# 차세대 방송통신 융합서비스를 위한 Security 기술개발 동향

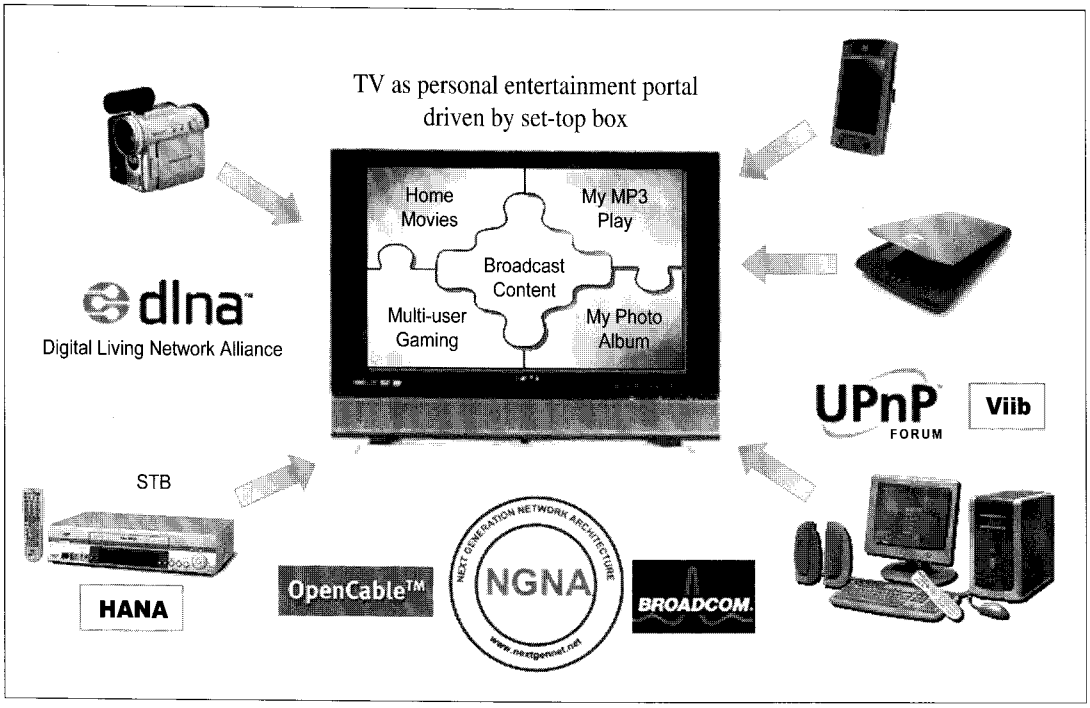
□ 홍인화, 이석필, 박병하, 김찬규, 이상원 / 전자부품 연구원 디지털미디어 연구센터

## Ⅰ. 개 요

최근의 방송, 통신 서비스 분야의 주된 화두는 방송컨텐츠를 기반으로 한 방송통신 융합서비스의 제공에 있다. 방송통신 융합서비스의 주도권을 확보하기 위해 방송사업자, 통신 사업자, 가전사, PC 업계는 각자의 장점을 살려 방송통신 융합 서비스를 제공하기 위한 표준화, 기술개발에 주력하고 있다.

〈그림 1〉에 나타낸 바와 같이 방송사업자의 경우 거대 케이블 방송사업자를 중심으로한 NGNA (Next Generation Network Architecture) 표준에서는 광대역 엑세스망 제공을 위한 기술(DOCSIS 3.0), 다양한 미디어 포맷을 지원하기 위한 미디어 코덱 기술(H.264/VC-1/MPEG-2 동시지원), 방송통신 복합 Security 기술(Downloadable Security), 방송통신 복합 미들웨어 기술이 핵심을 이루고 있다.

