[방송기술] 케이블 망 기반 제한수신 기술 표준화 동향

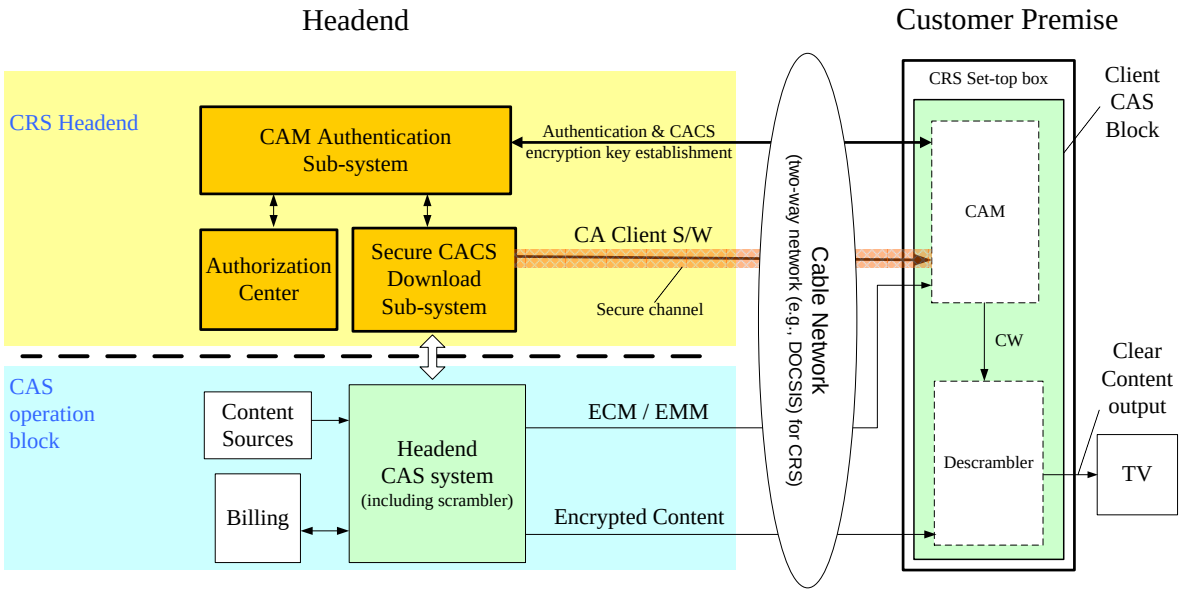
ITU-T SG9은 케이블망 기반의 방송 및 통신 기술에 대한 표준화를 담당하고 있다. ITU-T SG9 산하에는 총 14의 Question 그룹들이 존재한다. 이 중 Question 3(이하 Q.3/9)은 케이블 망 기반 제한수신 기술 및 방송의 댁내 재전송에 대한 복제방지 기술에 대한 표준화를 담당하고 있다. 현재 Q.3/9은 세 개의 work programme들을 운영하고 있다. 그 첫 번째는 원격 제한수신모듈 갱신 기술에 대한 기술적 요구사항을 정의하고 있는 J.rcas-req이다. 두 번째는 케이블 헤드엔드와 단말 간 네트워크 프로토콜을 규정하는 J.rcas-net이다. 마지막 work programme은 단말 내 보안모듈과 디스크램블러 간의 쌍(pair)관리를 통해 불법적인 유료시청을 방지하는 프로토콜을 정의하는 J.rcas-pair이다.

본 고에서는 현재 Q.3/9에서 개발 중인 세 개의 work programme들에 대한 간단한 소개 및 향후 일정에 대해 논하고자 한다.

J.rcas-req 소개

ITU-T SG9에서는 2010년 7월부터 소프트웨어 기반의 제한수신 모듈을 원격으로 갱신할 수 있는 기술에 대한 표준화를 시작하였다. 그 첫 번째 단계로 현재는 요구사항 수립 단계로 J.rcas-req라는 권고표준안을 개발하였다. J.rcas-req은 2012년 1월 현재 AAP LC상태에 있다.

