情報保護學會論文誌
第 20卷 第 6號, 2010. 12

iCAS 환경의 국내 IPTV 서비스를 위한 인증기관 설립방안에 관한 연구*

최 현 우† , 정 영 곤, 여 돈 구, 염 흥 열‡
순천향대학교

Trust Authority(TA) Establishment Strategy for Domestic IPTV Service in iCAS environment*

Hyun-Woo Choi† , Young-Gon Jung, Don-Gu Yeo, Heung-Youl Youm‡
Soonchunhyang University

요 약

서버로부터 단말로 제한수신시스템을 다운로드 하기 위한 기술인 iCAS(interchangeable CAS) 규격은 사업자간 IPTV 단말의 호환성 및 이동성을 제공한다. 하지만 이와 같은 단말의 이동성을 보장하기 위해서는 규격 내의 생태계(eco-system)에서 키 혹은 인증서를 체계적으로 관리하는 주체인 인증기관(TA)이 필요하게 되는데, 기존 제한수신시스템에서는 솔루션 제공 업체가 인증기관의 역할을 수행했으나 표준화가 되어 단말의 이동성이 제공되기 위해서는 iCAS 기술이 적용된 전체 생태계를 관리하는 단일의 인증기관 설립이 필요하다. 따라서 본 논문에서는 iCAS 상용화를 위한 인증기관 관련 이슈들을 분석하고, iCAS 환경의 IPTV를 위한 인증기관 설립 방안을 제시한다.

ABSTRACT

The iCAS specification that download CAS s/w image from the IPTV provider's server to the IPTV devices provides compatibility and service mobility between the IPTV service providers. However, to ensure mobility of the device, a TA(Trust Authority) within an IPTV eco-system that is capable of systematically managing keys or certificates is required. In the Legacy CAS, solution providers for CAS play a critical role of carrying out the TA. However, in order to standardize the device mobility, a TA should be established by implementing iCAS technology that manages the entire IPTV eco-system including iCAS. In this paper, we analysis TA issues related iCAS commercialization, and propose TA establishment strategy for IPTV service in iCAS environment.

Keywords: IPTV, TA, iCAS

접수일(2010년 9월 25일), 수정일(2010년 11월 22일), 게재확정일(2010년 12월 14일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2010-(C1090-1031-0005))
† 주저자, zemisolsol@sch.ac.kr
‡ 교신저자, hyyoum@sch.ac.kr
§ 방송통신발전기본법 제정에 따라 현행 「인터넷 멀티미디어 방송사업의 전기통신설비에 관한 기술기준」(전파연구소고시 제2008-47, 2008.10.31)을 변경한 개정(안)이 2010년 9월 현재 의견수렴 중에 있음.

I. 서 론

2010년 10월 31일부터 적용되는 인터넷 멀티미디어 방송사업의 방송통신설비에 관한 기술기준 개정(안)[8][4]에는 "① 가입자 제한수신 모듈은 가입자 단말장치와 분리 또는 교환되어야 하고 상호호환이 가능해야 한다. ② 제1항에 따른 제한수신 모듈의 분리 또는 교환과 상호호환에 대한 사항은 한국정보통신기술협회의 'IPTV용 교환 가능한 CAS(iCAS) (TTAK.KO-08.0023)' 표준을 따른다."라는 조항이 명시되어 있다. 이에 한국정보통신기술협회는 지난 2009년 12월에 IPTV 사업자 3사(KT, SK브로드밴드, LG텔레콤)와 합의한 "TTA와 IPTV 사업자간 IPTV 표준화 협약서"의 추진일정 중 1단계(IPTV용 표준 제정)에 해당하는 IPTV용 표준 제정으로써 "IPTV 용 교환 가능한 CAS(iCAS)[1]" 표준을 제정·공고 한 바 있다.

iCAS 규격은 제한수신 모듈을 네트워크를 통하여 IPTV 단말기에 안전하게 다운로드 받고 관리하는 기술로써, 기존 특정 단말에 한정되던 제한수신시스템과 달리 iCAS 프레임워크(Framework)를 적용하는 단말들 간에는 제한수신 모듈의 교환과 상호호환 및 이동성을 보장하도록 하고 있다. 하지만 iCAS 규격이 제한수신 모듈의 호환 및 단말의 이동성을 위한 기술적인 문제를 해결했다 하더라도, 실제 iCAS 상용화를 위해서는 서비스 사업자, 콘텐츠 사업자 그리고 단말 제조업체 등간에 풀어야할 문제가 남아 있다.

그 중 단말의 이동성을 보장하기 위해서 가장 중요한 문제는 IPTV 서비스 규격 내의 생태계에서 키 혹은 인증서를 체계적으로 관리 하는 인증기관의 필요성이다. 기존 제한수신시스템에서는 솔루션 제공 업체가 인증기관의 역할을 수행했기 때문에 서비스 사업자별로 상이한 키 관리 및 인증 체계를 사용해 왔다. 하지만 표준화가 되어 서비스 사업자간 단말의 이동성이 보장되기 위해서는 iCAS 기술이 적용된 전체 생태계를 관리하는 단일의 인증기관 설립이 필요하다.

지난 2010년 8월, 정부 주도하에 구성 및 운영된 IPTV 표준화전담반 산하 TA-TFT는 6차 회의를 끝으로 방송통신위원회에서 인증기관 구축 및 운영에 관련하여 정책, 제도 이슈 검토, 그리고 방안 수립에 활용될 iCAS 표준 적용을 위한 TA 구축 및 운영 계획(안)을 마련했다[10].

