

[정보보호] IPTV Transcodable 보안 표준동향

현재 IPTV라는 키워드로 대변하는 기술은 Digital TV, Mobile TV, Internet TV, IPTV, Mobile IPTV 등과 같은 것이 있다. 각 기술들이 방송형 서비스를 근간으로 한다는 것에는 동의하지만 IPTV 서비스가 방송·통신 융합이라는 관점에서는 약간의 견해를 달리하고 있다. 즉 방송 서비스와 통신서비스가 새롭게 융합 서비스를 창출하는 것이며, 그 융합의 특성상 정형화된 융합서비스 정의를 내릴 수 없을 뿐 아니라, 어떤 서비스가 킬러앱(Killer Application)이 될 것이라고 누구도 장담을 하지 못하는 시점인 것이다. 이러한 상황에서 각 사업자는 국내시장과 국제 시장을 동시에 공략할 수 있는 표준의 중요성을 인식하고 있다. 특히 콘텐츠 시장이 여러 개의 SDO(Standard Development Organization) 영역으로 나뉘어져 있어서 오히려 혼선을 겪고 있는 것이 현실이다.

ITU-T에서는 2006년 7월 IPTV Focus Group 제 1차 회의를 시작으로 2007년 12월까지 총 7 차례 회의가 개최되었으며, 2008년 1월 IPTV-GSI 회의로 승계되었고, 2008년 11월 24~28일 스위스 제네바에서 제 5차 회의가 준비 중에 있다. IPTV 콘텐츠 보안 관련 CAS, DRM이 주종을 이루고 있지만 X.iptvsec-1(X.1191) 표준초안에 새롭게 추가된 E2E(End-to-End) Transcodable 콘텐츠 보안 서비스와 지난 9월 제네바에서 개최된 ITU-T SG17 회의에서 한국 주도로 제안된 보안 메커니즘(X.iptvsec-2)에 대하여 살펴본다.

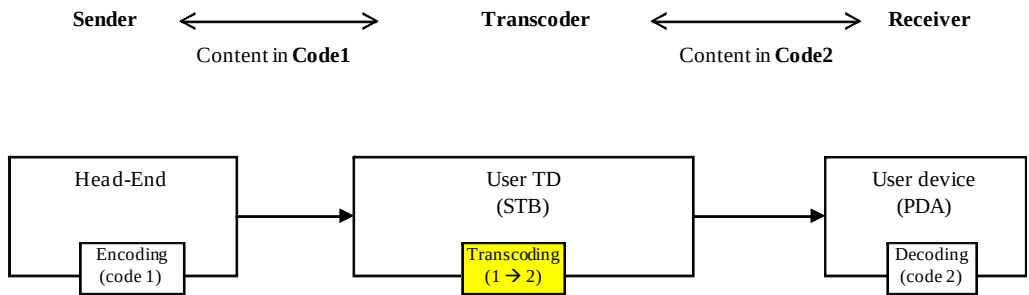
IPTV 트랜스코딩 구조

트랜스코딩은 주로 이미지, 텍스트, 오디오 및 비디오와 같은 것을 한 포맷에서 다른 포맷이나, 다른 품질(Quality)로 변환을 하는 것을 의미한다. 즉, IPTV에 이동성 서비스가 추가되면서 이에 따르는 사용자 단말기의 유형이 다양하게 변화되고, 이러한 상황에서 트랜스코딩이 중요한 역할을 하게 된다. 트랜스코딩은 <그림 1>과 같이 네트워크 중간 노드가 수행하는 것이 기본적 구조이며 다음과 같은 목적을 갖는다.

- 네트워크 한계 극복:** 광대역 네트워크로부터 전달된 콘텐츠를 협대역 접속네트워크로 전송할 때에 시간과 대역폭이 감소하는 경우
- 콘텐츠의 포맷 불일치 극복:** 사용자의 단말기가 지원하지 않는 콘텐츠 포맷이나, 단말기에 표시하기에는 너무 길거나, 화면 사이즈가 큰 콘텐츠 경우에, 전송되어진 포맷 그대로 사용자의 단말기에 표시하기가 적절하지 못한 경우
- 성능 제약 극복:** 사용자 단말기의 화면에 콘텐츠 원본의 포맷을 그대로 표시하기가 단말기의 성능이나 전원의 제약사항으로 문제점이 있는 경우
- SCP 간 불일치 극복:** 한 도메인에 속한 콘텐츠 보안 메커니즘인 SCP(Service & Content Protection)를 다른 도메인의 단말이 지원하지 못하는 경우

헤드엔드는 원본의 콘텐츠를 Code1으로 코딩하고, STB(Set-Top Box)에서 콘텐츠를 Code1

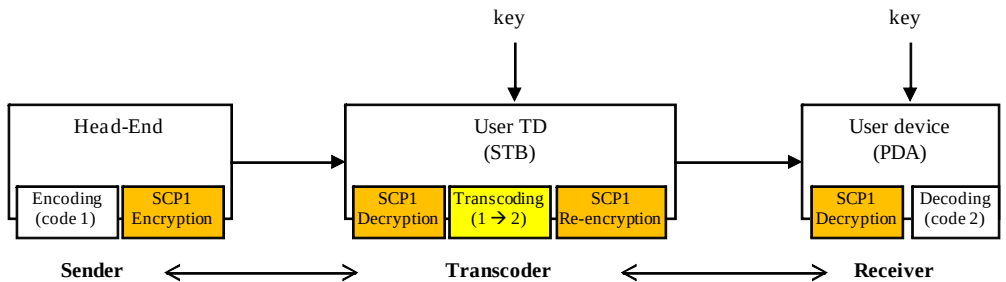
에서 Code2로 변환(트랜스코딩)하면, 최종 사용자 단말은 Code2로 포맷되어진 콘텐츠를 받아보게 된다. 수신 단말기는 Code2만을 인식할 수 있기 때문에 중간 노드인 트랜스코더가 Code2 포맷으로 원본 콘텐츠를 변환하여 전송하는 것이다.



