

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

개요

인터넷 방송서비스 제공자(Service Provider) 관점에서 SVC(Scalable Video Codec) 활용은 커다란 의미를 갖는다. 요즘 화제가 되고 있는 스마트 스크린 서비스를 제공하기 위해서는 OsMu(One Source Multi Use) 개념을 기반으로 하는 SVC를 이용하는 것이 시스템 및 네트워크 구축을 원활하게 하는 것이다.

네트워크 전송 효율성을 제고한 SVC를 기반으로 하는 유무선 통합의 IPTV 환경은 무선 인터페이스의 협소한 대역폭, 또는 이동용 단말기의 제한적 성능과 같은 열악한 네트워크 환경에서도 원활한 영상서비스를 제공하기에 장점을 갖는 기술이다. 헤드엔드(Head End)에서 전송되는 콘텐츠가 여러 종류의 단말에 적응적(Adaptive)으로 정보보호 서비스가 제공되는 기술의 표준이 지난 ITU-T SG17 12월 회의에서 국제표준 채택을 위한 최종안(X.ipytvsec-2)이 제출되었으며, 보안 메커니즘 적용을 위한 정책의 필요성, 정책구성요소, 정책협상 절차를 위한 기고문에 대하여 논의가 이루어졌다.

안전한 트랜스코더블 메커니즘

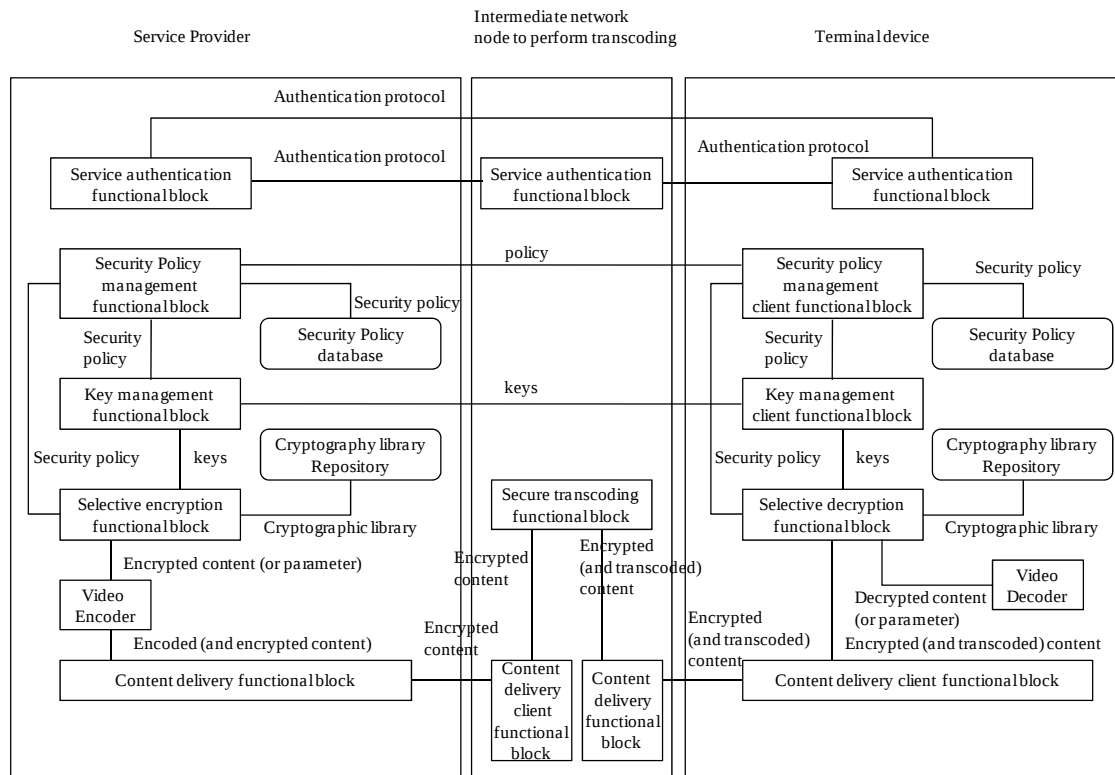
안전한 트랜스코더블 메커니즘은 계층적(Scalable) 비디오 압축 알고리즘에(MPEG4 FGS, H.264/SVC 등) 의하여 부호화된 스케일러블 콘텐츠에 기반을 둔다. MPEG4 FGS, H.264/SVC의 알고리즘과 구조는 [ISO/IEC 14496-2]와 [ITU-T H.264]에 잘 정의되어 있다. 그리고 또 다른 참조표준으로 JPEG2000이 있으며, 이 표준도 비디오 계층성(Scalability)을 제공한다. JPEG 2000은 정지 이미지 기반의 압축 알고리즘이며 트랜스코더블 정보보호 구조를 제시하고 있다[ITU-T T.807].