미국의 MS, 인텔주도의 UPnP 표준의 경우는 PC를 기반으로한 홈네트워크에서의 미디어 기기의 검색 및 연결, 홈네트워크에서의 미디어 데이터의 소비와 관련된 기술들을 정의하고 있으며, DLNA의 경우는 일본의 가전사(소니, 마쓰시다 등)를 중심으로 홈네트워크에서의 다양한 이종 미디어 기기 간의 컨텐츠 소비를 위한 검색, 연결, 네트워크, 코덱 등에 대한 기술을 정의하며, 인텔주도의 Viib의 경우는 인텔 프로세서를 기반으로 홈네트워크 에서의 이종 미디어 기기간의 컨텐츠 소비를 위한 기술들을 정의한다. 또한 삼성전자 주도의 HANA 표준의 경우는 TV에 IEEE 1394 네트워크를 연동하여 홈 네트워크 에서 이종 미디어 기기간의 컨텐츠 공유, 검색, 소비를 위한 핵심기술을 정의한다. 이같이 최근의 홈 네트워크를 기반으로 한 방통융합 서비스의 주된 흐름은 방송 컨텐츠를




〈그림 1〉 홈네트워크 기반 홈미디어 서비스 표준화 동향

비롯한 미디어 컨텐츠를 다양한 미디어 기기에서 원활하게 소비할 수 있도록 하는 것이 핵심으로 대두되고 있다. 이를 위해서는 크게 3가지 핵심기술이 요구된다.

첫 번째는 다양한 미디어 기기에서 다양한 미디어 컨텐츠의 소비를 위한 미디어 변환기술, 두 번째는 방송통신 융합 환경에서의 컨텐츠의 안전한 소비를 위한 방통융합 Security 기술, 세 번째는 홈네트워크 환경에서의 방송 컨텐츠, 개인저작 컨텐츠, 공유 컨텐츠, 저장매체 기반 컨텐츠 등 다양한 컨텐츠의 손쉬운 소비를 위한 지능형 사용자 인터페이스(I-GUI) 기술이다.

본 논문에서는 이중에서 방통융합 Security 분야를 다루고자 한다.

## II. 컨텐츠 보호기술

미디어 컨텐츠의 사용에 있어서 최근에 가장 중요시되고 있는 분야는 컨텐츠 지적재산권 보호 분야이다. 컨텐츠 보호 기술의 경우 크게 방송분야에서 다루고 있는 CAS(Conditional Access System) 기술과 통신분야(PC)에서 다루고 있는 DRM(Digital Right Management)분야로 나뉘며, 최근의 경우 방통융합 서비스가 핵심 쟁점으로 대두됨에 따라 이 두 기술을 융합한 CAS-DRM 연동 Security 기술이 핵심으로 부각되고 있다.

〈표 1〉에서는 분야별 컨텐츠 보호기술에 대한 정의를 나타내고 있다.

〈표 1〉 컨텐츠 보호기술

| 보호 기술 분야 | 설 명 | 비 고 |
|---|---|---|
| DRM<br>(Digital Rights Management) | - 디지털 콘텐츠및 전 유통 과정을 대상<br>- 디지털 콘텐츠 저작권의 보호 및 유통 관리<br>* 다양한 권한제어/포맷 지원<br>* 다양한 콘텐츠 유통 모델 지원 | - 표준 기술 부재<br>- 상호호환성 거의 불가능 |
| CAS<br>(Conditional Access System) | - 방송 서비스/콘텐츠 보호/제어를 대상<br>- 수신 자격이 있는 시청자에게 프로그램 수신 권한 부여<br>- 유료 디지털 방송 서비스/적용 사례가 풍부함<br>- 구체적인 표준 규격 정의됨. | - 방송 서비스/콘텐츠에 제한 |
| Copy Protection | - 디바이스간 전송되는 디지털 콘텐 츠의 불법 복제 방지 기능<br>- 기록장치로 저장되는 콘텐츠의 불법 복제 방지 | - 제한된 범위<br>- 독립된 기능/제품 |

## Ⅲ. 매체별 Security 기술동향

미디어 컨텐츠를 대상으로 한 플랫폼 사업자는 크게 기존의 방송 사업자와 최근 새롭게 대두되고 있는 IPTV와 이동방송(DMB) 사업자로 구분할 수 있다. 이들 사업자가 추구하는 핵심 사업모델은 방송컨텐츠를 기반으로 하기 때문에 플랫폼별 컨텐츠 Security의 기술동향을 고찰해봄으로써 차세대 방통융합 Security의 발전방향을 가늠해 볼 수 있을 것이다.