<그림 1> Transcoding Architecture

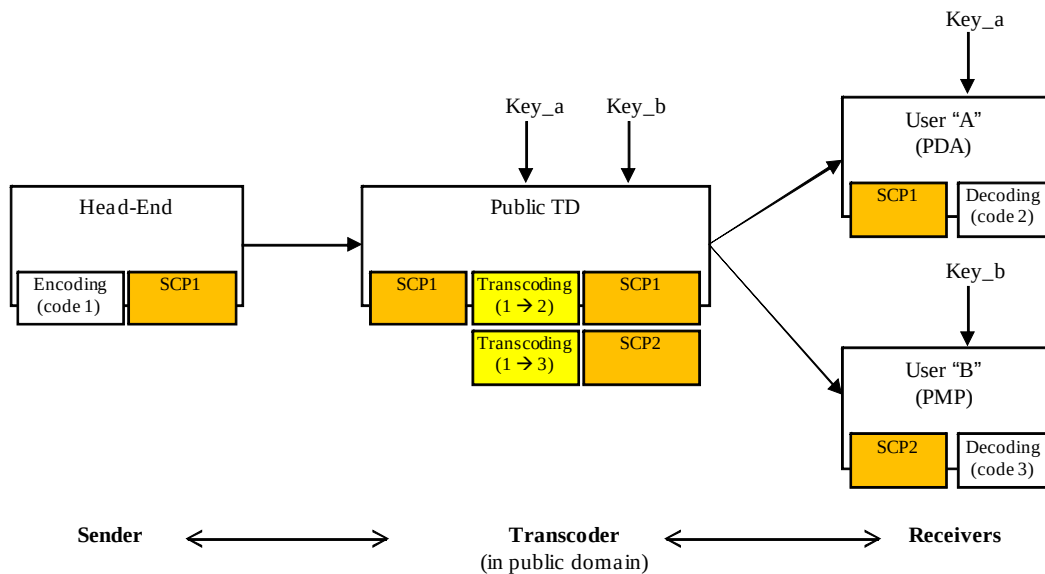
전통적 IPTV 트랜스코딩 보안 메커니즘의 문제점

IPTV의 콘텐츠들은 하나의 SCP를 사용하여 보호를 한다. 콘텐츠는 최종 이용자에게 권한이 이양되기 때문에, 콘텐츠는 트랜스코딩을 하기 전, 하는 동안, 그리고 후에도 반드시 보호되어야 한다. <그림 2>는 전통적인 트랜스코딩 구조로, 불필요한 복호와 재암호가 필요한 트랜스코딩이다. 3개의 노드가 동일한 서비스 도메인에 속하므로, 단일한 SCP를 사용하는 경우이다. 하지만 트랜스코더는 트랜스코딩을 위하여 원본 콘텐츠를 얻기 위하여, 복호 그리고 암호 처리를 수행하여야만 한다.



<그림 2> Transcoding Architecture with Protection

좀 더 복잡한 경우를 생각해 볼 수 있는데, <그림 3>은 트랜스코더가 무선랜의 경우와 같이 “Hot-Spot” 서비스 지역에 놓여 있는 경우를 생각할 수 있다. 여러 개의 SCP를 지원하는 트랜스코더는 SCP2를 인식하는 수신 단말기를 위하여 SCP1의 콘텐츠를 SCP2로 트랜스코딩을 해주어야 한다. 이런 경우 SCP2를 지원하는 단말기는 수신되는 콘텐츠를 변환할 필요가 없고, 단순히 동일한 인터페이스를 유지하기만 하면 되는 장점을 가지게 된다.



<그림 3> Multiple Transcodings and Multiple Protections

향후 전망

방송·통신 융합서비스인 IPTV는 방송서비스와 통신서비스의 융합으로 탄생된 서비스이다. CAS는 방송용 콘텐츠를 보호하는 메커니즘이며, DRM은 통신용 콘텐츠를 보호하는 메커니즘이다. 방송·통신 융합서비스인 IPTV 콘텐츠를 보호하기 위해서는 현재의 방안으로는 CAS와 DRM의 연동 또는 통합 방안이 제시되고 있다. 그러나 방송과 통신서비스 보안의 공통점을 추출하고 이에 걸 맞는, 즉 E2E를 지원하고, 이동성을 지원하며, 다양한 단말 지원이 용이한 새로운 Transcodable 보안 메커니즘이 필요성이 인식되고 있으며, 이에 대한 기술 표준으로 MPEG4(H.264) 또는 향후 SVC(Scalable Video Codec) 기반의 IPTV 보안 메커니즘 표준화가 활발히 진행되고 있다.

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