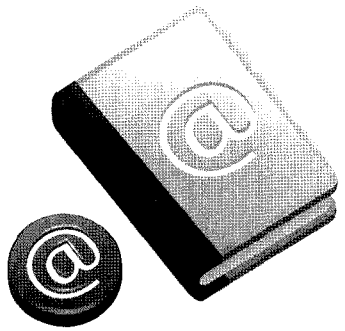
IPTV를 위한 다운로드 가능한 CAS 기술

황용호 | TTA IPTV PG 위원,
삼성전자 Digital Media & Communications 연구소 책임연구원
최문영 | TTA IPTV PG 부의장 및 보안 실무반 의장,
삼성전자 Digital Media & Communications 연구소 수석연구원



1. 머리말

통신 기술과 디지털 기술의 발달로 인터넷을 활용한 IPTV 서비스가 상용화되고 IPTV를 통해 다양한 디지털 콘텐츠 서비스가 가능해짐에 따라 IPTV 환경에 적합한 콘텐츠 보호 시스템의 중요성이 부각되고 있다. 이를 위해 기존의 디지털 케이블 방송 및 위성 방송에 적용되어온 CAS(Conditional Access System) 시스템을 이용하여 IPTV 서비스를 보호하려는 시도들이 일어나고 있다. 그러나 IPTV 서비스는 기존 케이블 방송이나 위성 방송과는 달리 인터넷을 통한 양방향 서비스를 기반으로 다양한 콘텐츠 서비스 시나리오를 지원해야 하기에 기존의 콘텐츠 보호 시스템보다 효율적이고 동적으로 적용 가능하면서도 시스템에 대한 충분한 안전성을 제공해야 한다. 또한, 특정 보호 시스템이 IPTV 셋톱박스에 고정적으로 설치되어 사용자의 서비스 선택권 및 편리성에 제약을 받거나 유동적인 서비스 시나리오 확장에 제한을 받지 않아야 한다. 이러한 IPTV 환경에서 효율적이고 안전한 콘텐츠 서비스를 가능하도록 지원하기 위해 필요한 보안 기술을 서버로부터 다운로드 받아 사용하는 다운로드 형태의 CAS 시스템을 표준화하려는 움직임들이 활발히 진행되고 있다.

실제적으로 다운로드 가능한 CAS 시스템에 대한 표준화 시도는 케이블 TV에서 먼저 진행되었으며 대표적인 기술로 미국 케이블 방송 사업자들이 주도한 Polycipher의 DCAS(Downloadable CAS)[1] 시스템을 들 수 있다. 그러나 DCAS 표준은 방송 사업자, 단말 제조업체, 콘텐츠 제공업체, 통신 사업자 등 참가자들 간 이해관계가 얽혀 있어 표준화 작업을 진행하는 데 많은 어려움이 존재하며 케이블이라는 제한된 통신 환경과 다양한 기존 방송 사업자들을 모두 만족시킬 수 있는 표준 기술을 제정하는 것은 현실적으로 한계가 있다. 결국 이러한 한계를 극복하지 못하고 현재 표준화 진행이 중지되어 있는 상태이다. 국내에서도 한국디지털케이블연구원(KLabs) 주도 하에 케이블 향 다운로드 가능한 CAS 기술 표준을 만들기 위한 작업이 진행 중이기는 하나 복수 기술에 대한 표준화가 진행되면서 기존 모든 케이

1) "DCAS"라는 용어는 Polycipher에서 제안한 다운로드 구조를 가진 CAS 시스템의 고유 명칭이다. 따라서, 본 고에서는 일반적인 CAS SW를 다운로드 할 수 있는 구조를 가진 시스템을 DCAS와 구분하여 "다운로드 가능한 CAS"로 사용한다.

블 방송 사업자들 간에 자유로운 이동성을 제공하는 것이 현실적으로 쉽지 않다. 특정 기술이 적용되는 범위에 한정된 상태로 CAS SW가 다운로드 되는 형태의 표준으로 진행되고 있기에 기존 케이블 방송 사업자들을 모두 수용할 수 있는 Eco-system을 구축하여 상용화하는 데는 어려움이 존재한다.