### 1. 방송 사업자

■ 케이블 방송 사업자의 경우 세계 최대의 시장을 형성하고 있는 미국과 미국의 차세대 표준을 세계 최초로 채택, 상용화 서비스하고 있는 한국의 경우를 분석해 보았다. 미국의 경우는 현재는 Motorola, SA의 전용 CAS 사용 중에 있으며, OpenCable에서 표준으로 정의한 Cable Card를 수십만 가입자에게 적용 시범서비스를 실시하고 있으나 가격 부담으로 인해 Embedded CAS에서 Downloadable-CAS로의 전환을 준비하고 있으며, 이를 위한 기술개발 및 사업자 플랫폼에서의 안전성 검증을 수행하고 있다. 한국의 경우는 개방형 표준인 OpenCable 규격을 세계최초로 상용화 서비스 중에 있으며, 이 규격을 기반으로 Cable Card를 상용화 플랫폼에 적용 서비스 중에 있다. 그러나 한국의 경우도 Cable Card의 가격부담으로 인해 D-CAS의 상용모델 출시 전까지 과도기적으로 Cable Card 와 Embedded CAS의 병행 사용을 심각하게 고려하고 있다. 또한 D-CAS를 조기에 상용화하기 위한 연구개발 노력을 병행하고 있다.

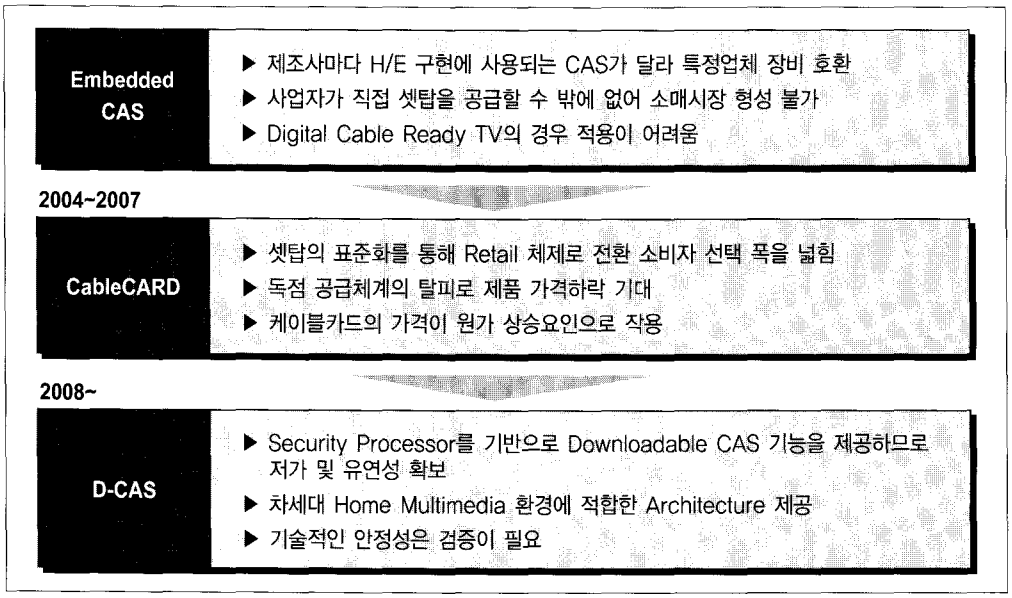
■ 위성방송 사업자의 경우는 현재까지 대다수의 사업자가 NDS, Nagra, Iredeto 등 거대 미디어 기업의 Embedded-CAS 솔루션을 채택 서비스 중에 있다. 현재 CAS 시스템의 경우는 방송장비(Headend), 어플리케이션, 단말을 하나의 솔루션에서 제공하므로 방송사업자도 CAS 업체 영향력 하에 놓여 있으므로 케이블 방송사업자가 추진하는 D-CAS에 많은 관심을 가지고 있으며 이의 상용화시 D-CAS 시스템으로의 큰 변화가 예상된다.

