제4회 정보통신표준화 우수논문집

최 우 수 상

CAS와 DRM의 연동을 위한 표준 인터페이스에 관한 연구

A research on standard interface for interoperability between CAS & DRM

남도원, 정연정, 윤기송 /
한국전자통신연구원

Do-Won Nam, Yeonjeong Jeong, Kisong Yoon
Electronics and Telecommunications Research Institute

CAS와 DRM의 연동을 위한 표준 인터페이스에 관한 연구

A research on standard interface for interoperability between CAS & DRM

남도원, 정연정, 윤기송 / 한국전자통신연구원
Do-Won Nam, Yeonjeong Jeong, Kisong Yoon /
Electronics and Telecommunications Research Institute

요 약

통신과 방송이 융합되고 그 경계가 모호해짐과 동시에 사용자들은 다양한 단말기에서 통신, 방송의 구분 없이 콘텐츠를 소비하고 있다. 불법 복제나 인터넷을 통한 불법 유통으로부터 콘텐츠와 저작권자를 보호하고 허가받은 사용자만을 콘텐츠에 접근할 수 있도록 해 주었던 저작권 보호 기술은 자신이 소유한 다양한 단말기에서 콘텐츠를 자유롭게 이용하고자 하는 사용자들의 요구를 가로막는 장애 요인이 되고 있다. 모든 단말기에서 동일한 저작권 보호 기술을 채택할 수는 없는 상황에서 이를 해결하기 위한 현실적인 대안은 저작권 보호 기술간의 연동을 통해 다양한 단말기 사이에서 콘텐츠가 유통될 수 있는 안전한 경로를 제공하는 것이다. 본 논문에서는 방송 서비스가 사용자에게 제공해 온 풍부한 양질의 콘텐츠를 PC, PVR, 휴대단말 등에서 자유롭게 이용할 수 있도록 하기 위해 방송 서비스에서 이용되고 있는 제한수신 시스템(CAS) 기술과 일반 사용자 단말의 DRM 기술간의 연동을 위한 표준 인터페이스를 다루도록 한다.

I. 서론

2007년 6월에 TTA 운영위원회에서는 방송 콘텐츠 보호 시스템과 DRM간의 연동 기술에 대한 표준화 과제를 승인하였다. 이 표준화 과제는 정보보호 기술위원회 산하의 DRM 프로젝트 그룹에서 진행되고 있으며 CAS 기술로 보호된 방송 콘텐츠를 DRM 기술로 보호된 콘텐츠로 변환하기 위한 표준 프로세스와 기술 규격의 작성을 목표로 하고 있다. 여기서 진행중인 표준은 이미 다양한 CAS 기술과 DRM 기술이 시장에 존재하고 있음을 전제로 하여 이들 간의 N:M 조합에 따른 자유로운 연동이 가능하도록 하고 있으며, 방송 콘텐츠가 DRM 콘텐츠로 변경된 이후의 유통 과정에 대한 방송 사업자의 정책을 반영할 수 있도록 하고 있다. 본 논문에서는 이러한 목표를 달성하기 위해 CAS+DRM 연동 표준에서 다루어야 할 이슈와 접근 방법, 그리고 작성된 표준 규격에 대해 다루도록 한다.

II. 기술 동향

1. CAS 기술

CAS 기술은 방송 사업자가 방송 콘텐츠를 스크램블하여 전송하고, 허가 받은 사용자만이 이를 언스크램블하여 시청할 수 있도록 제어하기 위한 기술이다. DVB 표준 규격[1]에서는 CA ID를 명시하기 위한 필드만을 제공하고 CAS의 세부적인 메커니즘이나 구현 방법은 각 CAS 기술 제공사에게 맡기고 있는데, 이로 인해 CAS 기술 제공사가 시장과 기술에 있어서 자유롭게 경쟁하며 발전시킬 수 있도록 하고 있다. 현재 NDS, Irdeto Access, Nagravision을 비롯한 많은 업체들에 의해 시장이 분할되어 있으며 유료 방송 사업자마다 그들에게 적합한 CAS 기술을 채택하고 있다.

최근에는 하나의 셋톱박스 단말기 상에서 다양한 CAS 기반의 방송 서비스를 받을 수 있도록 하기 위해 DCAS(Downloadable CAS) 기술이 개발되는 추세이며 IPTV나 모바일 방송과 같은 새로운 비즈니스 영역으로의 확장을 위한 기술 개발 및 표준화[2] [3]가 진행되고 있다.

2. DRM 기술

DRM 기술은 사용자가 자신이 부여받은 권한과 조건의 범위 내에서만 디지털 콘텐츠를 이용할 수 있도록 제어하는 기술로 CAS 기술이 방송 서비스에 한정되어 있는 것과 달리 특정한 서비스에 종속되지 않고 디지털 콘텐츠에 대한 저작권 관리 전반 기술을 의미하고 있다. 본 논문에서는 방송 서비스 제공자가 방송 콘텐츠의 보호를 위해 사용하는 기술을 CAS로 지칭하고, CAS 이외의 콘텐츠 보호 기술을 DRM으로 구분하여 사용한다.

MPEG-21[4]이나 DMP[5], OMA 등과 같은 DRM 기술의 표준화에 관한 움직임이 있어 왔으나 모바일 환경에서의 OMA 기술을 제외하면 실질적으로 이용되는 표준 기술은 거의 없다고 봐도 무방하다. DRM 간의 연동을 위해 Coral[6] 이나 DReaM[7]과 같은 기술이 시도되고 있으나 비즈니스 상의 제휴 관계를 이용한 서비스 규격이거나 공통 라이센스 포맷을 이용한 기술이어서 쉽게 확산되기 어려운 상황이다. 국내에서는 음악 콘텐츠와 동영상 콘텐츠와 같은 다운로드형 DRM 기술간의 연동을 위한 EXIM 기술이 표준화 되어 있다.[8] [9]

III. 표준 기술에 대한 요구사항

CAS+DRM 연동 기술의 표준화에서는 다음과 같은 세가지의 원칙을 우선적으로 고려한다. 첫번째는 표준이 기술의 난립으로 인한 혼란은 줄이되 기술의 발전을 제한하거나 시장에서의 경쟁을 저해하지는 않아야 한다는 것이다. CAS와 DRM간 연동의 필요성이라는 것이 시장에 서로 호환되지 않는 다양한 CAS와 DRM 기술

이 존재하기 때문에 발생하는 것이긴 하지만, 이를 모든 CAS와 DRM이 단일한 표준 규격을 준수하여 호환성 있게 만들도록 강제함으로써 해결하려 한다면 결국 더 나은 기술로 발전시키기 위한 연구 개발을 가로막는 결과를 낳을 것이다. MPEG-21, DMP, OMA 등과 같은 표준화 활동에서 잘 정의된 DRM 기술 규격을 만들고는 있지만 이 기술 규격이 현재와 가까운 미래에 생길 수 있는 다양한 비즈니스 모델과 요구사항들을 모두 커버할 수 있는 것이 아닌 이상 모든 CAS와 DRM이 단일 표준 규격으로부터 만들어질 수는 없는 것이다.