그러나 IPTV 서비스의 경우 양방향 통신이 가능하고 자유롭게 데이터 전송이 가능한 IP 네트워크를 사용하기에 기술적인 제약 사항에서 더 자유로울 수 있으며, 서비스 초기 단계에서부터 표준화가 함께 고려되고 있기에 표준 기술을 기반으로 서비스를 상용화하는 것이 가능할 것으로 예상된다. 물론 IPTV 서비스 역시 지상파 및 케이블 TV 방송, 위성방송, 인터넷 포털 사업자 등 각종 사업자와 경쟁관계에 있는 데다 단말 제조업체, 콘텐츠 제공업체, 통신사업자 등 참가자들의 이해관계가 얽혀 있어 표준화 작업이 쉽지 않은 것이 사실이다. 그러나 인터넷 환경에서의 다양한 IPTV 서비스 시나리오들이 소개되고 있고 이에 따른 서비스 호환성과 단말의 이동성 제공을 위해서는 반드시 표준화된 형태의 기술이 요구된다. 본 고에서는 IPTV 향 다운로드 가능한 CAS 기술과 관련된 국내외 표준화 활동 등에 대해 살펴보고, 국내 TTA PG219 산하 Security 실무반(WG4)에서 진행 중인 다운로드 가능한 CAS 기술에 대한 국내 표준 진행 현황에 대해 소개한다.

2. IPTV 서비스 보안 기술의 국제 표준화

ITU-T(전기통신 표준화 부문)는 국제연합(UN) 산하에 설립된 국제표준 제정기구로 전기통신에 관한 국제표준을 만드는 기구이다. ITU-T는 2006년 4월 IPTV FG(Focus Group)을 구성해 표준화 작업을 시작했으며 2007년 12월에 21개의 표준화 의제를 확정하고, 2008년 1월부터 IPTV-GSI(Global Standard Initiative)를 통해 IPTV 서비스 표준화 작업을 진행하고 있다. IPTV-GSI에서는 IPTV의 전반적인 요구사항 및 구조, 시나리오 등을 논의하고 있으며 ITU-T Recommendation Y.1901 'Requirements for the support of IPTV services'를 통해 IPTV를 위해 필요한 요구사항들을 정리했다. 보안과 관련된 요구사항들은 콘텐츠 보호, 서비스 보호, 네트워크 보호, 단말기 보호, 가입자 보호 등에 따른 요구사항들로 구분되어 작성되어 있다. ITU-T의 서비스 보호에 대한 요구사항들을 살펴보면 특정 HW나 SW에 의존적이지 않으면서 콘텐츠에 따라 필요한 보안 서비스를 검색하여 다운로드 받을 수 있는 형태의 보안 시스템 구조를 가지고 있다. 세부 기술규격 및 권고안은 7개의 SG(Study Group)에서 분야별로 나눠 표준화를 제정하고 있으며 보안과 관련된 부분은 SG17에서 담당하고 있으나 아직까지 세부적인 기술 규격 작업은 이루어지지 않고 있다.

북미 통신 표준기구인 ATIS(Alliance for Telecommunications Industry Solutions)는 IIF(IPTV Interoperability Forum)를 통해 IPTV를 위한 산업 표준을 개발하고 있다. IIF는 서비스 제공자, 소프트웨어 회사, 콘텐츠 공급자, 단말기 제조사 등 전체 IPTV 산업 관련자들이 모여 IPTV 네트워크 구조, QoS, 보안, 메타데이터와 상호호환성 테스트 등에 대한 표준을 진행 중이다. ATIS 역시 아직까지 구체적인 기술 규격이 완성되지 않은 상태이다.

