiom 등 주요 개발업체들이 직간접적으로 개발에 참여해왔으나 작년부터 FCC가 CableCard 의무화 정책을 시행하고 모토로라, SA 등 북미 케이블 업계를 주도하는 업체들의 Security에 대한 문제점 제기 등으로 인해 현재로서는 진행이 중단된 상태로 관망을 하고 있다. 한편, 2007년 BBT(BeyondBroadband Technology LLC.)는 PolyCipher의 DCAS를 지원하는 저가형 STB를 개발하였다고 발표하였으며, Widevine은 PolyCipher에서 개발한 DCAS와는 다른 DCAS솔루션을 개발하였다고 발표하였다[7]. <그림 3>은 NGNA 보안 참조 모델이다[8]. 이 모델을 살펴보면, PolyCipher에서 규격화 하고자 하는 대상은 DCAS를 지원할 수 있는 제한수신 프로세서의 기능 및 구조와 제한수신 프로세서와 송수신부 간에 CAS 모듈을 안전하게 다운로드 받을 수 있도록 하기 위한

것이다.

제한수신 프로세서는 여러 개의 디스크램블링 알고리즘들을 처리할 수 있는 유연한 복호화 엔진(Flexible Decryption Engine)과 제한수신 키 관리를 위한 키 관리 애플리케이션 등으로 구성된다. 유연한 복호화 엔진은 서비스운영자가 선택할 수 있는 CAS 시스템의 폭을 넓혀주기 위하여 DES(Data Encryption Standard), Triple DES, AES(Advanced Encryption Standard), DVB-Common Scrambling Algorithm, MediaCipher(Motorola®), PowerKey (Scientific Atlanta®) 등의 알고리즘을 포함해야 한다. 송신부와 제한수신 프로세서간은 인증 메커니즘 및 데이터 암호화 등을 포함하는 안전한 다운로드(Secure Download) 방식이다.