두번째는 CAS와 DRM은 기본적으로 보안 기술에 속하기 때문에 상호 연동을 위해 상호간에 기술의 세부적인 내용을 공개하는 것은 결국 보안성의 약화로 이어진다는 것이다. DMP나 OMA의 표준에서는 non-DMP 이거나 non-OMA 기반의 장치로 콘텐츠를 반출(export)할 경우, 보호 기술이 해제된 원본 콘텐츠를 전송하는 것으로 정의하고 있으며 이를 수신한 DRM 장치가 자신의 DRM 콘텐츠 포맷으로 패키징하는 것을 기본으로 하고 있다. 원본 콘텐츠를 연동의 대상이 되는 두 보호 기술 간에 전송하는 것은 보호기술이 해제된 콘텐츠가 유출될 위험이 높다는 것을 의미한다. 하지만 이를 송신측 DRM이 수신측 DRM 규격에 따라 콘텐츠를 제공하거나(송신측 DRM이 수신측 DRM의 기술 규격을 알고 있을 경우) 수신측 DRM이 송신측 DRM 규격에서 자신의 콘텐츠를 생성(수신측 DRM이 송신측 DRM의 기술 규격을 알고 있을 경우)하지 않는 것은 양자간에 기술 규격을 공개하는 것이 해당 보호 기술의 보안성을 완전히 무너뜨리는 것이 되기 때문이다. 따라서 OMA, DMP 등의 규격에서는 원본 콘텐츠의 전송을 기본 전제로 하고 이에 대한 적절한 보호 조치를 갖추도록 요구하는 선에서 표준을 제정하는 것이다.

세번째로 사용자가 콘텐츠를 이용하고자 하는 단말기에는 다양한 CAS나 DRM이 탑재되고 있으며 연동을 위해 특정한 CAS나 DRM을 요구하지 않아야 하며 사용자의 단말기에 대한 선택권을 제한하지 않아야 한다. 현재 사용되고 있는 CAS와 DRM 기술은 매우 다양하다. 이 제품들 중에는 CAS로 보호된 방송 콘텐츠를 수신하여 DRM 기반의 콘텐츠로 저장해 주는 PVR 장치도 있다. 하지만 이러한 장치는 자체에 내장된 특정 CAS 기술과 특정 DRM 기술만을 연동시켜주고 있으며 이를 통해 생성된 DRM 콘텐츠를 사용자가 원하는 단말기에서 이용할 수 있도록 해 주지 못하고 있다. 즉, CAS 기술과 DRM 기술을 연동은 시켜주되 특정 CAS와 특정 DRM 만을 지원함으로써 콘텐츠 이용 단말기에 대한 사용자의 선택권을 보장해 주지 못하는 것이다. 표준 기술은 특정 업체의 기술간 연동을 위한 것이 아니라 N 가지의 CAS 기술과 M 가지의 DRM 기술 사이에 NxM 이나 되는 다양한 조합을 모두 지원할 수 있는 보편적인 구조를 가져야 한다.

본 논문에서는 이상과 같은 세가지의 원칙에 입각한 CAS+DRM 연동 기술의 모델링 과정과 그 결과로 작성된 세부 표준 기술에 관해 설명한다.

Ⅳ. 표준 기술 모델링

CAS+DRM 연동 기술을 모델링 하기 위한 전제가 되는 세가지 원칙을 간략히 요약해 보면 다음과 같다.

① 연동 표준으로 인해 CAS와 DRM 개별 기술의 형태와 발전에 제약이 가해지지는 않아야 한다.
② CAS와 DRM 상호간에 보안 기술의 세부적인 내용이 공개되지 않아도 연동이 가능해야 한다.
③ 임의의 CAS, DRM 조합간에도 연동이 가능한 구조를 가져야 한다.

이러한 각각의 원칙에 따라 연동 기술이 가져야 할 특징과 형태를 설계해 보자.

1. 개별 기술에 대한 비 제약성

CAS와 DRM 기술은 세부적인 기술에 있어서는 서로 다른 형태를 가지고 있지만 일반적인 메커니즘은 대부분 유사하다.

CAS의 경우 방송 서비스 제공자의 서버 환경에서 방송 콘텐츠를 스크램블 하고, 스크램블된 콘텐츠가 전송 네트워크를 따라 사용자의 셋톱박스에 도달하게 된다. 사용자에 따라 제공된 방송 콘텐츠에 대한 접근 권한이 다른데, CAS 기술에서는 허가된 사용자에게 스크램블된 콘텐츠를 언스크램블할 수 있는 키(key)를 ECM/EMM 이라는 자격부여 메시지에 담아 제공한다. 사용자는 자신에게 주어진 키를 이용하여 콘텐츠로부터 스크램블을 해제하여 재생하게 되며 방송 서비스 제공자에 위치한 CAS 서버는 각 사용자마다의 방송 콘텐츠 접근 권한을 관리하고 이에 관한 적절한 키 관리 체계를 수립하는 것이다.

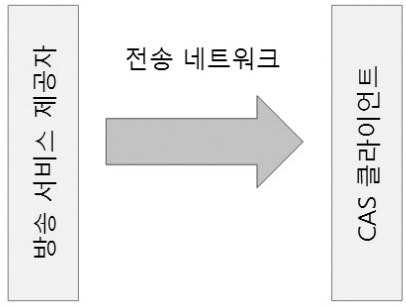
DRM의 경우는 암호화 기술로 콘텐츠를 패키징하여 암호화된 DRM 콘텐츠를 생성하고 이를 사용자에게 전송한다. 사용자가 DRM 콘텐츠를 재생하기 위해서는 암호화를 해제해야 하는데, 이를 위해 필요한 복호화 키는 라이센스라는 정보체에 담긴채로 사용자에게 전달된다. 라이센스에는 DRM 콘텐츠를 복호화 하기 위한 키 뿐만 아니라 사용자에게 부여된 콘텐츠의 사용 기간과 재생 횟수와 같은 여러 가지 권한과 이용 조건이 명시되어 있으며, DRM 클라이언트는 이러한 권한과 조건의 범위 내에서만 사용자가 콘텐츠를 이용할 수 있도록 제어하는 역할을 한다.