3. IPTV 서비스 보안의 국내 표준화

국내 IPTV 서비스 제공을 위한 표준 규격은 정부의 미래 핵심 표준기술을 선점해 IPTV 3대 기술 강국으로 도약하기 위한 방안으로 방송통신위원회에서 체

계적인 IPTV 표준화 추진을 위한 IPTV 실무전담반을 구성해 표준화 추진을 진행하고 있다. 국내 표준화는 TTA 산하 IPTV PG(Project Group)에서 담당하고 있으며, 단말 이동성 및 콘텐츠 호환성 제공이 가능한 IPTV 표준 기술 규격 제정을 목표로 진행 중이다. IPTV PG 산하 보안 실무반(WG4)에서는 단말의 이동성 관련하여 이슈가 되고 있는 다운로드 가능한 보안 기술에 대한 기술 규격을 준비하고 있다. 단말의 이동성은 IPTV 사용자가 서비스를 이동하더라도 단말의 교체가 필요하지 않는 것을 의미하며, 이는 기존의 IPTV 단말들이 특정 IPTV 서비스 사업자들과 결합된 형태로 구성되어 있기에 사용자가 서비스 이동을 원할 때 새로운 단말을 구입하거나 이에 대한 비용을 IPTV 서비스 사업자가 감당해야 하는 문제를 해결하고자 하는 것이다. 보안 기술의 교체는 단순히 애플리케이션의 교체를 의미하는 것이 아니라 전체 서비스의 안전성을 보장해야 하기에 서로 다른 보안 기술들이 IP 네트워크 하에서 안전하게 다운로드 되고 수행될 수 있는 환경을 제공해 주는 기술에 대한 표준이 반드시 필요하다. WG4에는 서비스 사업자, 단말 제조사, 보안 솔루션 업체 등이 참여하여 2009년 12월까지 표준 초안을 완성하는 것을 목표로 활동 중이다. 실무반 내에서는 HW/SW 기반 다운로드 보안 기술에 대한 표준 제정을 모두 고려하고 있으나 국내 IPTV 서비스 사업자들이 IPTV 수신 단말의 원가 상승 등의 이유로 SW 기반 보호 기술을 선호하고 있기에 SW 기반 다운로드 보안 기술에 대한 규격 작업이 선행되어 진행 중이다.

4. IPTV 향 다운로드 가능한 CAS 국내 표준화 진행 현황

현재 WG4에서 진행 중인 다운로드 가능한 CAS 기술 표준 작업은 서비스 사업자들의 요구에 따라 SW 기반 시스템을 표준화하는 것을 우선 목표로 진행 중에 있으며, Secure Microprocessor와 같은 보안 칩을 이용하는 구조와 Cable Card 형태의 HW 기반 구조에 대한 기술들에 대해서도 배제하지 않고 표준 활동을 진행하고 있다. SW 기반 다운로드 가능한 CAS기술에 대해 2009년 12월까지 1차 규격 작성 작업을 완료하는 것을 목표로 진행 중이며, 규격이 완료된 후 실제 상용화 서비스 적용을 위해 추가적으로 필요한 기술들과 다른 구성요소들과의 호환성을 위해 필요한 기능들에 대한 표준화 작업을 진행할 예정이다.

WG4에서는 서비스 보호에 대한 기술 규격 작업을 중심으로 규격을 작성하고 있으며 ITU-T IPTV FG의 요구사항들을 기반으로 현재 국내 IPTV 서비스를 위해 수용 가능한 요구사항 27개 항목을 도출했고, 국내 환경에 맞는 2개의 요구사항을 추가하여 총 29개의 요구사항을 확정했다. 확정된 요구사항들에 기반하여 IPTV 서비스는 IPTV 수신 단말이 정당한 기기인지를 인증 후 서비스 보안 시스템을 다운로드 시켜주어야 하며, IPTV 서비스 보호 시스템은 특정 HW/SW에 의존적이지 않고 상황에 따라 다양한 서비스 보호 기술을 다운로드 받을 수 있도록 설계되어야 한다.

이러한 보안 요구사항을 기반으로 단말의 이동성을 제공하며 안전한 서비스 보호 시스템을 제공해주기 위해 현재 검토 중인 다운로드 가능한 CAS 기술은 다음의 3단계로 구성되어 있다.