■ IPTV의 경우 신규 서비스 이고, Security 시스템의 기술 표준규격의 부재로 다양한 신규 보호 기술 요구 및 출현 가능성이 높으나 주된 흐름은 방송 서비스가 주된 사업모델 이므로 기존의 CAS 솔루션 채택 상용화 및 상용화 준비를 하고 있다.

■ Mobile Broadcast의 경우 국내에서 추진 중인 DMB 표준과 유럽의 DVB-H 표준에서 독자표준화를 추진중에 있다. 국내 위성 DMB(DMB-S)의 경우 DVB Common Scrambling(TS-Level Scrambling), DVB SimulCrypt 서버 규격을 이용 Iredeto사의 Embedded CAS와 국내 개발 Mobile-CAS를 병행 사용 중에 있다. M-CAS의 경우 국내 최초의 상용서비스 적용 CAS 시스템으로 향후 다양한 미디어 플랫폼 분야에서 사용이 기대된다. 지상파 DMB-T의 경우는 ETSI TS 102 367 "DAB; Conditional access" V1.2.1 규격으로 표준화가 진행중이며, 지상파 DMB의 유료서비스 정책에 맞물려 상용화가 진행될것으로 예상된다. 국내에서 먼저 상용화가 시작된 DMB와 달리 유럽은 독자 표준인 DVB-H 규격 표준화 및 상용서비스를 준비중에 있다. DVB-H의 Security 표준의 주요내용은 "IP Datacast over DVB-H: Service Purchase and Protection"(DVB Doc A100), Protection: IPsec, ISMACryp, Secure RTP, Key Mgmt, Right Format and Mgmt 기술에 대하여 구체적 명시를 하고있다.

## Ⅳ. 케이블 방송 사업자의 Security 발전단계

디지털 위성방송과 함께 양대 유료방송 서비스




〈그림 2〉 케이블 방송 사업자의 Security 발전단계

플랫폼 사업자인 케이블 방송 사업자는 Security 분야에서 가장 앞선 사업자로 평가받고 있으며 미디어 Security 분야를 선도하고 있다. 케이블 방송 사업자의 Security 발전단계를 분석하면 차세대 방통융합 Security의 발전단계를 예측할 수 있다.

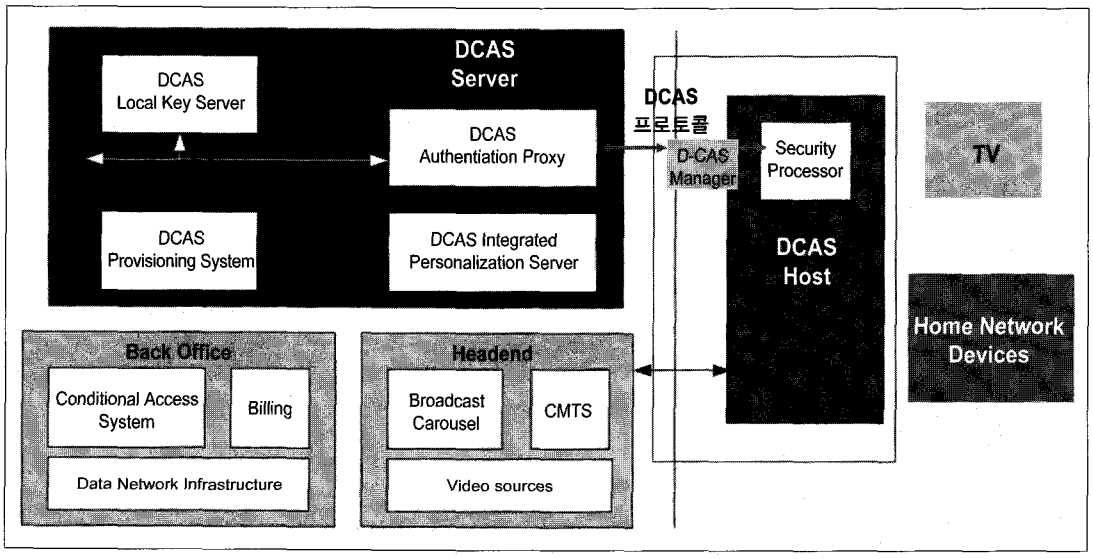
〈그림 2〉에 케이블 방송 사업자의 Security 발전단계를 나타내었다.