CAS 기술에 있어서 각각의 개별적인 기술 제공사는 독자적인 스크램블 방식, 사용자 관리 체계, 키 관리 및 업데이트 메커니즘 등과 같은 부

분을 서로 차별화 하고 있으며, DRM 기술의 제공사는 DRM 콘텐츠의 포맷, 암호화 알고리즘 및 키 관리 체계, 라이센스 발급 기술 및 클라이언트 제어 기술과 같은 부분을 서로 차별화 하고 있다. CAS+DRM 연동 기술이 이와 같은 개별 기술의 차별화나 발전에 대해 제약을 가하지 않도록 하려면 각각의 CAS, DRM 기술의 특징이 되는 세부 기술에 대해 특정 기술이나 구조를 요구하지 않아야 한다. 현재 CAS 기술에서는 하나의 셋톱박스 단말기에서 여러가지 CAS가 동작할 수 있도록 하기 위해 스크램블 알고리즘을 표준화 하고, CAS 모듈을 셋톱박스 장치와 분리할 수 있도록 하는 DCAS (Downloadable CAS) 기술을 표준화 하고 있다. 하지만 CAS+DRM 연동 기술은 DCAS 기술보다도 훨씬 기술 바깥에서 규격이 만들어 져야 하며, 스크램블 알고리즘과 같은 세부적인 부분까지 건드리지 않아야 한다.

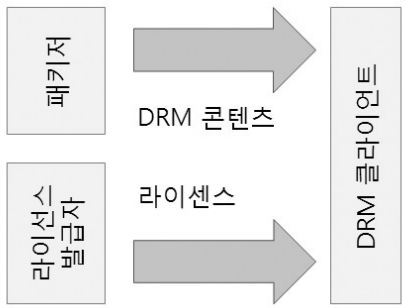
DRM 기술 역시 기술 제공사에 따라 독자적인 DRM 콘텐츠 포맷, 메타데이터 기술 언어, 사용권한 및 조건에 대한 기술 언어, 암복호화 알고리즘, 라이센스 발급 메커니즘, 클라이언트 제어 기술 등의 특징 있는 기술로 차별화 하고 있다. CAS+DRM 연동 기술을 위해 특정 DRM 콘텐츠 포맷을 강제하거나 기술언어, 알고리즘과 같은 DRM 세부 기술을 규격화 하는 것은 바람직하지 않으며, 그러한 세부 기술과 조금 멀리 떨어져서 일반적인 DRM 기술의 형태를 기준으로 한 규격을 제시해야 한다.

이러한 관점에서 CAS 기술과 DRM 기술을 간소화 시켜보면 다음 그림과 같다.



(그림 4-1) CAS

CAS 기술은 위 그림과 같이 방송 서비스 제공자, 전송 네트워크, CAS 클라이언트로 크게 구성될 수 있다. 이는 현재 시장에 나와 있는 CAS 기술의 공통적인 형태이며 CAS+DRM 연동 기술에서는 이 형태에서 더 세부적인 부분으로 접근하지는 않아야 한다.

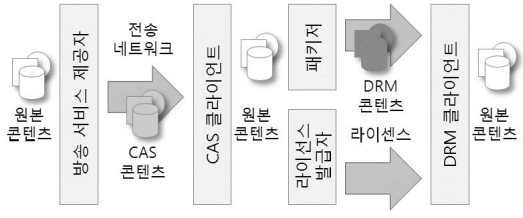


(그림 4-2) DRM

DRM 기술은 위 그림과 같이 패키저, 라이센스 발급자, DRM 클라이언트로 크게 구성되며, 현재의 DRM 기술들의 공통적인 형태라 할 수 있다.

앞서 표준 기술에 대한 요구사항 두번째 항목에서 예시했듯이 OMA, DMP 등의 규격에서는 콘텐츠 보호 기술간의 비 공개성을 이유로 원본 콘텐츠를 통한 반출(export), 반입(import)를 이용하고 있다. 그림 1, 2 에 콘텐츠의 흐름을 더하게 되면 (그림 4-3)과 같은 CAS+DRM 연동 흐름도가 된다.

방송 서비스 제공자가 보유한 원본 콘텐츠는 CAS 기술에 의해 CAS 콘텐츠로 변경이 되고 이는 CAS 클라이언트에서 다시 원본 콘텐츠로 환원된 이후 재생된다. 환원된 원본 콘텐츠는 DRM 패키저에 입력되어 DRM 콘텐츠로 변환되고 DRM 클라이언트에서 원본 콘텐츠로 다시 환원되어 사용자가 이용하는 형태를 가진다.



(그림 4-3) CAS+DRM 연동 흐름도

2. 보안 기술의 비 공개성

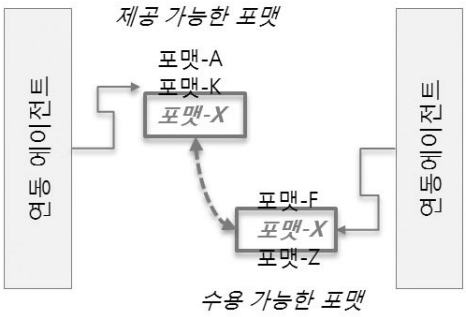
콘텐츠의 경우에는 원본 콘텐츠라는 기술 중립적인 매개체가 존재하지만, 연동 과정에서 변환되어야 할 것에 콘텐츠만 있는 것은 아니다. CAS 기술에서 제시한 콘텐츠의 사용 권한이나 그에 따르는 조건들, 그리고 콘텐츠에 대한 부가 정보를 담고 있는 메타데이터 역시 연동을 통해 변환 되어야 하는 것들이다. 각각의 CAS, DRM 기술은 지원 가능한 비즈니스 모델이나 서비스 형태, 콘텐츠 타입에 따라 다양한 형태의 사용 권한이나 메타데이터 규격을 마련하여 이용하고 있고, 이러한 정보 역시 비 공개성을 원칙으로 하는 중요한 요소이다.

이와 같은 정보의 변환을 위한 기존의 기술들은 크게 몇가지로 나뉠 수 있다. 정보의 송신측과 수신측이 존재하고 송신측의 정보 포맷을 송신측 포맷, 수신측의 정보 포맷을 수신측 포맷이라고 할 때, 첫번째로 송신측이 수신측 포맷을 알고 있어서 수신측 포맷에 맞추어 변환한 후 전송하는 방식이 있고, 두번째로 수신측이 송신측 포맷을 알고 있어서 수신한 정보를 수신측에서 자신의 포맷으로 변환하는 방식이 있으며, 세번째로 송신측과 수신측이 공통으로 알고 있는 중립 포맷을 설정하여 송신측은 송신측 포맷을 중립 포맷으로 변환하여 전송하고, 수신측은 수신한 중립 포맷의 정보를 다시 수신측 포맷으로 변환하는 것이다.