① 서버와 단말의 인증을 통해 CAS SW의 다운로드 권한을 획득하는 단계

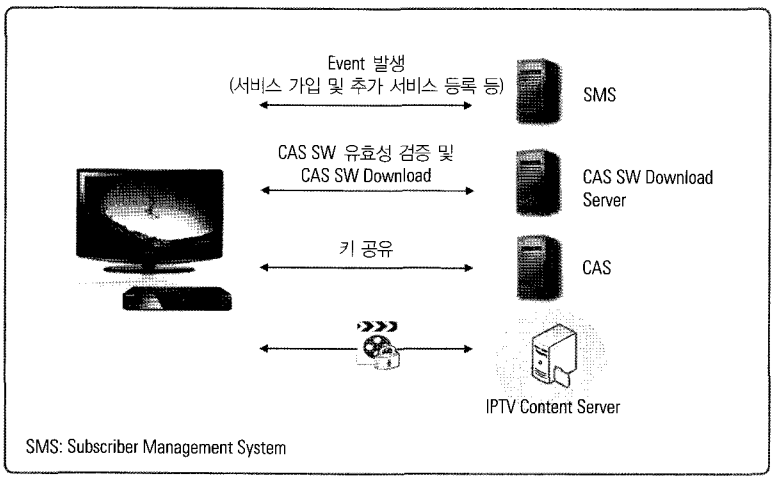
② 인가된 단말에 한해 안전하게 보호된 형태로 CAS SW를 내려주는 단계

③ 내려 받은 CAS SW를 안전하게 저장하고 실행하는 단계

서버와 단말 상호 간에 새로운 세션을 형성하기 위해서는 상호 간의 인증 과정이 수행되어야 하며, 사용자가 새로운 IPTV 서비스에 가입을 하거나 추가 서비스 등록 등 새로운 Event가 발생할 경우 서버는 정당한 단말이 사용 권한을 획득하는 것인지를 판단하기 위해 단말을 인증할 수 있어야 한다. 또한 CAS SW 등을 내려 받기 위해 자신의 사용 권한과 안전성을 서버에게 증명할 수 있어야 한다. 서버는 정당한 사용자 단말에만 가용 CAS SW를 다운로드 시켜주며 단말은 CAS SW를 실행 전에 합법적인 서버에 의해 전송된 CAS SW인지를 확인한 후 CAS SW를 로딩하여 안전하게 실행한다. [그림 1]은 표준에서 검토 중인 다운로드 가능한 CAS 시스템의 구조이다.

IPTV 수신 단말은 CAS SW를 다운로드 받기 위해 먼저 서버로부터 정당한 시청 권한을 가진 사용자라는 것을 인가 받아야 하며, 이에 대한 인증 결과로 서버를 단말에게 다운로드 서버 정보와 시청 가능한 콘텐츠 정보 등이 포함된 Token을 수신 단말과 결합된 형태로 전달한다. 따라서 다른 IPTV 수신 단말에서는 다른 단말로 발급된 Token을 획득한다 하더라도 사용하는 것이 불가능하다. 단말은 해당 CAS SW를 다운로드 받기 위해 자신이 보유한 Token을 인증 정보와 함께 CAS SW 다운로드 서버에 전달한다. 이때 서버는 정당한 사용자인지를 확인하기 위해 Token을 검증하여 정당한 단말인지를 확인 한 후, 추가적으로 해킹된 단말인지를 확인하는 과정을 수행한다.

서버는 사용자 단말이 정당한 기기인지 사용자 단말에서 사용 가능한 CAS SW가 존재하는지를 확인한 후, CAS SW를 다운로드하여 주는 것이 필요하다고 판단되면 CAS SW를 단말의 공개키로 암호화된 상태로 내려준다. 이 때 CAS SW 관리를 위한 policy가 함께 패키지된 형태로 전달된다. 또한 악의적인 서버나 사용자에 의해 불법 SW가 다운로드 되는 것을 방지하기 위해 정당한 서버로부터 전송되는 것인지 확인하기 위한 검증 메커니즘이 추가된다. 만약 사용자 단말이 이미 사용 가능한 CAS SW를 보유하고 있다면 해당 CAS SW 사용을 알려주게 된다. 다운로드 된 CAS SW는 로딩되어 사용될 때를 제외하고는 암호화된 형태로 단말에 저장되어 있게 된다. 인증 과정 및 CAS SW 다운로딩 과정 등



[그림 1] 다운로드 가능한 CAS 시스템 구조

을 포함한 모든 서버와 IPTV 수신 단말과의 통신은 보안 메커니즘인 SSL/TLS에 의해 보호된다.