본 논문은 TA-TFT 회의를 근거로 하여 iCAS 환경의 국내 IPTV 서비스를 위한 인증기관 설립 방안을 제시한다. 기존 타 표준화 기구의 인증기관 사례에서부터 인증기관의 필요성, 역할, 기능 등에 대해 분석 및 분류하고, 역할 및 운영 주체에 따라 최종 인증기관 설립을 위한 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로써 제한수신시스템 및 iCAS 규격에 대해 살펴보고, 3장에서는 인증기관의 기본적인 사항과 타 표준화 단체의 인증기관 사례, 그리고 국내 IPTV 서비스를 위한 인증기관의 필요성 및 요구사항에 대해 분석한다. 그리고 4장에서 iCAS 환경의 국내 IPTV 서비스를 위한 인증기관의 설립 방안을 분류한 뒤, 5장에서 기존 인증기관과 제안한 방안들을 비교 평가하여 최종 설립방안을 제안한다. 그리고 마지막으로 6장에서 결론을 맺는다.

II. 관련 연구

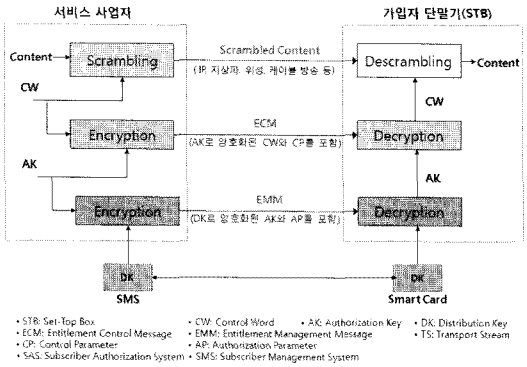
본격적으로 인증기관을 논의하기에 앞서, 본 절에서는 IPTV 서비스의 콘텐츠 보호기술인 제한수신시스템과 제한수신 모듈의 상호호환 및 이동성을 제공하기 위해 개발된 iCAS 표준 규격에 대해 간략히 살펴본다.

2.1 제한수신시스템 (CAS)

제한수신시스템은 과거 아날로그 방송 시절부터 유료 방송 서비스를 위해 방송 서비스에 대한 고객의 접근 여부를 제어하는 기본 시스템으로 사용되어 왔다. 주로 서비스 사업자가 콘텐츠를 암호화(scramble)하여 멀티캐스트 방식으로 전송하면 가입자의 단말기(STB)에서 복호화(descramble)하는 방식으로 사용된다[2]. 따라서 서비스에 가입한 사용자의 단말기만이 암호화된 콘텐츠를 복호화하여 해당 방송 콘텐츠를 시청할 수 있게 된다.

[그림 1]은 제한수신 시스템에서 콘텐츠를 스크램블/디스크램블 하는 과정을 나타낸다. 제한수신시스템은 자격관리메시지(EMM)와 자격제어메시지(ECM)를 사용하여 시청권한이 있는 사용자만이 가입한 채널을 시청할 수 있게 한다. 자격관리메시지와 자격제어메시지는 아래에 기술한 역할을 수행하며, 서비스 사업자의 네트워크에서 사용자의 단말기로 주기적으로 전송된다.

- 자격제어메시지: 채널마다 다른 인증키(AK)로 암호화된 제어단어(CW)와 제어변수(CP)를 포



〔그림 1〕 제한수신시스템 구조

함하고 있다. 자격제어메시지는 가입자의 채널변환에 대응하기 위해 주기적으로 전송되며, 이때마다 제어단어가 새롭게 생성되고 암호화된다.

- 자격관리메시지: 사용자의 단말기에 자격을 부여, 갱신, 관리하는 기능을 한다. 분배키(DK)로 암호화된 인증키와 인증변수(AP) 포함되어 있다. 서비스 사업자와 단말기 간에는 반드시 동일한 분배키를 공유하고 있어야 한다.

서비스 사업자는 콘텐츠를 스크램블하여 IP망 또는 지상파, 위성, 케이블망 등을 통해서 가입자의 단말기로 전송한다. 이때 서비스 사업자의 네트워크에서 콘텐츠를 스크램블하기 위해 사용되는 키를 제어단어라고 하며, 제어단어는 가입자의 단말기에서 스크램블된 콘텐츠를 디스크램블하기 위해서도 사용된다. 제어단어는 인증키에 의해 암호화된 후 제어변수와 함께 자격제어메시지에 포함되고 MPEG-2 전송스트림(TS)과 함께 단말기로 전송된다. 또한 인증키는 서비스 사업자와 단말기가 사전에 공유하고 있는 분배키를 이용해 암호화된 후 인증변수와 함께 자격관리메시지에 포함되어 단말기로 보내지게 된다. 여기서 말하는 분배키는 스마트카드 안에 내장되어 고객 정보를 관리하는 가입자관리시스템(SMS)에 의해서 사전에 가입자에게 배포되어 있는 비밀키를 의미한다.

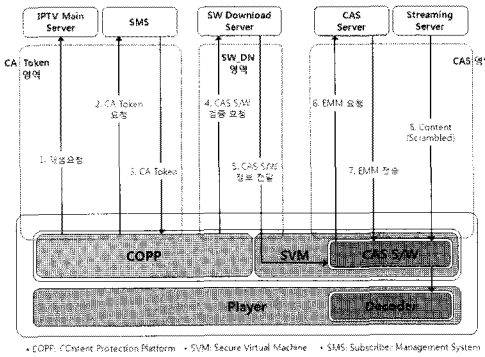
한편, 단말기에서는 수신한 스크램블된 콘텐츠의 디스크램블을 위해 서비스 사업자가 스크램블한 과정을 역으로 수행한다. 먼저, 단말기의 접근제어 모듈은 자격관리메시지의 인증변수와 자격제어메시지의 제어변수를 비교하고, 일치한다면 스마트카드 내에 저장된 분배키를 이용하여 자격관리메시지로부터 인증키를 추출해 낸다. 그 뒤, 추출한 인증키를 이용하여 자격제어메시지에 포함되어 있는 제어단어를 복호화 해낸다. 이렇게 복호화된 제어단어는 스크램블된 콘텐츠를 실시간으로 디스크램블링 하는데 사용된다.