첫번째와 두번째 방식은 둘 중 어느 한쪽의 정보 포맷을 상대방에게 알려주어야 하므로 이로 인해 보안상의 위험도가 증가할 수 있고, 양측 어느 한쪽의 포맷에 업데이트가 가해진 경우에 이를 다시 상대방에게 알려주어야 한다는 문제가 발생한다. 세번째 방식은 양측이 중립 포맷을 이용하여 통신하므로 각자 자신의 비밀스러운 포맷의 세부 사항을 상대방에게 노출하지 않아

도 되므로 보안상의 이점이 있으나 중립 포맷이 얼마나 풍부한 표현 방식을 제공하느냐에 따라 포맷 변경 시의 정보 손실이 최소화 된다는 측면을 고려해야 한다. 즉, 중립 포맷은 모든 송신측, 수신측 포맷을 오류없이 기술할 수 있어야만 송신측과 수신측 사이의 정보 교환에서 의미상의 오차가 발생하지 않는다는 것이다.

우리가 사용한 방법은 보안 기술의 비 공개성이 지켜지는 세번째의 중립 포맷 방식을 이용하되, 정보 교환에서의 오류 가능성을 줄이기 위해 송신측과 수신측이 어떤 중립 포맷으로 정보를 주고 받을 것인지 양자간의 협의하에 결정하는 협상 기법을 도입하는 것이다.



(그림 4-4) 협상에 의한 중립 포맷 결정

위 그림과 같이 CAS, DRM 기술간에 교환할 사용 권한이나 메타데이터와 같은 정보는 중립 포맷을 이용하여 교환하도록 하되, 교환 이전에 양측의 협상 과정을 통해 어떠한 포맷을 중립 포맷으로 삼을 것인지를 미리 결정하도록 하는 것이다.

3. 임의의 조합간 자유로운 연동

현재의 CAS, DRM 제품을 보면 CAS에 DRM 기능을 확장한 것과 DRM에 CAS 기능을 확장한 것들이 있다. 이는 방송 서비스/셋톱박스 환경과 유무선 인터넷/PC, 모바일 단말기라는 그동안 분리되어 있던 사업 영역에서 각각 개발해 왔던 기술이 통방 융합이라는 현재의 트렌드에 맞추어 각자의 개발 영역을 확대하는데 따른 결과이다. 셋톱박스를 기반으로 한 방송 서비스에 주력하던 CAS 기술은 DRM 기술을 받아 들여 셋톱박스의 CAS 클라이언트 이후의 콘텐츠 보호에 이용할 수 있는 기술로 확대하고 있고, PC나 모바일 단말 등을 중심으로 한 콘텐츠 유통에 주력하던 DRM 기술은 CAS 기술을 받아 들여 방송 서비스를 넘보고 있는 것이다.

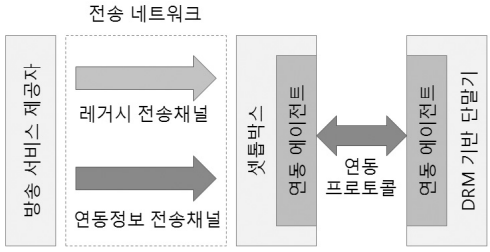
하지만 이러한 제품들이 채택하고 있는 CAS와 DRM 간의 연동 기술은 자사의 CAS와 DRM 간의 연동이나 제휴관계를 맺은 특정 몇몇 DRM 제품과의 연동만을 지원하고 있는데다가, 새로운 제휴관계를 맺은 DRM 기술이 추가되면 이를 위해 새로운 연동 소프트웨어를 추가하는 형식을 취하고 있다. 결국 N가지의 CAS 기술과 M가지의 DRM 기술이 연동하기 위해서는 각각의 CAS 기술마다 M가지의 DRM과 연동하기 위한 노력이 필요하므로 모두 NxM 이라는 많은 비용이 소요된다. 이러한 접근 방법은 표준 기술에서는 채택하기 곤란하며 우리가 목표로 하는 임의의 CAS 기술과 DRM 기술 조합간의

연동을 쉽게 지원한다는 목표와도 부합되지 않는다.

이를 위해 우리는 CAS 기술과 DRM 기술 사이의 연동을 위한 표준 인터페이스를 제안한다. 이는 CAS 기술이 표준 인터페이스를 지원하고 다시 DRM 기술이 이 표준 인터페이스를 지원함으로써 CAS와 DRM 기술이 표준 인터페이스를 통해 연동하게 하는 방식인데, N가지의 CAS 기술은 각각 한가지 표준 인터페이스만을 지원하면 되고, M가지의 DRM 기술 역시 표준 인터페이스만 지원하면 연동이 가능하게 된다. 기존 제품들이 취하고 연동 방식 구현에 NxM 만큼의 자원이 소요된다면 표준 인터페이스 방식에 필요한 자원은 N+M 밖에 되지 않으므로 훨씬 저비용으로 다양한 조합간 연동이 가능하다는 장점이 있다.

V. 연동 표준의 구성

CAS+DRM 연동을 위한 표준은 (그림 4-3)에서 도식화 한 CAS+DRM 연동 흐름도로부터 도출된 (그림 5-1)과 같은 연동 시스템 구성에 기반하여 작성된다.



(그림 5-1) 연동 시스템 구성

연동 시스템은 CAS 기반의 방송 서비스와 DRM 기반의 사용자 단말기가 연결된 형태를 가지며 연동을 위한 표준 인터페이스는 이 두가지가 서로 만나는 곳에 위치하게 된다.

① 방송 서비스 제공자

사용자에게 방송 서비스를 제공하는 주체로 방송 콘텐츠를 관리하고 콘텐츠에 대한 사용자의 이용 권한을 결정하며 CAS 기술을 이용하여 콘텐츠를 스크램블해서 사용자의 단말기(셋톱박스)로 전송한다.

② 전송 네트워크

방송 콘텐츠가 방송 서비스 제공자로부터 사용자 단말로 전송되는 경로를 말하며, 케이블 네트워크, 공중파, 위성, IP 네트워크 등의 여러 가지가 있다. 또한 그 특성에 따라 단방향 네트워크로 구성될 수도 있고 양방향 네트워크나 단방향 네트워크와 별도의 리턴 채널이 조합된 형태가 될 수도 있다.