단말의 이동성을 제공하고 다양한 CAS SW가 수행되기 위해 단말에서는 하드웨어에 독립적인 실행환경을 제공해야 한다. 일반적인 다운로드 가능한 CAS 시스템 구조에서는 Security Processor라고 불리는 영역에서 이를 처리하게 되며 본 규격 작업에서는 VM(Virtual Machine) 개념을 이용해 CAS SW가 하드웨어에 독립적으로 동작하도록 설계하고 있으며, VM상에서 동작하는 동안 CAS SW를 보호하기 위한 메커니즘들에 대한 세부적인 사항들을 논의하고 있다. 기본적으로는 CAS SW는 암호화된 형태로 저장되어 있다가 로딩되어 VM 메모리에 적재될 때 랜덤 마스킹 기법을 사용해 보호하게 되며 실행되는 명령어 1개 단위로 코드를 fetch하게 된다. 또한 CAS SW는 서버로부터 함께 다운로드 받은 policy에 의해 control하게 되고, policy는 CAS SW가 수행 가능한 동작이나 접근 가능한 system 영역 등에 대해 정의하며, CAS SW가 실행되는 동안 CAS SW를 모니터링하여 허가되지 않은 영역의 접근이나 행동을 제어하게 된다.

앞에서 언급했듯이 현재는 서비스 보호 기술 중심으로 표준 규격작업을 진행 중에 있으나, 다운로드 가능한 CAS 기술이 안전하게 수신 단말에 적재되어 수행되기 위해서는 단말의 안전도도 중요한 이슈사항이다. WG4에서 제정하는 표준에서는 단말과 관련한 보호 기술에 대해서는 표준의 인증 기관인 TA(Trusted Authority)에서 제정하는 Robustness Rules에서 정의하기로 결정했다. 따라서 WG4에서 제정한 보호 기술을 적용하기 위해서는 Robustness Rules을 포함한 해당 TA의 관련 규정을 준수해야만 한다.