제한수신시스템은 가입자의 시청료 납부에서부터 가입자관리시스템과의 연동을 통해 가입자가 원하는 방송 프로그램의 제공 및 PPV(Pay Per View), VOD(Video On Demand) 등의 부가서비스를 제공할 수 있어, 방송사업자는 과거 광고를 통한 수익모델에서 벗어나 유료방송 사업을 통해 다방면으로 수익을 창출할 수 있게 됐다.

2.2 IPTV 용 교환 가능한 CAS (iCAS)

제한수신시스템은 가입자 단말기 내에 내장된 형태로 존재하거나 또는 케이블카드의 형태로 단말기에 탈착 가능한 방식으로 존재하는 것이 일반적이다. 하지만 이와 같은 제한수신시스템은 단말기와 서비스 사업자에 종속적이고 제한수신 모듈의 교체 및 상호호환이 제공되지 않을 뿐더러 단말의 이동성이 제공되지 않기 때문에 가입자가 서비스 사업자를 변경해야 할 때는 새로운 서비스 사업자를 위한 또 다른 단말을 구입해야 하는 등의 불편함과 추가 비용을 발생시킨다. 따라서 제한수신 모듈과 같은 필요한 보안 기술을 서버로부터 단말로 다운로드 받아 사용하는 형태의 제한수신 시스템을 표준화 하려는 일환으로 나온 것이 바로 IPTV 용 교환 가능한 CAS(iCAS) 표준 규격이다[1].

iCAS는 정부의 제한수신 모듈 분리 의무화 정책에 따라 2008년 8월 규격 개발에 착수하여 2010년 3월 한국정보통신기술협회의 IPTV 보안 실무반(WG-2194)에서 최종 표준으로 제정되었다. iCAS 표준에서는, IPTV에서 제한수신 모듈을 네트워크를 통하여 안전하게 다운로드 받고 관리하기 위한 필요 요구사항



〔그림 2〕 IPTV 용 교환 가능한 CAS(iCAS) 시스템 구조[1]

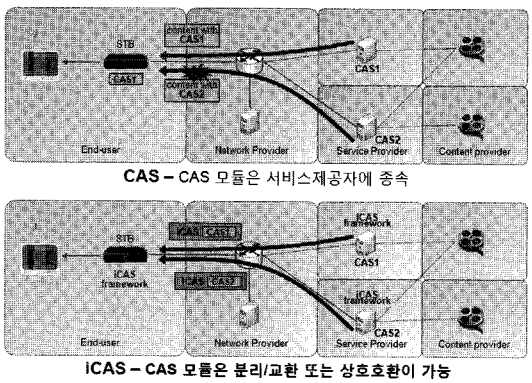
들을 정의하고, 이를 만족시키기 위한 세부 기술들을 포함하고 있다. 세부 기술로는, 제한수신 모듈을 안전하게 다운로드 받기 위한 서버와 IPTV 단말과의 프로토콜과, 다운로드 받은 서비스 및 콘텐츠 보호 기술을 안전하게 관리하고 실행시키기 위하여 IPTV 단말에서 필요한 컴포넌트들을 정의하고 있다. [그림 2]는 iCAS 시스템의 구조를 보여준다.

[그림 2]에서와 같이 iCAS 규격에서는 단말의 콘텐츠 획득을 위해 세 개의 영역인 CA Token 영역, SM_DN 영역, 그리고 CAS 영역으로 각 영역을 구분하고 각각의 단계를 정의했다. 각 단계에 대한 구체적인 설명은 다음과 같다.

① 서버와 단말의 인증을 통해 CAS SW의 다운로드 권한을 획득하는 단계 (CA Token 영역)
② 인가된 단말에 한해 안전하게 보호된 형태로 CAS SW를 내려주는 단계 (SW_DN 영역)
③ 내려 받은 CAS SW를 안전하게 저장하고 실행하는 단계 (CAS 영역)

특히, ③의 단계는 가상머신(Virtual Machine, VM) 개념을 이용하여 CAS SW가 하드웨어에 독립적이게 동작가능 하도록 하고 있으며, 다운로드 된 CAS SW는 로딩 되어 사용될 때를 제외하고는 암호화된 형태로 단말에 저장되어 있게 했다.

[그림 3]은 기존 제한수신시스템과 iCAS를 비교한 그림이다. 그림과 같이 제한수신시스템에서는 단말에 탑재된 제한수신 모듈이 서비스 사업자에 종속적이지만, iCAS에서는 제한수신 모듈이 서비스 사업자로부터 가입자 단말로 다운로드 가능하기 때문에 제한수신 모듈의 분리/교환 또는 상호호환이 제공된다.



[그림 3] CAS/iCAS 비교

iCAS 표준은 향후 상용 서비스 적용에 따른 문제점 해결의 일환으로 IPTV사업자/IPTV산업체/ETRI/TTA 등 13개 참여업체들로 결성된 iCAS 컨소시엄을 통해 iCAS 표준에 대한 참조구현 개발 및 상호운용성을 시험 중에 있으며, 2010년 10월 31일부터 적용될 예정인 「인터넷 멀티미디어 방송사업의 전기통신설비에 관한 기술기준 개정(안)」에서는 제한수신 모듈의 분리 또는 교환과 상호호환을 위해 IPTV 사업자가 따라야 할 표준으로써 iCAS를 명시해 놓고 있다.

III. IPTV를 위한 인증기관(TA) 이슈

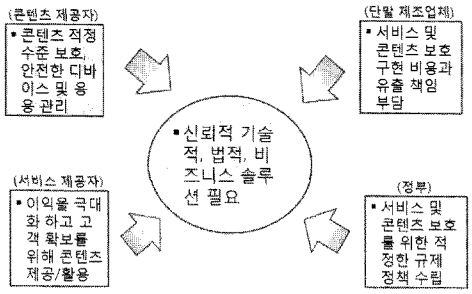
제한수신 모듈을 교체 및 상호호환 가능하게 하는 기술인 iCAS 표준 규격이 마련됐다 하더라도, 실제 서비스 사업자간 단말의 이동성이 보장되기 위해서는 동일한 생태계 내의 단말들을 인증해 주는 단일 체계의 인증기관이 필요하다. 본 절에서는 인증기관의 기본적인 사항과 타 표준화 기구에서의 인증기관 사례를 살펴보고 국내 iCAS 환경의 IPTV를 위한 인증기관의 필요성과 요구사항을 분석한다.