③ 레거시 전송 채널

전송 네트워크 상에서 CAS 기반의 방송 서비스를 위해 이용되었던 전송 채널을 말하며, 이를 통해 콘텐츠, ECM/EMM 메시지 등이 전송된다.

④ 연동 정보 전송 채널

CAS와 DRM의 연동을 위해서는 기존의 레거시 전송 채널을 통해 전송되었던 것 이외의

추가적인 정보가 필요하며 이러한 정보가 전송되는 채널을 말한다. 실제의 구현에 있어서는 이러한 정보를 별도의 채널로 전송하지 않고 기존의 레거시 전송 채널을 통해 전송할 수도 있다.

⑤ 연동 에이전트

CAS 기술과 DRM 기술 사이에서 방송 콘텐츠의 상호 연동을 위해 인증 정보의 교환, 연동 파라미터의 협의, 데이터 전송 등을 담당하는 모듈이다. CAS와 DRM의 연동 과정은 양측의 연동 에이전트간 인증, 협상, 데이터 전송 과정이며 이들은 연동 프로토콜에 따라 동작한다.

⑥ 연동 프로토콜

CAS측 연동 에이전트와 DRM측 연동 에이전트 사이의 상호 인증을 위한 등록 과정, 정보의 교환을 통한 연동 파라미터의 협의, 연동 파라미터에 따른 데이터 패킷 전송 과정 등에 대한 절차 및 프로토콜의 집합이다.

이와 같은 연동 시스템 구성에서 표준화의 대상이 되는 것은 연동 프로토콜이며 연동 정보는 특별한 기술적인 규격화 없이 연동 과정에 필요한 데이터 항목만을 나열한다. 이는 연동 정보의 포맷이나 전달 방식 등이 CAS 기반의 방송 서비스 사업자에 의해 독자적으로 결정되어도 무방하기 때문이며 비즈니스 형태에 따라 어떠한 정보를 어떻게 관리할 것인지를 스스로 자유롭게 결정할 수 있도록 하기 위함이다.

VI. 연동 정보

표준에서 목표로 하는 것 중에 표준에서 제시한 인터페이스를 지원하는 임의의 CAS와 DRM 사이에 연동이 가능하도록 한다는 부분이 있다. 기술적으로는 당연히 그렇게 해야 하는 부분이지만 실제로 비즈니스를 수행하는 입장에서는 제휴관계가 있거나 자신이 신뢰하는 DRM 기술과만 선택적으로 연동을 수행하고 싶을 것이다. 또한 DRM 콘텐츠로 저장된 이후의 사용 권한 및 이용 제약 조건과 같이 CAS 기반의 방송 서비스에서는 필요하지 않았던 정보가 CAS+DRM 연동을 위해 추가로 요구되기도 한다. 어떠한 대상과 연동을 수행할 것인지, 그리고 어떠한 권한과 제약 조건하에서 연동을 수행할 것인지 방송 서비스 사업자가 직접 결정하고 이러한 결정 사항을 연동 에이전트에 전달하는 과정이 필요하다.

연동 정보는 CAS+DRM 연동을 의도한 대로 수행하기 위해 방송 서비스 사업자가 추가로 전송해 주어야 하는 정보를 말하며 다음과 같은 정보들이 포함된다.

① 연동 정책

어떠한 조건이 만족되어야 CAS+DRM 연동을 허가할 것인지에 대한 정책 정보를 의미한다. 예를 들어 화이트리스트에 포함된 DRM 기술에 대해서는 연동을 허가하고 블랙리스트에 포함된 DRM 기술에 대해서는 허가하지 않는 등의 정책이 포함되며, 이러한 정책 정보를 주기적으

로 서버를 통해 업데이트 하거나 비정기적으로 서버에서 즉시 전송되도록 하는 등의 여러 가지 정책이 지정될 수 있다.

② 인증 정책

CAS측, DRM측 연동 에이전트는 상호간의 인증과 주고 받는 프로토콜 메시지의 무결성 보장 등의 목적으로 인증서를 이용하게 되는데, 이러한 인증서의 신뢰 조건을 인증 정책으로 제공할 수 있다. 이러한 정책에는 사설 인증 기관으로부터 발급된 인증서를 인정하지 않거나 특정 인증 기관이 발급한 인증서만을 신뢰하는 등의 내용이 포함될 수 있다.

③ 사용 권한

방송 서비스 제공자가 전송한 방송 콘텐츠는 연동 과정을 통해 CAS의 제어에서 벗어나 DRM의 제어로 넘어간다. 방송 서비스 제공자는 DRM의 제어로 넘어간 이후에도 자신들이 설정한 범위와 조건 내에서만 콘텐츠가 이용될 수 있도록 제한하고자 할 것이며 이를 명시한 정보가 사용 권한 정보이다. 이러한 사용 권한 정보는 DRM 기술에서 사용하고 있는 사용 권한 기술 언어로 변환되고, 변환된 권한과 제약조건은 DRM 기술의 라이센스에 명시되어 DRM의 제어로 넘어간 방송 콘텐츠에 적용된다.

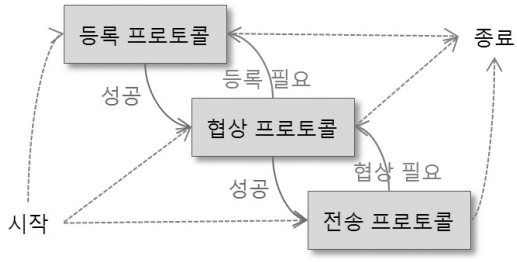
④ 메타데이터

콘텐츠에 대한 각종 부가 정보를 담고 있다. 콘텐츠의 식별 정보를 비롯하여 제목, 제작자, 저작권자 등을 비롯하여 콘텐츠의 해상도, 코덱, 데이터 전송률 등과 같은 기술적인 내용도 담고 있다. 이러한 정보는 DRM 기술에서 사용하는 메타데이터 포맷으로 변환되어 DRM 콘텐츠나 라이센스 등에 기록된다.

예시한 이외에도 필요에 따라 추가로 정보를 전송하거나 일부 정보를 전송하지 않을 수 있으며 이는 방송 서비스 제공자의 결정에 맡겨진다. 또한 이러한 정보의 포맷이나 전송 방법 등은 CAS 기반의 방송 서비스의 내부에서 동작하는 것이므로 연동 시스템을 구현하는 개발사에게 전적으로 일임되어 자유롭게 설계 가능하도록 한다.

