[정보보호] ITU-T SG17 트랜스코더블(Transcodable) 정보보호 동향

멀티미디어 환경에서 N-스크린 (OsMu: One Source Multi Use) 서비스가 가능하도록 핵심기술이 제공되는 것은 매우 반가운 일이 아닐 수 없다. 이러한 기술은 다각적인 연구를 거쳐서 상용화 단계에 와 있으며, 정보보호 기술 또한 동등한 수준으로 개발되어 현재 국내의 산업적인 여건이 잘 조성되고 있다. 이에 발맞추어 국제 표준(X.1192: Functional requirements and mechanisms for the secure transcodable scheme of IPTV)도 완성 단계에 있으며, 2011년 4월, SG17 국제회의에서 최종 표준초안이 승인되어, 현재 국가별 의견수렴에 들어가 있는 상태이다.

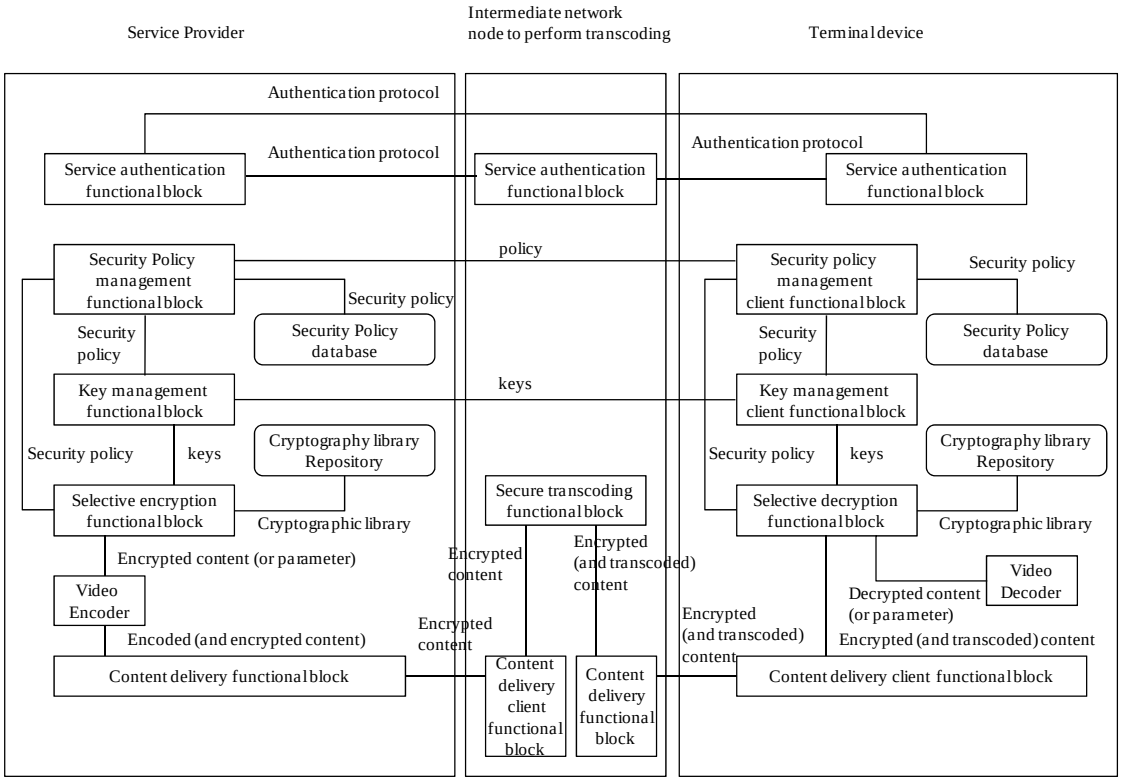
본 표준은 스마트TV 환경에서, 상황에 따라 변화하는 네트워크의 대역폭, 또는 단말기의 제한적 성능과 같은 열악한 단말기 환경에서도 원활한 영상서비스를 제공하기에 장점을 갖는 기술이다. 헤드엔드(Head End)에서 전송되는 콘텐츠가 SVC(Scalable Video Codec) 기반의 정보보호 스트리밍 데이터로 구성되어 있어서, 여러 종류의 단말에 적응적(Adaptive)으로 정보보호 서비스가 제공되는 표준 기술이다.

안전한 트랜스코더블 메커니즘

안전한 트랜스코더블 메커니즘은 계층적(Scalable) 비디오 압축 알고리즘에(MPEG4 FGS(ISO/IEC 14496-2), H.264/SVC(ITU-T H.264 ITU-T T.807) 등 기반을 둔다. 본 표준은 이러한 표준들에 적용 가능하며, 네트워크 상황 또는 단말의 처리능력에 따라 암호화된 콘텐츠의 복호 없이 동적으로 트랜스코딩이 진행되는 동안에 종단간(End-to-end) 스케일러블 정보보호 기능을 제공한다.

<그림 1>의 스마트TV 정보보호 서비스 구조를 보면, 서비스 제공자 측에서 부분(Selective) 암호 기능블록은 비디오 인코더와 상호협력을 하여 안전한 트랜스코더블 콘텐츠를 생성한다. 이러한 부분 암호 기능블록은 서비스 제공자의 정보보호 정책에 의해 제어되어야 한다. 암호화된 콘텐츠는 전달 기능블록을 통하여 네트워크나 단말의 능력에 따라 네트워크 중간노드에서 선택적인 트랜스코딩이 발생될 수 있다. 그리고 이용자 측의 부분 복호 기능블록은 서비스 제공자에 의하여 사전에 전달되는 키와 정책에 근거하여 계층적으로 암호화된 콘텐츠를 복호화 과정을 처리하여 최종 이용자가 원하는 영상을 재생할 수 있다.

주요 산업의 동향을 살펴보면, 캐나다의 Human-computer interaction와 Computer-supported cooperative work 분야의 학계 전문가 모임인 NECTAR에서는 암호화된 멀티미디어 콘텐츠를 복호화 없이 트랜스코딩하는 시스템의 개발을 위한 프로젝트인 SSMS(Secure Scalable Multimedia Streaming)를 들 수 있으며, 현재 MPEG-4 비디오 스트림의 크기 변환에 초점을 맞추고 있다.



<그림 1> 안전한 트랜스코더블 메커니즘 구성요소

(출처: ITU-T SG17 TD 1772 Rev.3)

향후 전망

안전한 트랜스코더블 메커니즘은 스마트 스크린 서비스에서 방송서비스 접근제어를 위하여 필수적인 정보보호 기술이며, 정보보호 서비스의 종단성(End-to-end), 계층성(Scalability), 효율성(Efficiency), 적응성(Adaptiveness)을 제공한다. 향후 추진되어야 할 표준 아이템은 중간 노드(Intermediate network node)에서 필요에 따라 추가적으로 암호화하는 기능이다. 본 표준에서 제공되는 부분 암호화로 인하여 상대적으로 약한 보안강도가 적용된 콘텐츠를 중간 노드에서 이후 전달되는 이용자의 접근 네트워크(Access Network)나 서비스의 종류에 따라 보안강도를 강화할 수 있는 기능이다.

나재훈 (한국전자통신연구원 지식정보보안연구부 팀장, jhnah@etri.re.kr)