3.1 인증기관 기본사항

인증기관은 DRM(Digital Right Management) /Security 관련 표준 규격을 사업화하기 위해 필요한 보안 이슈들을 담당하는 기구 혹은 기업이다. 특히, 특정 규격 내의 콘텐츠 생태계 범위 내에서 안정적으로 인증서 및 키 관리를 체계적으로 관리하는 역할 등을 수행한다. 여기에서 말하는 콘텐츠 생태계란 특정 사업자 등의 물리·기술·정책 환경 내에서 콘텐츠가 생성되고 유통되고 소비되는 단계에 있어 여러 참여 주체들이 함께 이익을 공유하는 상생시스템을 의미한다. [그림 4]는 콘텐츠 보호 생태계에서 각 참여 주체들의 역할을 나타내며, 결국 신뢰적, 기술적, 법적, 비즈니스 솔루션의 필요성은 인증기관의 필요성을 의미 한다고 할 수 있다.

인증기관은 앞서 언급한 키 혹은 인증서 체계의 관리 이외에도 아래에 기술된 바와 같이 다양한 기능 및 역할을 가질 수 있다.

• 콘텐츠 제공자가 만족할만한 강인성 규정(Robustness Rule) 및 준수 규정(Compliance



〔그림 4〕 콘텐츠 보호 생태계[9]

Rule) 제정/유지/관리

- 콘텐츠 제공자, 사업자, 기기제조사 간의 라이센스 협약서(License Agreement) 작성 및 어답터(Adopter)와 계약 체결을 통한 법적 구속력 확보
- 콘텐츠 제공자 (예, 헐리우드 스튜디오들)에 대한 홍보 및 승인 획득
- 기기 기술 및 활용에 대한 사후 감사
- 필요시 기기 및 규정 인증

3.2 타 표준화기구의 인증기관 사례

타 표준화기구에서는 동일 규격을 사용하는 멤버들이 모여 과세 혜택 및 개인적 책임으로부터 보호를 받을 수 있는 유한책임회사(Limited Liability Company, LLC) 형태로 인증기관을 설립하는 것이 일반적이다. 다음 〔표 1〕은 대표적인 타 표준화기구의 인증기관 운영 사례이다.

CMLA는 OMA DRM 또는 OMA/DVB-H 규격의 대응을 위한 목적으로 인텔, 노키아, 파나소닉, 삼성에 의해서 2004년에 설립됐다. 1년의 준비 기간이 있었으며 Cost Recovery Based 즉, 이윤을 추구하지 않고, 상주 직원이 존재하지 않는다. CMLA의 주요 활동으로는 CMLA 기술 규격의 이행, 신뢰 모델(Trust Model) 관리, 상업적 라이선스 제공, 강인성 및 준수 규정을 포함하는 CMLA 협약서(Agreement) 작성, 그리고 6여개의 헐리우드 스튜디오(Hollywood Studio)들을 대상으로 하는 콘텐츠 제공자 승인 등이 있다[5].

다른 예로, Marlin DRM 기술을 위해 상업적 라이센스를 승인하는 운용기구로써, 2005년에 인터트러스트, 파나소닉, 필립스, 삼성, 소니 등 5개사의 Marin 설립자에 의해 만들어진 MTMO가 있다. MTMO의 주요 역할로는 비 특허 지적재산권 승인, 키 관리 및 인증서 서비스 제공, 강인성 및 준수 규정 제공, 그리고 갱신(Renewability) 서비스 운용 등이 있다[8].

그 외에도, DTCP 규격을 위해 1999년 인텔, 히타치, 파나소닉, 소니, 도시바 등 5개사에 의해 설립된 DTLA[6]가 있으며, AACS 규격의 대응을 위해 IBM, 인텔, 마이크로소프트, 파나소닉, 소니, 도시바, 월트 디즈니, 워너브라더스 등 8개사에 의해 2004년에 설립된 AACSLA가 있다[7].

이상에서 살펴본 타 표준화 기구의 인증기관 사례에서는, 공통 기능으로써 키 발급 및 인증서 발급 기능을 가지고 있으며, 특히, 콘텐츠 유출과 같은 사고가 발생할 시에 책임으로부터 보호를 받을 수 있는 별도의 페이퍼 회사(Paper Company) 형태로 인증기관을 설립하는 경우가 일반적이다.

〔표 1〕 타 표준화 단체의 인증기관 운영 사례[3]

규격	OMA	DTCP	AACS	Marlin
기술규격 제정/유지	OMA	DTLA[6]	AACSLA[7]	MDC
Trust Management	CMLA[5]/others	DTLA	AACSLA	MTMO[8]
Robustness Rule	CMLA/others	DTLA	AACSLA	MTMO
Compliance Rule	CMLA/others	DTLA	AACSLA	MTMO
License Agreement	CMLA/others	DTLA	AACSLA	MTMO
Studio Promotion	CMLA/others	DTLA	AACSLA	MDC & MTMO

·OMA: Open Mobile Alliance ·CMLA: Content Management License Administrator
·DTCP: Digital Transmission Content Protection ·DTLA: Digital Transmission Licensing Administrator
·MDC: Marlin Developer's Community ·MTMO: Marlin Trust Management Organization
·AACSLA: Advanced Access Content System Licensing Administrator

3.3 iCAS 환경의 국내 IPTV 인증기관 필요성

기존 국내 IPTV 서비스에서는 서비스 사업자 마다 독자적인 생태계를 가지고 있기 때문에 사업자별로 각기 다른 제한수신시스템과 인증기관을 구축하고 사용해 왔다. 보통 제한수신시스템을 제공한 솔루션 업체가 인증기관의 역할을 수행하며, 인증기관의 주요 기능으로는 IPTV 단말에 대해 키 혹은 인증서를 발급하고 관리하는 것이다.