〈그림 2〉에서 나타낸바와 같이 미국의 케이블 방송 사업자들은 초기 임베디드 CAS에서 특정 CAS 업체에의 종속을 탈피하기 위해 Cable Card 도입을 추진하였으나 Cable Card의 가격부담으로 인해 D-CAS의 도입을 추진 중에 있다. D-CAS의 도입의 기본 목적은 미국의 경우 일반 TV 시청가구의 가구당 TV 보유 댓수가 4대에 이르므로 디지털 서비스의 활성화를 위해서는 저렴한 가격의 STB 보급이 필수적으로 요구되고, 방송 사업자의 다양한 서비스 발굴에 필요한 CAS 시스템 채택의 유연성 및 홈 네트워크 기반 미디어 서비스로의 확장을 위한 CAS-DRM 연동을 통한 확장성이 요구된다. 따라서 이를 만족하는 차세대 Security 시스템의 표준과 기술개발을 위해 NGNA에서 표준화와 거대 케이블 방송 사업자인 컴캐스트를 중심으로 D-CAS 기술개발 및 사업화 적용이 추진되고 있다.

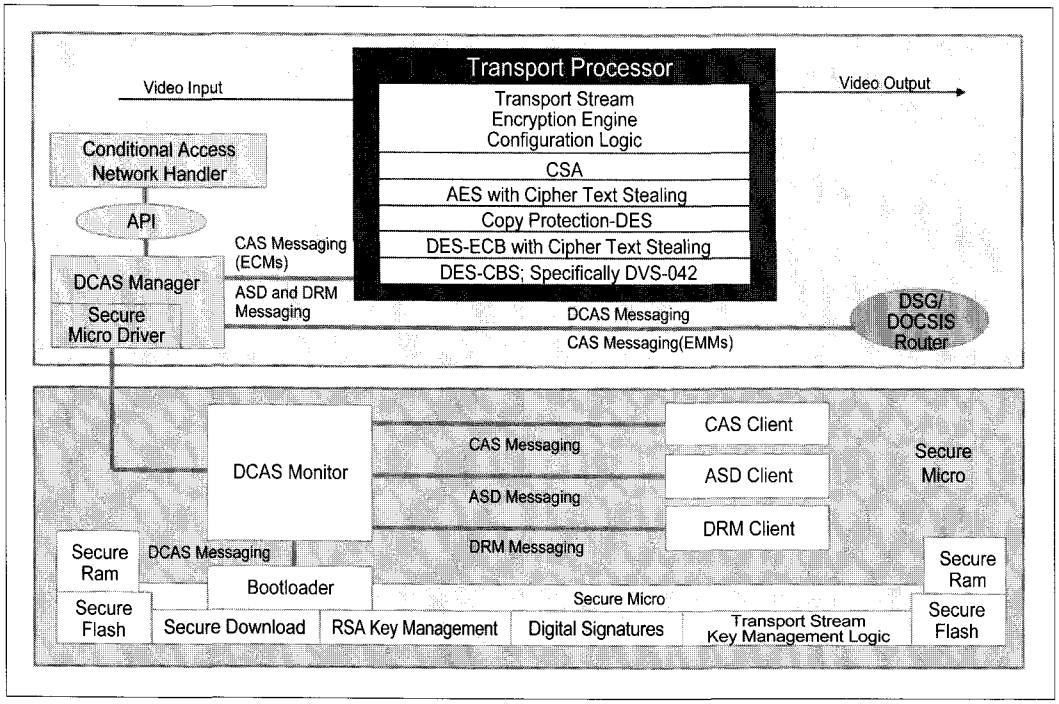
## V. D-CAS 기술

D-CAS는 가입자의 STB 또는 일체형 TV에 하드웨어 CAS 모듈을 별도로 두지 않고 사업자가 S/W CAS를 가입자에게 바로 다운로드 시켜 유료 디지털 방송을 시청할 수 있도록 하는 새로운 수신 인증 기술이다.

아래그림은 D-CAS 시스템에 대한 전체 구성도를 나타내고 있다.