J.rcas-req 권고표준안은 양방향 케이블 망을 사용하는 디지털 케이블 시스템에서 가입자 단말 내 제한수신모듈 클라이언트 소프트웨어를 원격으로 갱신할 수 있는 CRS(Conditional access client software Remote renewable security System)에 대한 요구사항을 담고 있다. J.rcas-req은 <그림 1>과 같은 CRS 참조 모델을 정의하고 있으며, CRS에 대한 요구사항을 구조적 요구사항과 기능적 요구사항 및 보안요구사항으로 나누어 정의하고 있다. 구조적 요구사항에서는 CRS 헤드엔드와 CRS 셋톱박스에 대한 구성 요소 및 각 구성요소들의 기능들에 대한 요구사항을 정의하고 있다. 기능 요구사항에서는 CRS가 반드시 제공해야 할 필수 기능들, 즉 단말인증과 페어링(pairing) 및 복제방지기능들에 대한 요구사항 정의하고 있다. 마지막으로 보안 요구사항에서는 키 생성과 관련된 보안요구사항들을 정의하고 있다.



<그림 1> Reference architecture of CRS

J.rcas-net 소개

J.rcas-net은 2011년 11월 ITU-T SG9 스위스 제네바 회의에서 새롭게 승인된 work progrmme 이다. J.rcas-net은 J.rcas-req에서 정의하고 있는 주요 요구사항 중 CRS 헤드엔드와 CRS 셋톱박스 간의 보안 네트워크 프로토콜을 규정한다. J.rcas-net은 다음의 기능들을 주요 내용으로 다룰 예정이다.

- Security Announce 기능: 초기 환경설정 정보와 업그레이드 정보 및 CRS 헤드엔드 서버 접속 정보 등을 CRS 헤드엔드에서 CRS 셋톱박스 내 제한수신모듈로 전달하는 기능
- Keying and Authentication 기능: 제한수신클라이언트 이미지를 암호화하고 제한수신모듈을 인증하기 위한 암호화 및 인증키를 생성하는 기능
- CRS pairing 지원 기능: CRS pairing 도중 제한수신모듈과 CRS 헤드엔드 간 필요한 통신을 지원하는 기능
- Download information 전달 기능: 제한수신클라이언트 이미지를 안전하게 CRS 헤드엔드에서 제한수신모듈로 다운로드 하는 기능

J.rcas-pair 소개

J.rcas-pair는 J.rcas-net과 마찬가지로 2011년 11월 ITU-T SG9 스위스 제네바 회의에서 새롭게 승인된 work progrmme이다. J.rcas-pair는 J.rcas-req에서 정의하고 있는 주요 요구사항 중 제한수신모듈과 디스크램블러 간 페어링을 위한 프로토콜을 규정한다. J.rcas-pair는 다음의 기능들을 규격 내에 포함할 예정이다.

- Authorization Center(AC)를 통한 제한수신모듈과 디스크램블러 간의 페어링 기능: 제한수신모듈과 디스크램블러의 식별정보는 암호화 되어 CRS 헤드엔드로 보내진다.

- CWEK(Control Words Encryption Key) 생성 기능: 제한수신모듈에서 디스크램블러로 control words(CW)가 보내질 때 CW의 보안을 위해 CWEK으로 암호화 된다. 이를 위해 제한수신모듈과 디스크램블러는 페어링 프로토콜을 통해 CWEK을 생성한다. 이 과정은 CRS 헤드엔드를 통해 유효성이 확인된 경우에 한해 이루어진다.

향후 일정

ITU-T SG9은 2011년 11월부터 CRS의 주요 기능 중 두 가지인 CRS 네트워크 프로토콜과 CRS 페어링 프로토콜에 대한 표준화를 각각 J.rcas-net과 J.rcas-pair라는 이름으로 시작했다. J.rcas-net과 J.rcas-pair는 현재 2012년 내에 표준화를 완료하는 것으로 하고 있다. 하지만, ITU-T SG9의 연구회기가 공식적으로 2012년 5월에 끝나기 때문에 완료 일정이 2013으로 미뤄질 가능성이 존재한다. ITU-T SG9 Q.3/9은 앞서 설명한 두 가지 work programme 이외에도 복제방지규격과 CRS 헤드엔드 서브시스템 간 인터페이스 규격 등을 추가로 표준화 할 계획이다.

구한승 (한국전자통신연구원 방송시스템연구부 선임연구원, koohs@etri.re.kr)