하지만 이동성이 제공되는 iCAS의 경우에는 사업자 모두를 묶는 단일의 인증기관이 필요하다. 단말이 서비스 사업자를 자유로이 이동하기 위해서는 서비스 사업자들과 단말들은 동일한 iCAS 표준 기술을 수용해야 한다. 키 혹은 인증서 발급과 관리 또한 단일의 체계를 따라야 하며, 이 체계를 만들고 관리하는 것이 바로 단일의 인증기관이 되어야 한다. [그림 5]는 기존 제한수신시스템에서의 인증기관과 표준의 iCAS 시스템에서의 인증기관 형태를 비교한 그림이다.

[그림 5]에서, 기존 제한수신시스템에서는 3개의 서비스 사업자가 각각 다른 종류의 제한수신시스템과 인증기관을 사용하고 있기 때문에 IPTV 단말들 간에 호환이 되지 않는 반면, 다운로드 가능한 제한수신시스템인 iCAS 시스템에서는 3개의 사업자가 각각 다른 종류의 제한수신시스템을 사용하더라도 공통의 인증기관을 이용하고 있기 때문에 IPTV 단말의 호환성 및 이동성을 보장받을 수 있다.

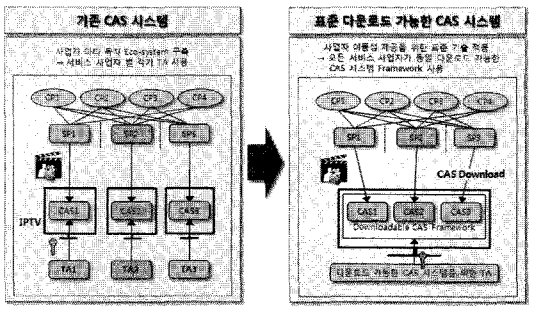
IPTV 서비스를 위한 키 혹은 인증서를 발급하고 관리하는 역할 이외에도 인증기관은 3.1절에 언급한 다양한 기능을 제공할 수 있다. 특히, 헐리우드 콘텐츠를 수급하기 위해 할리우드 스튜디오들을 상대로 하는 홍보 및 승인 절차에서 인증기관은 매우 유용하다고 할 수 있다. [그림 6]은 헐리우드 인증을 위한 절차 중, 스펙인증을 받기 위한 절차를 보여준다. 스펙인증이란 표준 규격에 대해 인증을 받는 것을 말하는데, 일반적으로 할리우드 콘텐츠를 수급하기 위해 할리우드 스튜디오들이 요구하는 보안 요구사항을 만족시켜야 하는 절차를 의미한다. 스펙인증에서 솔루션 업체는 할리우드 스튜디오들이 인정하는 보안 감사 회사로부터 자사의 제품에 대한 보안 감사를 수행함으로써 스펙인증을 받게 된다. 기존에는 헐리우드 콘텐츠를 수급하기 위해 서비스 사업자 혹은 제한수신 솔루션 업체 별로 별도로 인증을 받아 운영되었지만, 인증기관이 콘텐츠 수급을 위한 인증 기능을 수행한다면, [그림 6]에서처럼, 인증기관은 할리우드 스튜디오들로부터 보안 요구사항을 만족시키기 위해, 보안 감사 회사로부터 iCAS의 스펙 인증을 받음으로써 헐리우드 콘텐츠를 수급할 수 있게 된다. 인증기관이 콘텐츠 수급 인증 기능을 가지지 않는다면 여러 사업자 혹은 업체 별로 각각 스펙인증을 받아야 하지만, iCAS를 위한 인증기관이 존재한다면 TA가 대표하여 스펙인증 등을 한 번에 수행할 수 있으므로 사업자별로 들어가는 인증 절차와 비용을 절감할 수 있게 된다.

iCAS를 위한 인증기관의 또 다른 필요성은 콘텐츠 유출시 책임을 회피하기 위해서이다. 인증기관은 iCAS의 문제로 인해 콘텐츠가 유출 되거나 보안상 문제점이 발생했을 때, 기존 서비스 사업자나 제한수신 솔루션 업체가 책임을 지는 형태가 아닌 인증기관으로 모든 책임을 제한 할 수 있다는 장점이 있다. 보통 인증기관을 페이퍼 회사 형태로 설립함으로써 모든 책임을 인증기관으로 한정 지을 수 있게 된다.

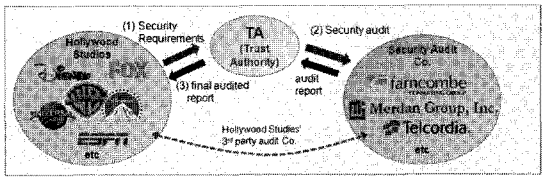
3.4 iCAS 환경의 국내 IPTV 인증기관의 요구사항

3절의 내용을 토대로 하여 iCAS 환경의 국내 IPTV 인증기관이 반드시 필요로 하는 요구사항을 정의하면 다음과 같다.

- 콘텐츠에 대한 종단 간 보안을 보장해야 한다.
- 서비스 사업자간의 IPTV 단말 이동성을 보장해야 한다.



[그림 5] 제한수신시스템과 iCAS 규격의 인증기관 형태 비교[3]



[그림 6] 스펙인증(보안 감사) 절차

- IPTV iCAS 표준 규격을 유지해야 하며, 이 표준을 유지하기 위한 체계를 가져야 한다.
- 인증서 및 키의 발급과 관리의 기능을 가져야 한다.

또한, 인증기관의 필요에 의한 추가적인 요구사항을 정리하면 다음과 같다.

- iCAS 안전성 검증(스펙인증 등) 시 서비스 사업자간의 중복 검사를 방지해야 한다.
- 가능한, 각각의 개별 콘텐츠제공자가 요구하는 법준수 사항을 만족해야 한다.
- 콘텐츠 유출 등 보안상의 문제가 발생할 시에 책임의 경계가 명확해야 한다.