이러한 표준들에 적용 가능한 안전한 트랜스코더블 메커니즘이 제시되었으며, 네트워크 상황에 따라 또는 단말의 처리 능력에 따라 콘텐츠의 복호화 없이 동적으로 트랜스코딩이 진행되는 동안에 종단간(End-to-end) 스케일러블 정보보호 기능을 제공한다.

안전한 트랜스코더블 메커니즘은 콘텐츠의 생성, 트랜스코딩, 안전한 콘텐츠의 전달과 같은 과정으로 구성되었으며 전 과정에서 보안수준을 협약하고, 재조정하는 보안정책의 제어를 필요로 한다.

<그림 1>의 IPTV 정보보호 서비스 구조에서, 서비스 제공자 측의 부분(Selective) 암호 기능블록은 비디오 인코더와 상호협력을 하여 안전한 트랜스코더블 콘텐츠를 생성한다. 이러한 부분 암호 기능블록은 서비스 제공자의 정보보호 정책에 의해 제어되어야 한다. 정보보호 정책 관리 기능블록은 단말 단의 기능블록과 암호타입, 암호방식, 암호적용계층, 파라미터 등을 교환한다. 암호키는 키관리 기능블록에서 마련되며, 협상된 정보보호 정책과 키는 안전한 채널을 통하여 단말로 전달된다. 암호화된 콘텐츠는 전달 기능블록을 통하여 네트워크나 단말의 능력에 따라 네트워크 중간노드에서 추가적으로 트랜스코딩이 발생할 수 있으며 최종 이용자에게 전달되기까지 정보보

호 수준요구에 따라 암호화를 추가적으로 수행할 수 있다. 서비스 제공자 측면에서는 이용자 및 단말을 인증할 책임이 있다. 그 인증방법은 기존의 많은 기법들이 있으며, 이동환경에 맞게 다중 인증 메커니즘을 활용하는 것이 안전한 콘텐츠 제공 및 활용을 위한 초석이 된다. 그리고 단말 측의 부분 복호화 기능블록은 서비스 제공자에 의하여 사전에 전달된 키와 정책에 근거하여 계층적으로 암호화된 콘텐츠를 복호화 과정을 처리하면 최종 이용자는 원하는 영상을 재생할 수 있다.



<그림 1> 안전한 트랜스코더블 메커니즘 구성요소

(출처: ITU-T SG17 TD 1323 Rev.1)

향후 전망

안전한 트랜스코더블 메커니즘은 스마트 스크린 서비스에서 방송서비스 접근제어를 위하여 필수적인 정보보호 메커니즘이며, 정보보호 서비스의 종단성(End-to-end), 계층성(Scalability), 효율성(Efficiency), 적응성(Adaptiveness)을 제공한다. 본 표준초안은 2011년 4월 SG17 국제회의에서 최종 국제표준 채택을 위한 승인(Consent)을 추진할 예정이다.

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