VII. 연동 프로토콜

연동 프로토콜은 CAS측, DRM측 연동 에이전트가 방송 서비스 제공자의 방송 콘텐츠를 CAS 기술로부터 DRM 기술로 전달하기 위한 절차에 대한 기술적인 규격이다. 연동 프로토콜은 등록 프로토콜, 협상 프로토콜, 전송 프로토콜의 세가지 프로토콜로 구성되어 있으며 순차적 혹은 비 순차적인 동작을 모두 지원한다.



(그림 6-1) 비 순차적 연동 프로토콜

실제로 연동 과정이 수행되기 위해서는 CAS측, DRM측 연동 에이전트가 등록 프로토콜을 통해 상호 인증이 완료되어 있어야 하고, 협상 프로토콜을 통해 연동 파라미터가 모두 결정되어 있어야 하며, 전송 프로토콜을 통해 콘텐츠, 사용권한, 메타데이터가 전달 되어야 한다. 하지만 매번 콘텐츠를 연동할 때마다 등록 과정과 협상 과정을 거칠 필요가 없을 수도 있다. 예를 들어 CAS 셋톱박스에 DRM 기반의 PVR 기능이 내장되어 있을 경우, 제품의 출시시에 등록 과정과 협상 과정을 완료해 두었고 인증 정보나 협상 내용이 변경될 필요가 없다면 전송 프로토콜만을 반복적으로 수행하는 것이 효과적일 수 있다.

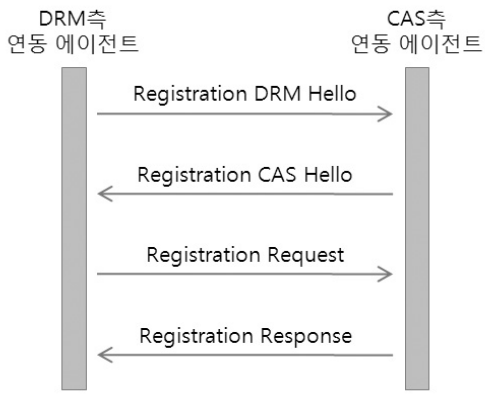
이러한 요구를 반영하기 위해 등록 프로토콜이 성공적으로 수행되면 상대측 연동 에이전트에 대한 등록 정보를 생성하여 관리하고, 협상 프로토콜이 성공적으로 수행되면 등록된 대상별로 협상 결과를 저장하여 관리하도록 한다. 이와 같이 하면 상대측 연동 에이전트로부터 협상 프로토콜이 개시되면 등록 정보를 확인하여 등록 프로토콜이 성공적으로 완료되어 있는지를 검사할 수 있다. 만약 정상적인 등록 정보가 존재한다면 등록 과정을 건너뛰고 바로 요청된 협상 프로토콜을 진행하고, 만약 등록이 되어 있지 않거나 유효 기간을 넘어선 등록 정보일 경우 등록 프로토콜을 먼저 수행한 이후 협상 프로토콜을 진행하도록 지시할 수 있다. 이와 같은 비 순차적 동작의 지원은 잦은 연동 과정에서의 반복적인 등록/협상 프로토콜 수행으로 인한 부담을 줄여줄 수 있다.

연동 프로토콜을 구성하는 세가지 프로토콜은 다음과 같으며 각 프로토콜의 첫 메시지는 DRM측 연동 에이전트가 CAS측 연동 에이전트에게 보냄으로써 프로토콜이 시작된다.

만약 CAS측 연동 에이전트로부터 CAS+DRM 연동 과정이 시작되어야 할 필요가 있다면 CAS측 연동 에이전트는 프로토콜 트리거를 생성하여 DRM측에 전송한다. 프로토콜 트리거에는 등록, 협상, 전송 중의 하나의 프로토콜이 명시되어 있으며 트리거를 수신한 DRM측 연동 에이전트는 명시된 프로토콜을 트리거 발송자를 대상으로 수행한다.

1. 등록 프로토콜 (Registration Protocol)

등록 프로토콜은 양측의 연동 에이전트 상호간에 인증 정보를 교환하고, 연동 정책에 따라 상호 인증을 수행한 후 이를 등록 정보로 기록해두기 위한 것으로 4개의 프로토콜 메시지로 구성된 4-pass 프로토콜이다.



(그림 6-2) 등록 프로토콜

① Registration DRM Hello
- 자신이 지원하는 연동 프로토콜 버전 제시
- 자신의 고유 식별자 전달 (고유 식별자는 자신의 인증서의 해쉬값을 이용한다)

② Registration CAS Hello
- 연동 과정에 사용할 프로토콜 버전 결정, 통보 (DRM측 연동 에이전트가 제시한 프로토콜 버전과 자신이 지원 가능한 프로토콜 버전을 비교하여 둘 중 낮은 버전으로 결정)
- 자신의 고유 식별자 전달 (인증서 해쉬값)
- 자신이 관리하고 있는 인증서 목록 중에서 DRM측의 식별자에 해당하는 인증서가 있는지 확인하고, 없으면 인증서 발송을 요청

③ Registration Request
- 자신이 관리하고 있는 인증서 목록 중에서 CAS측의 식별자에 해당하는 인증서가 있는지 확인하고, 없으면 인증서 발송을 요청
- CAS측의 인증서 발송 요청이 있으면 자신의 인증서를 포함한 인증서 체인 전송
- 지금까지 수신한 메시지에 대한 전자서명 발송

④ Registration Response
- DRM측의 인증서 발송 요청이 있으면 자신의 인증서를 포함한 인증서 체인 전송
- 지금까지 수신한 메시지에 대한 전자서명 발송

이상의 과정이 완료되면 양측은 연동 과정에 사용할 연동 프로토콜의 버전과 상대방의 인증서를 보유하게 된다. 실제 구현에 있어서는 상대방의 인증서를 수신하면 연동 정책이나 인증 정책에 따라 이후의 연동 과정을 진행할 것인지의 여부를 결정하게 되며 이 과정을 모두 통과해야만 등록 절차가 완료된다. 등록 프로토콜이 성공적으로 완료되면 양측은 상대방의 인증서와 등록 과정에서 확인한 정보(프로토콜 버전, 기준 시각 등)를 저장/관리한다.