IV. iCAS 환경의 IPTV를 위한 인증기관 설립 방안

타 표준화 기구에 의한 인증기관은 하나의 표준화 기구에서 개발된 콘텐츠 보호 표준이 콘텐츠 보호 전 주기를 포함하기 때문에, 법률 준수, 스펙 인증 등을 인증기관이 콘텐츠 제공자로부터 인증을 받고 난 후, 인증기관이 표준 준수/강인성을 자체적으로 관리하여 보장한다면 콘텐츠 제공자에게 보호 체제의 신뢰성을 제공할 수 있었다[9]. 하지만 국내 iCAS를 위한 인증기관의 경우에는, iCAS가 오직 제한수신 모듈을 다운로드하는 기능만을 담당하기 때문에, 콘텐츠 제공자의 인증을 받기 위해서는 iCAS 부분의 콘텐츠 제공자 인증을 iCAS 인증기관이 받았더라도, 종단 간 보안 감사를 위해서는 제한수신 모듈에 대한 별도의 콘텐츠 제공자 인증 절차와 비용이 필요하게 된다. 따라서 iCAS를 위한 인증기관의 설립 방안은 이와 같이 타 표준화 기구와의 차별점을 염두에 두어 고려되어야 한다.

본 절에서는 IPTV를 위한 인증기관의 설립 방안으로 인증기관의 기능 및 역할에 따른 설립 방안과 인증기관의 운영 주체에 따른 설립 방안으로 구분하여 각각의 방안을 분류 한다. 또한 인증기관이 가져야할 가장 최소한의 기능인 인증서 및 키 관리 체계 방안에 대해서도 논의한다.

4.1 인증기관의 기능 및 역할에 따른 설립 방안

4.1.1 방안1) 인증서 및 키 관리

인증기관이 가져야 할 최소한의 기능은 인증서 및 키 관리 기능이다. 인증서 및 키 관리가 단일의 인증기관을 통해서 이루어 져야만 서비스 사업자간 단말의 이동성이 보장되기 때문이다. 본 방안은 인증기관이 인증서 및 키 관리 기능만을 가지는 형태로써 이 외의 인증기관이 가져야 할 다른 기능들은 사업자 및 업체별로 자율에 맡기는 경우이다. 따라서 헐리우드 콘텐츠 수급 등을 위한 스펙인증과 법률인증은 사업자 및 업체별로 수행하게 되고 콘텐츠 유출 사고 발생 시에 책임은 iCAS 업체 및 제한수신시스템 업체가 분산 책임을 지게 된다.

4.1.2 방안2) 인증서 및 키 관리 + 헐리우드 인증 (스펙인증+법률인증)

본 방안은 인증서 및 키 관리 기능과 할리우드 콘텐츠 수급을 위한 스펙인증 및 법률인증을 인증기관의 기능으로 가지는 경우이다. 따라서 iCAS와 관련하여 콘텐츠 유출 사고가 발생했을 때의 책임은 전적으로 인증기관이 지게 된다. 본 방안은 기존 타 표준화 기구에서 인증기관이 일반적으로 수행하는 역할과 같다고 볼 수 있다.

4.1.3 방안3) 인증서 및 키 관리 + 스펙인증(paper audit)

본 방안은 인증기관이 인증서 및 키 관리 기능과 콘텐츠 수급을 위한 스펙인증 기능만을 가지는 경우이다. 따라서 기타 법률인증 등은 각 사업자 및 업체 별로 자율적으로 수행하게 되고, 콘텐츠 유출에 대한 책임 역시 사업자 및 업체별로 분산하여 지게 된다.

4.2 인증기관의 운영 주체에 따른 설립 방안

4.2.1 방안1) 관심 주체들의 투자로 설립된 별도 회사

본 방안은 표준 규격에 대한 인증기관의 가장 일반적인 형태로써, 관심 있는 주체들이 일정 금액을 투자하여 별도의 회사를 설립하는 경우이다. 별도의 회사를 설립함으로써 콘텐츠 유출 등에 대한 책임을 인증기관으로 제한할 수 있다는 장점이 있다. 별도의 회사 형태로 설립된 인증기관은 직접적인 이윤 추구를 목적으로 하지 않고, 표준 규격을 활용한 사업화 지원에만 목적을 둔다는 특징을 가진다. 3.2절에서 살펴본 타 표준화 기구의 인증기관 사례인 CMLA, MTMO,

DTLA, AACSLA 등이 관심 주체들의 투자로 설립된 별도 회사의 예이다.

4.2.2 방안2) IPTV 서비스 사업자들의 연합

본 방안은 IPTV 서비스 사업자들 간에 공통 생태계를 형성하여 키 발급/관리, 호환성 테스트, 기술 홍보, 구현 가이드라인 등을 주관하는 방법이다. 서비스 사업자들이 연합하여 인증기관을 운영함으로써 서비스 사업자들이 설정한 정책을 추진하기가 쉽다는 장점이 있는 반면, 콘텐츠 유출 등에 대한 책임은 서비스 사업자들이 져야 하는 단점이 있다.

4.2.3 방안3) 공공 기관에서 운영

본 방안은 공공기관에 인증기관의 역할을 부여하는 방법으로써, 정부의 지원 사업 형태로 추진되는 경우이다. 사업 활성화 지원 차원에서 정부가 주도하는 방법이지만, 비용 부담 문제와 잠재적인 책임 등에 대한 위험 부담이 존재하므로 이를 회피할 수 있는 전략이 필요하다.

4.3 인증서 및 키 관리 방안

iCAS를 위해 필요한 인증서는 코드서명 인증서와 디바이스 인증서이다. 코드서명 인증서는 다운로드 될 제한수신 모듈의 무결성 확보와 메시지 인증을 보장하는 역할을 하고, 디바이스 인증서는 단말의 위변조 여부를 확인하기 위해 사용된다. 따라서 코드서명 인증서와 디바이스 인증서에 대한 프로파일이 규격화되어야 한다. 그리고 이들 인증서 및 개인키는 하드웨어 모듈(스마트카드, USIM 카드 등)에 저장될 필요가 있다.

iCAS를 위한 인증서 및 키 관리 체계는 인증기관이 설립되고 나서 인증기관에서 결정될 사항이지만, 표준 규격의 활용 측면에서 공인인증체계의 사용과 기존 인터넷전화 디바이스 인증 체계와의 연동을 고려할 필요성이 있다.