2. 국내 DCAS 기술 동향

국내의 DCAS 기술 개발은 삼성전자와 LG전자가



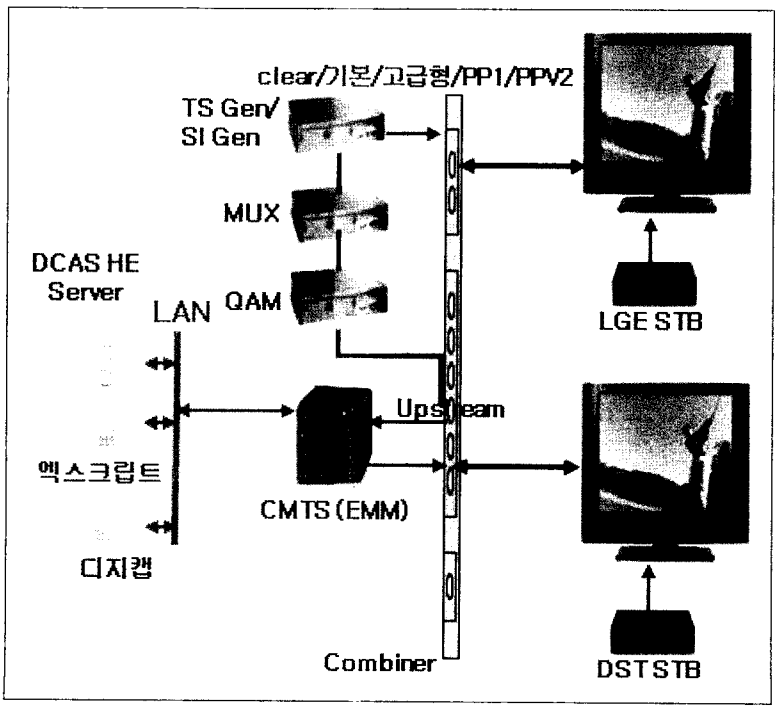
<그림 3> NGNA 보안 참조 모델

2005년11월과 2006년 1월에 DCAS 방식의 STB을 'FCC' 와 '2006 CES'에서 시연한 사례가 있으나 구체적인 내용은 알려지지 않고 있으며, 알려진 본격적인 개발은 2006년 7월부터 디지캡과 LGCNS가 공동으로 추진하여 개발한 DCAS 시스템으로서, 현재 개발을 완료하여 상용화 준비 중인 것으로 알려졌다. 또한, 미들웨어 기술로 유명한 Alticast에서도 소프트웨어 기반의 DCAS 기술을 개발 완료하여 상용화 준비 중에 있는 것으로 알려졌으며, 국책연구기관인 ETRI(전자통신연구원)에서도 2007년부터 Klabs, 코어트러스트, DST, 코어크로스 등과 함께 "Downloadable 제한수신 시스템 기술개발" 사업을 수행하고 있는 것으로 알려졌다.

Klabs에서는 2008년 1월부터 Klabs, LGCNS, 디지캡, 알티캐스트, LG전자, 삼성전자, 엑스크립트, DST, TVStrom 등이 참여하는 DCAS 컨소시엄을 진행하여 2008년 6월에 부산에서 열린 KCTA 전시회에서 ETRI, 알티캐스트, 삼성전자 등과 함께 개발 중인 DCAS 시스템 또는 STB 제품들을 전시하였으며, 2008년 9월 Klabs Conference 전시에서는 DCAS 상용화 가능성과 DCAS 기술을 국가적으로 쟁점화 시켰다.

현재 이들 3개의 DCAS 솔루션 업체들은 방송통신위원회가 중심이 되어 진행 중인 국내의 DCAS 표준화에 참여하고 있으며, 2009년 상반기에는 TTA를 통해 표준화를 완료할 계획이다[2] [9].

<그림 4>는 2008 Klabs Conference에서 Klabs 컨소시엄 group1 (LGCNS, 디지캡, LG전자, Xcrypt, DST, TVStorm)이 시연한 System 구성도로서, 컨



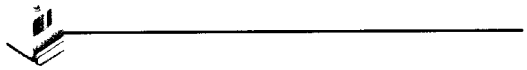
<그림 4> 2008 KLabs Conference Klabs DCAS 컨소시엄에서 시연한 시스템 구성도

소시엄에서는 두 개의 CAS를 동시에 서비스하는 SimulCrypt 기술과 두 종류의 CAS 이미지를 각각 다운로드하여 CAS 서비스를 제공하는 DCAS 기술을 시연하였다.

IV. DCAS 기술 표준화 동향

1. 국외의 DCAS 기술 표준화 동향

해외의 경우 미국의 PolyCipher를 중심으로 DCAS 프로토콜과 단말 및 보안 칩 관련 기술 규격이 개발완료 된 것으로 파악되고 있으나, CableLabs를 통한 표준화 움직임은 아직까지 파악되지 않고 있다. 향후 표준화 논의 시 PolyCipher를 중심으로 개발된 기술 규격들이 DCAS 표준 규격으로 채택될 가능성이 높을 것으로 예상된다. 현재 PolyCipher에서 개발된 일부 DCAS 규격들은 미국 CableLabs를 통해 "DCAS Host Liecense Agreement"를 체결한 업체에 한해 다음과 같은 규격이 공개되고 있으며, 일반인에게는 비공개로 하고 있다[9].