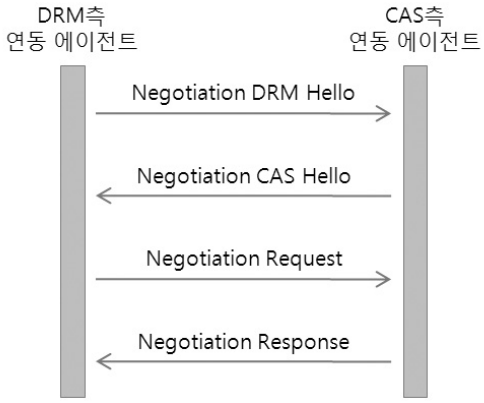
2. 협상 프로토콜 (Negotiation Protocol)

협상 프로토콜은 향후 전송 프로토콜에서 전달하기 위한 콘텐츠, 권한 정보, 메타데이터의 중립 포맷을 결정하고 연동 에이전트간의 전송 패킷의 크기와 전송 경로에 사용할 어떠한 보안 채널을 사용할 것인지를 협의하기 위한 것으로 4개의 프로토콜 메시지로 구성된 4-pass 프로토콜이다.

① Negotiation DRM Hello
- 고유 식별자를 발송한다.

② Negotiation CAS Hello
- DRM측이 보내온 식별자와 등록 프로토콜을 통해 생성/관리한 등록 정보를 참조하여 사전에 정상적으로 등록된 대상인지 검사한다. (등록된 대상이 아니면 등록 프로토콜부터 수행하도록 오류 메시지를 전송하고 종료)

– 상대방이 등록된 대상임이 확인되면 자신의 고유 식별자를 발송한다.



(그림 6-3) 협상 프로토콜

③ Negotiation Request

– CAS측의 식별자를 확인하여 자신에게 등록된 대상인지 검사. (등록되지 않았으면 등록 프로토콜부터 수행하도록 오류 메시지를 전송하고 종료)
– 중립 포맷용 권한 정보의 포맷 목록 제시
– 중립 포맷용 메타데이터의 포맷 목록 제시
– 데이터 전송 과정에 사용 가능한 채널 보안 기술의 목록 제시
– 연동 에이전트간 교환될 데이터 패킷의 최대 크기 제시
– 지금까지 수신한 메시지에 대한 전자서명 발송

④ Negotiation Response

– DRM측이 제시한 권한 정보 포맷 목록과 자신이 제시 가능한 목록을 비교하여 상호 매칭되는 포맷을 결정하여 통보 (상호 매칭되는 포맷이 없으면 오류 메시지 통보 후 종료)
– DRM측이 제시한 메타데이터 포맷 목록과 자신이 제시 가능한 목록을 비교하여 상호 매칭되는 포맷을 결정하여 통보 (상호 매칭되는 포맷이 없으면 오류 메시지 통보 후 종료)
– DRM측이 제시한 채널 보안 기술 목록과 자신이 제시 가능한 목록을 비교하여 상호 매칭되는 채널 보안 기술을 결정하여 통보 (상호 매칭되는 채널 보안 기술이 없으면 오류 메시지 통보 후 종료)
– DRM 측이 제시한 데이터 패킷의 최대 크기 범위 내에서 자신이 수용 가능한 패킷의 크기를 결정하여 통보 (수용 가능한 패킷 크기를 결정할 수 없으면 오류 메시지 통보 후 종료)
– 지금까지 수신한 메시지에 대한 전자서명 발송

이상의 과정이 완료되면 양측은 데이터 전송 과정에서 사용할 중립 포맷(권한 정보, 메타데이터)과 전송할 데이터 패킷의 크기, 데이터 패킷의 전송에 사용될 통신 채널을 위한 채널 보안 기술의 종류에 대한 합의 사항을 서로 교환하게 된다. 이렇게 합의된 내용은 협상 내용으로 저장/관리된다.

3. 전송 프로토콜 (Transmission Protocol)

전송 프로토콜은 협상 프로토콜의 결과에 따

라 콘텐츠를 적절한 크기의 패킷으로 분할하여 전송하고, 권한 정보와 메타데이터를 협의된 중립 포맷으로 변환하여 전달하기 위한 것으로 6개의 프로토콜 메시지로 구성된 6-pass 프로토콜이다.

① Transmission DRM Hello
- 고유 식별자를 발송한다.

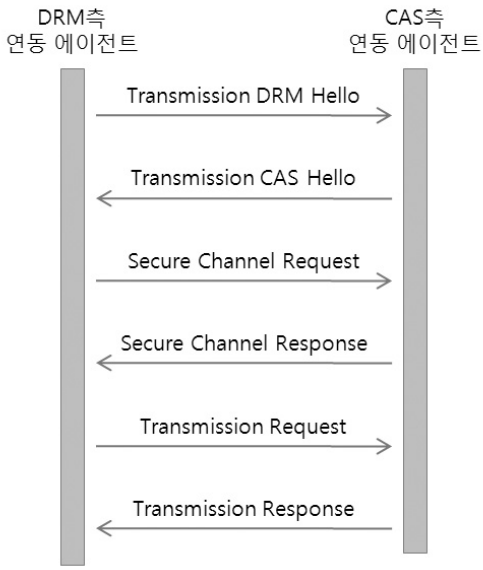
② Transmission CAS Hello
- DRM측이 보내온 식별자를 이용하여 상대방이 협상 과정을 성공적으로 마친 대상인지의 여부를 판단한다. (그렇지 않으면 협상 프로토콜부터 수행하도록 오류 메시지를 전송하고 종료)
- 대상 인증을 위해 랜덤값을 하나 생성하여 전송

③ Secure Channel Request
- 대상 인증을 위해 랜덤값을 하나 생성하여 전송
- 지금까지 수신한 메시지에 대한 전자서명 발송

④ Secure Channel Response
- DRM측에서 받은 전자서명을 확인하고 전송했던 랜덤값을 확인하여 상대방 인증 (전자서명 확인에 실패하거나 Transmission CAS Hello 메시지에서 전송한 랜덤값과 달라진 경우 오류 메시지를 보내고 종료)
- 지금까지 수신한 메시지에 대한 전자서명 발송 (DRM측은 이 전자서명의 확인에 실패하거나 Secure Channel Request 메시지에서 전송한 랜덤값과 달라진 경우 오류 메시지를 보내고 종료한다)

⑤ Transmission Request
- 데이터 패킷 전송에 대한 컨트롤 정보를 전송 (start, pause, resume, finish)

⑥ Transmission Response
- 데이터 패킷 전송 요청에 대한 응답 및 컨트롤 정보 전송



(그림 6-4) 전송 프로토콜

전송 프로토콜에서 1~4번째 메시지는 순차적으로 실행되면서 보안 채널을 확인하고 통신 대상이 등록 및 협상 과정과 동일한지 인증한다.

5번, 6번 메시지는 연동 과정에서 필요에 따라 반복적으로 주고 받게 되며 연동의 시작(start)과 종료(finish), 잠시 멈춤(pause), 전송 재개(resume) 등의 동작을 수행한다.