〈그림 3〉 D-CAS 시스템 구성도

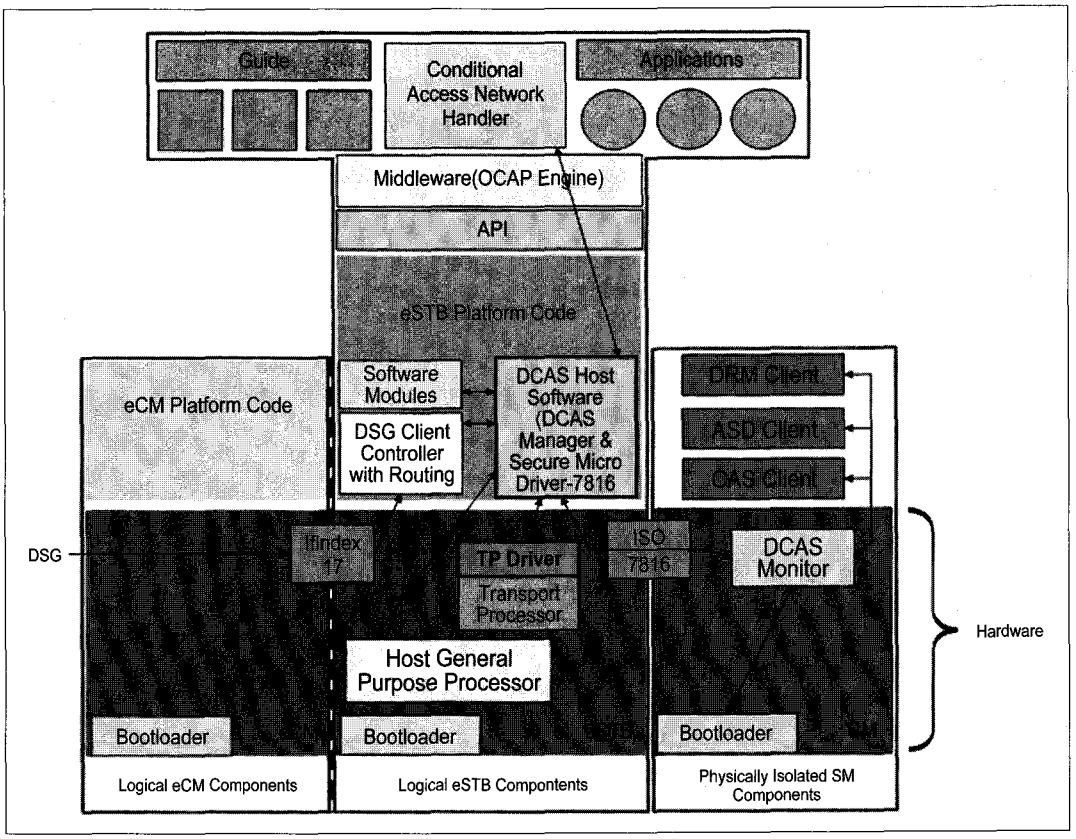



〈그림 4〉 D-CAS 시스템 단말측 구성도

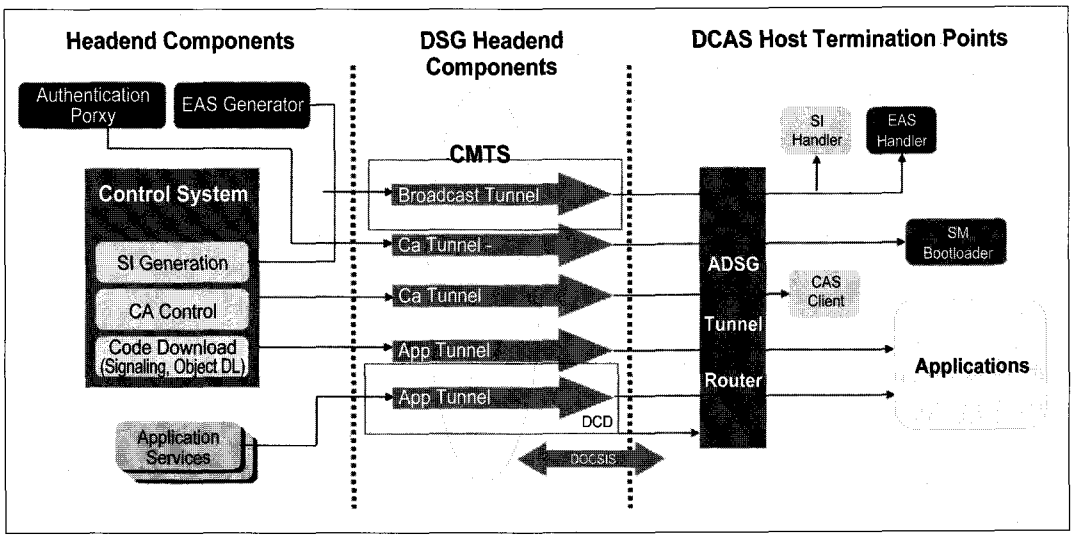
D-CAS 시스템의 전체 구성은 방송장비인 D-CAS Headend 부와 STB에 내장되는 D-CAS Host부로 나뉘어 진다. D-CAS Headend의 경우 기존의 CAS System Headend와 다양한 CAS System을 수용할 수 있는 D-CAS Server로 구성된다.