- OpenCable DCAS Specifications – Host Device 2.5 Core Functional Requirements
- OpenCable DCAS Specifications – DCAS System Overview Technical Report
- DCAS Content Protection Specification
- DCAS Authorized Service Domain – DVR Specification
- DCAS Authorized Service Domain – Host Home Networking Specification
- DCAS Host Software Requirements Specification
- DCAS Pairing System Interface Specification
- DCAS Pairing System Operations Guide

2. 국내의 DCAS 기술 표준화 동향

국내 DCAS 기술의 표준화는 현재 방송통신위원회를 중심으로 진행 중이며, 2009년 상반기에는 TTA를 통해 표준화를 완료할 계획에 있다[2]. 현재 Klabs, 케이블 방송 사업자(C&M, Tbroad, 큐릭스 등), DCAS 업체(LGCNS & 디지캡, ETRI, Alticast), STB 업체(LG전자, 삼성전자, 휴맥스 등), CAS 업체(디지캡, Xcrypt, 드리머아이 등), 유관기관(TTA, KISA, 한국정보인증 등) 등이 모여 DCAS 기술기준 제정 실무반을 구성하여 작업하고 있으며, 방송통신위원회에서는 DCAS 표준화를 위해 기본 아키텍처는 PolyCipher의 DCAS 아키텍처를 따르며 세부기술에 대해서는 국내 개발사의 기술을 활용하여 진행할 예정이다.

실무반 작업 중 여러 가지 쟁점사항이 발생하였으며, 그 중에서 가장 쟁점화 된 사항은 보안모듈이라 할 수 있다[10]. 보안모듈에 대한 쟁점화 내용은 소프트웨어 기반의 보안모듈과 하드웨어 기반의 보안모듈을 사용하는데 있어서 보안모듈에 대한 보안성 문제이다. 보안성 문제가 크게 쟁점화 되는 것은 CAS와 DCAS의 보안 영역이 서로 다르기 때문이다. CAS의 경우 콘텐츠 보호가 목적인 반면, DCAS는 보안모듈에 적용되는 CAS 모듈을 보호해야 하는 차이가 있다.

하드웨어 기반의 보안모듈은 보안칩 형태라 할 수 있으며, 보안칩은 MCU 플랫폼에 강화된 보안 시스템을 적용하여 펌웨어 해킹으로 인한 복제방지 시스템의 접근을 차단하며, 반도체칩 분해가 불가능한 형태의 칩이다. 하지만 소프트웨어 기반의 보안모듈은 STB의 OS에 로딩되어 역 엔지니어링 방지와 양방향 네트워크를 통해 수시로 인증을 실시하여 복제(cloning) 공격 등을 방어하는 보안 메커니즘을 사용

하여 보안을 강화한다고 하지만, 보안메커니즘에 대한 검증이 되지 않을 경우 소프트웨어 보안의 잠재적인 취약점은 여전히 존재하게 된다.

따라서 CAS 업체의 경우 타사가 개발한 보안모듈에 자신의 CAS 모듈을 업로드 하는 데 있어서, 자칫 보안모듈의 취약점으로 인하여 자사의 CAS 모듈에 대한 해킹이 일어날 시, 업체의 존폐를 위협할 수 있어, 자사의 CAS 모듈이 안전하게 보호되길 바란다. 일부 CAS 업체에서는 보안모듈에 대한 신뢰성이 확보되지 못하면 DCAS용 CAS 모듈을 제공할 수 없다는 입장이다. 방송통신위원회에서도 보안모듈과 관련하여 'ISO/IEC 19790(FIPS 140-2)' 레벨 3 이상의 인증을 받거나 'ISO/IEC 15408(CC EAL 4+)'에 준하는 보안 요구사항을 만족해야 한다는 규정을 넣고자하고 있다[10].

한편, 표준화시 PolyCipher의 DCAS 아키텍처를 따를 경우 IPR과 관련하여 향후 대책이 필요할 것으로 예상되며, 아키텍처에 대한 IPR 문제는 정부 주도하에 대응책을 마련해 줘야 할 것이다.