VIII. 평가

표준 규격을 평가하기 위한 기준은 여러가지가 있겠으나 표준 작성을 시작할 때 대전제로 삼았던 세가지 요구사항들과 작성된 표준의 특징을 기준으로 평가해 보기로 한다.

이 표준에서 규격화 한 것은 CAS측 연동 에이전트와 DRM측 연동 에이전트 사이의 프로토콜 및 인터페이스이다. 양측의 연동 에이전트는 연동을 위해 새롭게 추가된 요소이고 기존의 CAS나 DRM에 대해 어떠한 기술적 변경도 요구하지 않는다. 따라서 첫번째 전제였던 기존의 CAS, DRM 기술에 대한 비 제약성이 충족되고 있으며 CAS, DRM 각각의 개별 기술의 변경이나 발전에 영향을 주거나 받지 않는다.

CAS나 DRM에 있어서 상호간에 공개하기 곤란한 보안 항목에는 암복호화(스크램블) 알고리즘, 사용자 및 키 관리 메커니즘, 권한 정보나 메타데이터의 포맷, 클라이언트 제어 기술, 인증 기술 등이 있다. 이 표준에서는 스크램블이 해제된 콘텐츠를 보안 채널을 통해 전송하고 있고, 인증서 기반의 표준 인증 메커니즘과 협상 과정을 통해 결정된 중립 포맷의 권한 정보나 메타데이터를 이용함으로써 이러한 보안 항목들 중 어느 것도 상대방에게 알려주지 않은 채로 연동 과정이 수행된다. 따라서 두 보안 시스템의 연동으로 인해 보안에 민감한 정보의 누출로 인한 보안성의 저하는 발생하지 않는다.

마지막 전제였던 임의의 CAS와 DRM 조합간의 자유로운 연동 역시 특정 기술에 비 종속적인 규격화된 프로토콜을 제공함으로써 이루어 낼 수 있었다.

방송 서비스 사업자는 방송 콘텐츠를 이용한 비즈니스를 셋톱박스라는 한계를 벗어나 사용자가 소유한 모든 DRM 기반의 단말기로 확장할 수 있게 되었다. 연동 표준 없이는 방송 서비스 사업자가 사용자의 다양한 단말기에 DRM 기술을 제공하거나 수많은 DRM 기술 제공사와 제휴관계를 맺고 연동 소프트웨어를 제작해야 한다. 하지만, 연동 표준을 이용하면 연동 및 인증 정책만 수립하면 표준 인터페이스를 지원하는 어떤 DRM 기술과도 연동이 가능하다는 장점이 생긴다.

IX. 결론

지금까지 본 논문에서는 DRM 프로젝트 그룹에서 작성한 CAS와 DRM간 연동을 위한 표준 인터페이스 규격의 개괄적 내용과 특징에 대해 다루었다. 이 규격은 단일 장치 내에서, 혹은 네트워크나 기타 데이터 전송 채널을 통해 연결

된 CAS 기반의 셋톱박스 장치와 DRM 기반의 사용자 단말 사이에서 방송 콘텐츠와 그 사용 권한 및 제약 조건, 그리고 기타 부가 정보들을 변환하여 전송할 수 있는 절차와 XML 메시지를 이용한 프로토콜로 구성되어 있다. 여기에는 이미 시장에 널리 퍼져 있는 다양한 CAS와 DRM 기술로 인한 연동의 어려움과 두 보안 기술의 연동으로 인한 위험성을 해결하고자 하는 고민이 포함되어 있으며, 비즈니스의 용이성과 정책적인 사항을 반영할 수 있는 장치가 되어 있다.

논문의 작성 이전에 제출된 표준안은 TTA의 표준안 비준 과정을 거쳐 올해 안에 표준 채택 여부가 결정될 것이다.

>> 참고문헌

[1] DVB-CSA, ETSI Technical Report 289, 1996

[2] OMA BCAST, http://openmobilealliance.org

[3] IPTV Focus Group, ITU-T, http://itu.int

[4] MPEG-21 Multimedia Framework, ISO/IEC JTC1/SC29/WG11

[5] Digital Multimedia Project, http://dmpf.org

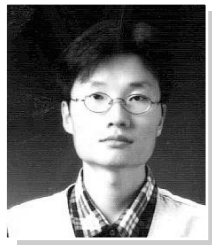
[6] Coral Consortium, http://www.coral-interop.org

[7] DReaM Project, http://openmediacommons.org

[8] Export/Import(EXIM)를 이용한 음악 콘텐츠의 DRM 상호연동 인터페이스, TTAS.KO-08.0013, 2006

[9] Export/Import(EXIM)를 이용한 동영상 콘텐츠의 DRM 상호연동 인터페이스, TTAS.KO-08.0014, 2006

>> 저자 소개



남 도 원 (Do-Won Nam)

· Email: dwnam@etri.re.kr

· Tel: +82-42-860-4994

· Fax: +82-42-860-6699

- 1996. 2 : 한국과학기술원 전산학과 학사
- 1998. 2 : 포항공과대학교 정보통신학과 석사
- 1998. 2 ~ 현재 : 포항공과대학교 컴퓨터공학과 박사 과정
- 2001. 2 ~ 현재 : 한국전자통신연구원 선임연구원
- 주관심분야 : 상이한 DRM 간의 상호 연동, 디지털저작권관리(DRM)

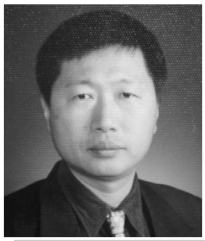
정 연 정 (Yeonjeong Jeong)

· Email: yjjeong@etri.re.kr

· Tel: +82-42-860-6303

· Fax: +42-860-6699

- 1994. 2 : 부산대학교 전자계산학과 학사
- 1996. 2 : 부산대학교 전자계산학과 석사
- 2005. 2 : 충남대학교 컴퓨터과학과 박사
- 1996. 1 ~ 현재: 한국전자통신연구원 선임연구원
- 주관심분야: 정보보안, 정보보호, 디지털저작권관리(DRM)



윤 기 송 (Kisong Yoon)
· Email: ksyoon@etri.re.kr
· Tel: +82-42-860-4992
· Fax: +82-42-860-6699

- 1984. 2: 부산대학교 조선공학과 학사
- 1988. 2: New York City University Computer Science 석사
- 1993. 2: New York City University Computer Science 박사
- 1993. 6 ~ 현재: 한국전자통신연구원 책임연구원
- 주관심분야: 정보보안, 정보보호, 디지털저작권관리(DRM), 디지털콘텐츠 유통