D-CAS Host부의 경우는 그림 4의 블록도와 같이 Descrambling, Encryption, Copy Protection 기능을 담당하는 Transport Processor칩 과 CAS, DRM Client의 Download와 D-CAS 운영을 담당하는 Secure Micro 칩의 H/W 블록과 서버와의 Networking, TP 칩과 Secure Micro와의 인터페이스 및 D-CAS 운영을 담당하는 D-CAS Manager S/W 블록으로 구성된다. 그림 5의 경우는 D-CAS Host 부를 STB 관점에서 바라본 구성도이다.

디지털 케이블 환경이 다른 미디어 플랫폼과의 가장 큰 차별점은 DSG( DOCSIS Service Gateway) 기능을 이용하여 다양한 양방향 어플리케이션을 구현하기 위한 리턴채널을 구축한 점이다. 그림 6에 나타낸바와 같이 기존의 초고속 인터넷 서비스를 위해 DOCSIS CM기능, EPG 데이터(OOB-SI)의 전송을 위한 Broadcast tunnel, CAS/DRM Client 이미지의 다운로드를위한 CA Tunnel, CAS 운영을 위한 CA Tunnel, 응용서비스를 위한 Application Tunnel로 구성된다. 이런 독립적 DSG Tunnel들을 활용하여 다양한 양방향 서비스 구현 및 Flexible 한 Security 시스템 구성이 가능해진다.




〈그림 5〉 D-CAS 시스템 단말 블록도




〈그림 6〉 D-CAS 시스템 기능 구현을 위한 Networking 구성도

## Ⅵ. D-CAS 표준화 및 구현현황

D-CAS 표준화 추진은 NGNA, CableLabs, MSO에 의해 규격 초안이 작성되어 CableLabs와 D-CAS NDA를 맺은 업체에 공개되어 여러 업체에 D-CAS System 구현 중에 있다. 현재까지 배포된 D-CAS 표준 규격은

- OC-TR-DCAS-D01-060206 : DCASTM System Overview Technical Report
- OC-SP-HOST2.5-CFR-D01-060206 : Host Device 2.5 Core Functional Requirements
- OC-SP-DCAS-CP-D01-060206 : DCAS Content Protection Specification

이며, 향후 CableLabs 에서 관련 업체의 의견을 수렴 표준화 과정을 거쳐 최종 규격을 발표할 예정이다. 또한 현재까지 D-CAS 시스템을 구현한 사례로는

- SA, 모토롤라, 나그라비전이 FCC에 D-CAS 기술 시연 ('05. 7월)
- SA와 모토롤라간 상호동작 시연 ('05. 11월)
- 삼성전자 : D-CAS 방식 STB 시연 (워싱턴, '05. 11)
- LG전자 : '2006 CES'에서 컴캐스트, 나그라비전, Infeneon과 공동 D-CAS 시연 ('06. 1월)

하였으며, 향후 주요 추진일정으로는 D-CAS 핵심 장비 구조설계 및 온라인화를 '06년, D-CAS 관련 Chip set 제작 및 망 개발을 '07년, 장비 테스트 및 소매시장 상용화를 '08년 상반기를 목표로 기술개발을 추진 중에 있다.