V. 결론 및 향후 전망

지금까지 정부의 CableCARD 유예에 따라 국내 디지털 케이블 사업자와 CAS 관련 업체들이 소프트웨어기반 CAS와 Embeded CAS 그리고 DCAS 등을 대안으로 고려하고 있으며, 이 중에서도 서비스 확장성과 비용절감, CAS Vender 종속성, 그리고 CableCARD 분리에 대하여 법적대응이 가능한 DCAS 기술이 대안으로 고려되고 있는 것을 확인할 수 있었다. 또한, CAS 국산화와 더불어 기존에 CAS가 설치된 STB과 병행하여 서비스를 할 수 있는 DVB의 SimulCrypt 기술과 DCAS 기술이 고려되고 있는 것도 확인할 수 있었다.

그리고 현재 대안으로 제시되고 있는 DCAS 기술과 SimulCrypt 기술에 대하여 살펴보았으며, DCAS 기술에 대한 국내외 기술동향과 국내외 표준화 동향을 살펴보았다. 국외의 경우 FCC가 케이블 업계의 보안모듈 분리 의무화 유예 요청을 거부한 것과 관련하여 표준화 작업이 중단된 것을 확인할 수 있었으며, 국내의 경우 국외와 다르게 표준화가 정부의 주도하에 2009년 상반기부터 이루어질 것으로 예상된다.

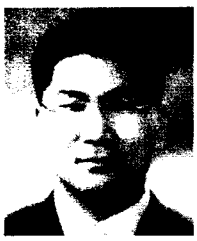
국내 표준화과정에서 여러 쟁점사항 중에 보안모듈이 핵심 쟁점으로 논의되는 것을 확인할 수 있었고, 보안모듈에 있어서 소프트웨어 기반의 보안모듈과 하드웨어 기반의 보안모듈이 논의되고 있는 것을 확인할 수 있었고, 보안모듈은 일정수준 이상의 보안성을 보장받아야 하는 것을 확인할 수 있었다.

향후 DCAS 기술의 상용화를 위해서는 기술의 완전성 및 안정성이 보장되어야 하며, DCAS 기술에 대한 표준화에 앞서 표준과 관련한 IPR 조사가 선행되어야 할 것이다. 그리고 정부의 강력한 정책추진과 케이블 사업자의 도입의지 및 도입 시 발생하는 비용의 적정성 등이 병행되어야 할 것이다.

참 고 문 헌

[1] "케이블TV, 임대형 셋톱 CAS분리 의무 유예", 아이뉴스, 2008.12.17
[2] 유선방송국설비등에관한기술기준, 방통위고시_제2008-35호, 방송통신위원회, 2008.5.19
[3] 디지털유선방송송수신정합표준, TTAS.KO-07.0020/R4, TTA, 2008.12.19
[4] OpenCable Specification, CableCard Interface 2.0 Specification, Cable Television Laboratories, Inc., Jan. 2008
[5] "CAS • DCAS • 사이멀크립트", 디지털타임즈, 2008.10.01
[6] "Digital Video Broadcasting(DVB) Head-end implementation of DVB SimulCrypt", ETSI TS 103 197 V1.4.1, ETSI, Dec. 2004
[7] http://www.lightreading.com/document.asp?site=cdn&doc_id=155749
[8] "NGNA Plan: Integrated Multimedia Architecture", NGNA LLC, 26 July 2004
[9] http://www.opencable.com/downloads/DCAS_New.pdf
[10] "DCAS 표준안 보안 인증 방식 놓고 논란", 아이뉴스, 2008.11.07

필 자 소 개



김 영 모

-2005년 : 대전대학교 컴퓨터공학과 졸업(공학석사)
-2005년 ~ 2006년 : 한국IP보호기술연구소 선임연구원
-2006년 ~ 현재 : (주)디지캡 기술연구소 사업3팀 과장
-주관심분야 : Conditional Access System, Digital Right Management, Digital Forensics

고 병 수

- 2004년 : 대전대학교 컴퓨터공학과 졸업(공학박사)
- 2004년 ~ 현재 : (주)디지캡 사업3팀 팀장
-주관심분야 : Conditional Access System, Digital Right Management, Access Control, Digital Forensics