V. iCAS 환경의 IPTV를 위한 인증기관 설립 방안

본 절에서는 4.1절에서 분류한 각 방안에 대해 특징 및 요구사항 만족 여부를 비교·평가 한다. 각각의 방안에 대해 종단간 보안, 단말의 호환성 및 이동성, 단일 인증서 및 키 관리, 표준 규격의 유지 관리 편리성, 정부/공공기관의 지원 또는 역할, 그리고 콘텐츠 유출에 대한 부담 및 IPTV 사업자의 부담 등을 비교 항목으로 하여 기존 인증기관과 비교·평가 한다.

5.1 인증기관의 기능 및 역할에 따른 비교

〔표 2〕의 종단간 보안에서, 방안1)~방안3) 및 기존 인증기관은 기본적으로 IPTV 서비스의 종단간 보안을 제공한다. 방안1)~방안3)은 iCAS를 수용하고 단일 인증서 및 키 관리 체계를 가지기 때문에 IPTV 단말들 간의 호환성과 이동성을 제공하지만, 기존 인증기관은 개별 인증기관이 인증서 및 키 관리를 각각 수행하기 때문에 단말들 간의 호환성 및 이동성을 제공하지 못한다.

표준 규격에 대한 수정 및 개정의 요구 발생 시에 표준 규격을 유지하는 주체 및 체계가 있다면 규격의 유지 및 관리가 편리해 진다. 따라서 표준 규격의 유지관리 편리성 측면에서는 스펙인증 기능을 제공하고 있는 방안2)와 방안3)이 편리성을 제공한다. 반면 스펙인증을 제공하지 않는 방안1)과 기존 인증기관은 서비스 사업자 및 업체 별로 각각 규격을 관리해야 하고 이중의 비용과 시간을 필요로 하기 때문에 표준 규격

〔표 2〕 기능 및 역할에 따른 각 제안 방식의 비교

비교 항목	방안1) 인증서 및 키 관리	방안2) 인증서 및 키 관리 + 할리우드 인증	방안3) 인증서 및 키 관리 + 스펙인증	기존 인증기관
종단간 보안	제공	제공	제공	제공
단말의 호환성 및 이동성	제공	제공	제공	제공안함
단일 인증서 및 키 관리	제공	제공	제공	제공안함
표준 규격의 유지관리 편리성	불편함	편리함	편리함	불편함
개별 콘텐츠 제공자에 대한 법준수 사항의 만족 여부	만족안함	만족함	만족안함	부분적 만족

의 유지관리 측면에서 편리성을 제공하지 못한다.

개별 콘텐츠 제공자에 대한 법준수 사항의 만족 여부 측면에서는 법률인증 기능을 제공하고 있는 방안2)만이 법준수 사항을 만족한다. 법률인증을 제공하지 않는 방안1)과 방안3)은 법준수 사항을 만족하지 못하며, 기존 인증기관에서는 개별적으로 법률 인증을 수행하기 때문에 부분적으로 만족한다고 할 수 있다.

5.2 인증기관의 운영 주체에 따른 비교

〔표 3〕의 정부/공공기관의 지원 또는 역할 측면에서, 방안3)은 공공기관에서 인증기관을 운영하는 형태이므로 정부 및 공공기관의 적극적인 지원을 필요로 한다. 반면 방안1)과 방안2)는 관심 주체들의 투자로 설립되거나 IPTV 서비스 사업자들이 연합하여 자율적으로 운영하는 인증기관의 형태이므로 정부 및 공공기관의 지원은 불필요하다. 기존 인증기관은 공공기관 혹은 사설 인증기관이 인증기관의 역할을 수행하고 있으므로 비교대상에서 제외된다.

방안1)은 콘텐츠 유출 사고 발생 시 책임을 인증기관으로 제한시킬 수 있기 때문에 참여 주체들은 초기 투자 금액 만큼만의 손해만 입게 된다. 따라서 콘텐츠 유출에 대한 부담 측면에서는, 관심 주체들의 투자로 설립된 별도 회사 형태의 인증기관인 방안1)이 부담이 낮다고 할 수 있다. 반면 방안2)는 콘텐츠 유출시 IPTV 서비스 사업자들이 책임을 부담해야 하므로 콘텐츠 유출에 대한 부담이 높다고 할 수 있다. 방안3)이 콘텐츠 유출에 대한 부담이 중(中)인 이유는 공공기관에서 운영하는 형태이기 때문에 공공 기관 및 정부에서 콘텐츠 유출에 대한 전체 혹은 일정 부분의 책임을 지기 때문이다. 그리고 기존 인증기관의 경우에는 콘텐츠 유출에 대한 책임을 각 제조업자가 지기 때문에 콘텐츠 유출에 대한 부담이 낮다고 할 수 있다.

마지막으로 IPTV 사업자의 부담 측면에서는 초기 투자비용이 발생하고 인증기관의 참여주체들이 각 인증기관의 기능을 수행해야 하는 방안1)과 방안2)가 IPTV 사업자의 부담을 높게 하며, 공공 기관에서 운영하는 형태인 방안3)이 IPTV 사업자의 부담을 가장 낮게 한다.