## Ⅶ. 결 론

서론부에서 언급했듯이 방송 컨텐츠를 중심으로 한 방통 융합 서비스의 흐름은 거스를 수 없는 대세가 되었다. 방통 융합서비스의 실제 상용화 성공의 Key는 방통융합 Security 기술의 확보에 달려있다 해도 과언이 아니며 기존의 방송강국인 미국과 유럽 등은 이를 위한 방송사업자, Security 기업이 공동으로 관련 시스템 개발에 박차를 가하고 있다. 한국의 경우도 다행스럽게 최근에 방통 융합 Security의 핵심인 CAS 시스템의 자체기술 확보 및 상용화 레퍼런스를 확보하였다. 또한 한국의 경우는 여러 가지 미디어 플랫폼의 세계 최초 상용화 및 시범 서비스 적용국가로 방통융합 Security 기술개발의 최적의 환경을 갖추고 있다. 따라서 연구소, 사업자, 관련기업이 공동으로 차세대 방통융합 Security 기술 개발을 통해 관련기술을 확보하는 것이 매우시급하고 중요한 현안이 되었다.

### 참고문헌

[1] Next Generation Network Architecture Vendor Forum October 13th,2004, Denver, CO
[2] Next Generation Network Architecture LLC 26 july 2004
[3] OC-TR-DCAS-D01-060206 : DCASTM System Overview Technical Report
[4] OC-SP-HOST2.5-CFR-D01-060206 : Host Device 2.5 Core Functional Requirements
[5] OC-SP-DCAS-CP-D01-060206 : DCAS Content Protection Specification
[6] CableHome 1.1 Specification : CH-SP-CH1.1-102-030801

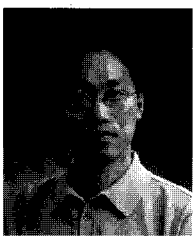
## 필 자 소 개


### 홍 인 화

- 1992년 : 서울산업대학교 전자공학과 졸업
- 1995년 : 숭실대학교 전자공학과 졸업(석사)
- 1990년~현재 : 전자부품연구원 디지털미디어연구센터 SBMS(Smart Broadband Media System) 기술팀장
- 주관심분야 : 디지털방송, 방송통신 융합서비스, 방송통신 융합 Security, 지능형 미디어처리기술

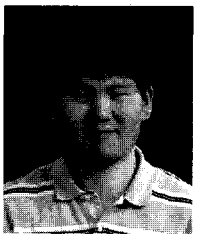
### 이 석 필

- 1990년 : 연세대학교 전기공학과 졸업
- 1992년 : 연세대학교 전기공학과 졸업(석사)
- 1997년 : 연세대학교 전기공학과 졸업(박사)
- 1997년~2002년 : 대우전자 영상연구소 팀장
- 2003년~현재 : 전자부품연구원 디지털미디어연구센터 센터장
- 주관심분야 : 디지털방송, 개인맞춤형 방송, 양방향 멀티미디어서비스, DRM



### 박 병 하

- 1999년 : 세종대학교 전산학과 졸업
- 2001년 : 세종대학교 전산학과 졸업(석사)
- 2001년~현재 : 전자부품 연구원 디지털미디어연구센터 선임연구원
- 주관심분야 : 디지털방송, 유비쿼터스 미디어 서비스



### 김 찬 규

- 1993년 : 안양과학대 졸업
- 1990년~현재 : 전자부품연구원 디지털미디어연구센터 책임연구원
- 주관심분야 : 디지털방송, USN, RTOS, 임베디드 시스템

### 이 상 원

- 1993년 : 단국대학교 전자공학과 졸업
- 1999년 : 단국대학교 대학원 전자공학과 졸업(석사)
- 2006년 : 단국대학교 대학원 전자공학과 졸업(박사)
- 2001년~현재 : 전자부품연구원 디지털미디어연구센터 선임연구원
- 주관심분야 : RTOS, MPEG-2/4, 음성/영상 처리, 인식, DSP, DTV, 임베디드 시스템, USN