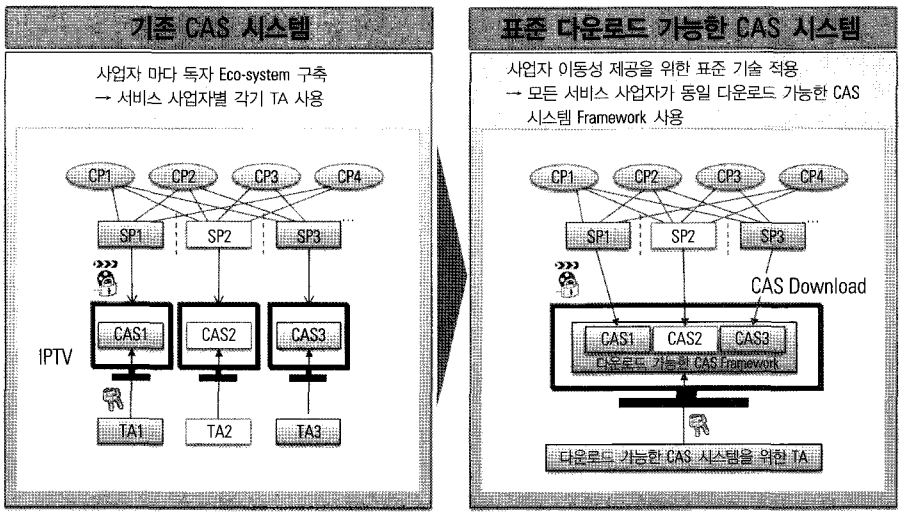
5. 맺음말

다운로드 가능한 시스템은 기술적인 문제 외에도 실제 상용화를 위해 콘텐츠 사업자, 서비스 사업자, 단말 제조업체, 보안 솔루션 업체 간에 풀어야 하는 많은 숙제들이 남아 있다. 기술적인 부분은 TTA IPTV PG 산하 WG4에서 진행 중에 있으나 기술 제정만으로는 상용화하는 데 많은 어려움이 존재한다. 특히 단말의 이동성을 보장하기 위해 반드시 해결해야 하는 중요한 문제는 규격 내의 Eco-system에서 키 혹은 인증서를 체계적으로 관리 할 인증기관(TA)의 필요성에 관한 것이다. 기존 CAS 시스템에서는 솔루션 제공 업체가 TA의 역할을 수행했으나 표준화가 되어 단말 이동성이 제공되기 위해 다운로드 가능한 CAS기술이 적용된 전체 Eco-system을 관리하는 하나의 TA가 존재하는 것이 필요하다. 단말의 이동성을 제공하기 위해 TA로부터 인증(인증서 또는 키 발급) 받은 단말은 동일 Eco-system 내에 포함된 IPTV 서비스 사업자 사이에서만 이동이 가능하기에 모든 서비스 사업자가 동일한 다운로드 가능한 CAS Framework 안에 들어와 있어야만 한다[그림 2].

또한 표준 규격의 TA는 아래 사항에 대한 관리 책임의 의무가 있다.

- 콘텐츠 사업자들이 만족할 만한 Compliance Rules과 Robustness Rules 제정
- 콘텐츠 제공자, 사업자, 단말 제조사 대상 License Agreement 작성 및 Adopter와 계약 체결
- Hollywood Studio들에 대한 홍보 및 승인 획득
- 기술 활용에 대한 사후 Audit
- 위의 규정에 대한 인증(필요시)

TA의 설립 형태에 대해서는 몇 가지 방안이 고려될 수 있지만 일반적으로 표준 시스템을 위한 TA들은 표



[그림 2] 기존 CAS 시스템과 표준 다운로드 가능한 CAS 시스템 간 TA의 형태 비교

〈표 1〉 표준 기술 규격별 TA 구성 현황

표준 기술	OMA	DTCP	AACS	Marlin	IPTV PG Security
기술규격 제정/유지	OMA	DTLA	AACSLA	MDC	TTA
Trust Management	CMLA/Others	DTLA	AACSLA	MTMO	미정
Robustness Rule	CMLA/Others	DTLA	AACSLA	MTMO	미정
Compliance Rule	CMLA/Others	DTLA	AACSLA	MTMO	미정
License Agreement	CMLA/Others	DTLA	AACSLA	MTMO	미정
Studio Promotion	CMLA/Others	DTLA	AACSLA	MDC&MTMO	미정

준 시스템 적용에 관심을 가지는 회사들이 공동 투자하여 별도 회사를 설립하여 운영되며, 이 회사는 직접적인 이윤 추구가 아닌 표준 규격을 활용한 사업화 지원을 목적으로 한다. 〈표 1〉은 타 표준화 단체의 TA 구성에 대해 보여준다.

국내 환경을 고려해 본다면 서비스 제공자들이 연합해 운영하는 방식이나 공공기관에서 운영하는 방식 등도 고려해볼 수 있다. 단 TA는 이윤을 추구하는 것이 목적이 아닌 표준 규격을 이용한 사업화 지원이 목적이 되어야 한다. TA를 운영하기 위해 일반적으로 1년 이상의 준비 기간이 필요하기에 2011년 표준 기술 상용화를 위해서는 지금부터 준비가 시작되어야 하나 아직까지 여러 사업자들의 필요성 인식 부재로 인해 준비가 미흡한 상황이다. TA에 대한 준비가 이루어지지 않는다면 기술 규격 제정과는 상관없이 표준 기술 상용화는 불가능하기에 IPTV 향 다운로드 가능한 CAS 표준 기술 상용화를 위해 반드시 해결해야 하는 숙제이다. TTA