5.3 최종 인증기관 설립 방안 제안

5.1절과 5.2절에서 비교·평가 했듯이 iCAS 환경의 국내 IPTV 인증기관 설립 방안은 기능별 및 운영 주체별로 다양하게 분류할 수 있다. 가장 이상적인 인증기관의 설립 방안은 정부 및 공공 기관에서 인증기관의 역할을 수행하고 인증서 및 키 관리 기능과 스펙 인증 및 법률인증 기능, 그리고 헐리우드 스튜디오들에 대한 인증 기능 모두를 수행하는 형태인 4.1절의 방안2)와 4.2절의 방안3)을 결합한 방안이라고 할 수 있다. 하지만 이와 같은 형태는 예산 비용과 잠재적인 책임 등에 대한 위험 부담을 해소해야 하는 문제가 존재하므로 사실상 실현되기 어렵다. 또한 새로운 회사를 설립하여 운영하는 인증기관의 형태인 4.2절의 방안1)에서는 인증기관이 모든 기능을 가지는 방안2)를 따른다 하더라도 초기 회사 설립 시 들어가는 비용 투자 부담의 문제로 인해 참여 주체들의 자발적인 참여를 이끌어 내기가 쉽지 않다.

이와 같은 사항을 고려했을 때 국내 iCAS를 위한 인증기관 설립 시 에는 비용 측면과 책임에 대한 위험 부담, 그리고 인증기관이 가져야 할 기능들에 대한 trade-off를 고려해야 한다. 특히, 인증기관의 기능 중 헐리우드 스튜디오들에 대한 홍보는 헐리우드 콘텐츠 수급이 필요한 사업자만 필요로 하는 기능이므로 각 사업자 모두에게 해당되는 기능은 아니기 때문에 각 사업자가 자체적으로 수행해야 할 기능이다. 따라서 국내 iCAS를 위한 인증기관은 5.1절에서 분석했듯이 IPTV 사업자에게 반드시 요구되는 기능인 인증서 및 키 관리 기능만을 가지며 그 외 인증기관의 기능은 사업자의 자율에 맡기도록 하는 4.1절의 방안1)와 4.2절의 방안3)을 결합한 형태가 가장 적절할 것

〔표 3〕 운영 주체에 따른 각 제안 방식의 비교

비교 항목	방안1) 관심 주체들의 투자로 설립된 별도 회사	방안2) IPTV 서비스 사업자들의 연합	방안3) 공공 기관에서 운영	기존 인증기관
정부/공공기관의 지원 또는 역할	불필요	부분적 필요	필요	-
콘텐츠 유출에 대한 부담	하(下)	상(上)	중(中)	하(下)
IPTV 사업자의 부담	상(上)	상(上)	하(下)	하(下)

이다. 4.2절의 방안3)이 적절한 이유는 인증서 및 키 관리 기능은 기존 공인인증기관의 기능이므로 이를 활용하여 쉽게 적용이 가능하기 때문이다.

VI. 결론

본 논문에서는 사업자간 IPTV 단말의 호환 및 이동성을 제공하기 위한 표준 규격인 iCAS를 위한 인증기관의 설립 방안을 제안하였다. 인증기관의 설립 방안으로써 인증기관의 기능 및 역할에 따른 설립 방안들과 인증기관의 운영 주체에 따른 설립 방안들을 분류하였고, 인증기관이 가져야할 최소한의 기능인 인증서 및 키 관리 방안에 대해서도 논의 하였다.

본 논문에서 분석한 내용을 토대로 했을 때, 인증기관의 기능인 인증서 및 키 관리는 인증기관이 반드시 가져야 할 기본 기능이며, 기타 스펙인증과 법률인증 등은 iCAS 비즈니스와 연관되므로 각 서비스 사업자 혹은 업체 별로 자율적인 운영에 맡기는 것이 적절하다.

향후 인증기관이 설립되어 제 역할을 수행하기 위해서는 정부의 정책 지원과 IPTV 서비스 사업자 혹은 관련 주체들의 자발적이고 적극적인 협의/합의가 필요할 것이다.

참고문헌

[1] TTA Standard, "IPTV 용 교환 가능한 CAS (iCAS)," TTAK.KO-08.0023, 2010년 3월.

[2] EBU Project Group B/CA, "A functional model of a conditional access system for use with digital television broadcasts," EBU Technical Review, Vol.266, pp. 64-77, June. 1995.

[3] 황용호, 최문영, "IPTV를 위한 다운로드 가능한 CAS 기술," TTA Journal, Vol.126, pp. 83-88, 2009년 11월.

[4] 방송통신위원회 전파연구소, "전기통신설비의 기술기준에 관한 표준시험방법 개정(안)," http://www.rra.go.kr/join/policy/view.jsp?pc_status=0&pc_type=1&pc_seq=352, 2010년 9월.

[5] Content Management License Administrator (CMLA), http://www.cm-la.com/about/

[6] Digital Transmission Licensing Administrator (DTLA), http://www.dtcp.com/about.aspx

[7] Advanced Access Content System Licensing Administrator (AACSLA), http://www.aacsla.com/founders/

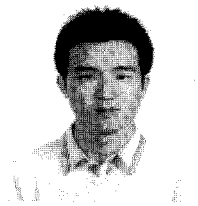
[8] Marlin Trust Management Organization (MTMO), http://www.marlin-trust.com/about

[9] 염홍열, "IPTV Trust Authority (TA)," VoIP Forum Summer Workshop, 2010년 8월.

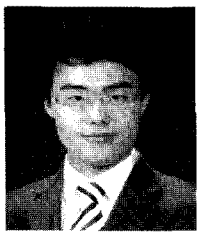
[10] 방송통신위원회, IPTV 표준화전담반 TA-TFT 6차 회의, 2010년 8월.

〈著者紹介〉

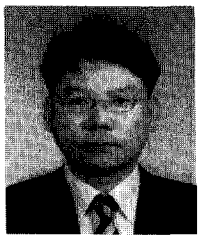
최 현 우 (Hyun-Woo Choi) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 IPTV 보안, 스마트그리드 보안, USN 보안, 역추적



정 영 곤 (Young-Gon Jung) 학생회원
2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 스마트그리드 보안, IPTV 보안, 역추적



여 돈 구 (Don-Gu Yeo) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적



염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재; ITU-T SG17 부의장/SG17 WP2 의장
〈관심분야〉 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