유무선 콘텐츠 유통 시스템 설계 및 개발

한국전자통신연구원

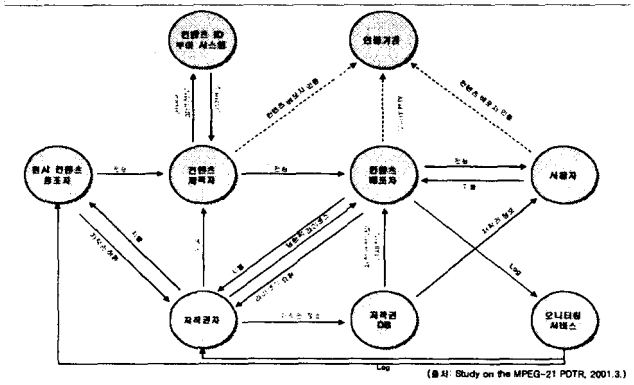
내용

- 개요
- Download방식 콘텐츠 유통
- VoD 스트리밍 방식 콘텐츠 유통

디지털 콘텐츠 유통 시스템

인터넷 환경에서, 컨텐츠의 창조자, 저작권자, 제작자, 배포자, 사용자 등 유통 주체의 권리를 보호하고, 안전하고 투명한 컨텐츠 유통을 지원하는 시스템

유통 모델 (예)



MPEG-21 멀티미디어 컨텐츠 유통 모델

컨텐츠 유통 기술개발의 기본 방향

▣ 현재 유통 시스템의 기능향상

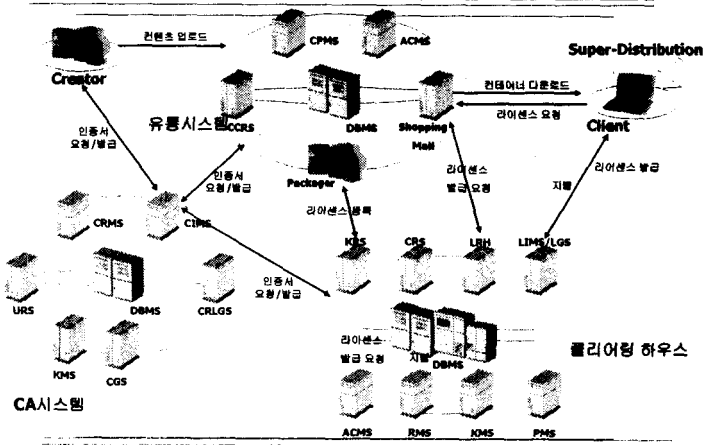
- ◆ 각 유통주체가 독립적으로 운영될 수 있는 형태
- ◆ 유통 주체가 필요에 따라 결합 또는 분리될 수 있는 형태
- ◆ 각 유통 주체간 신뢰성 보장
- ◆ 라이센스 서버로 부터 컨텐츠 보호
- ◆ 컨텐츠 종류, 메타데이터 및 시스템 확장 가능한 형태

▣ MPEG 21등 국제 표준안을 고려한 개발

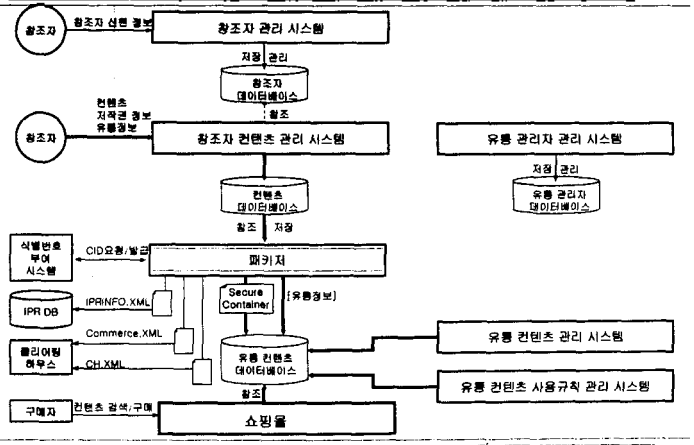
- ◆ DII (Digital Item Identification)
- ◆ DID (Digital Item Declaration)
- ◆ RDD (Rights Data Dictionary)
- ◆ REL (Rights Expression Language)
- ◆ IPMP (Intellectual Property Management and Protection)
- ◆ DIA (Digital Item Adaptation), PA (Persistent Association), ER (Event Reporting), System, , , .

Download 방식 컨텐츠 유통

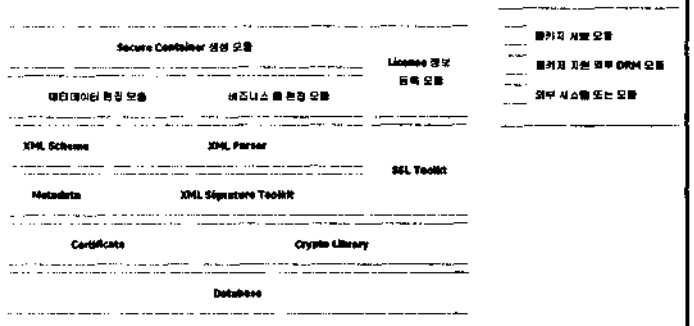
라이센스 기반 유통 솔루션



유통 시스템 구성도



패키저 시스템 구성도



클리어링 하우스 시스템

▣ 개요

◆ 클리어링 하우스는 구매자의 구매 요청에 따라 결제를 수행하고 구매자에게 라이센스를 발급하며, 유통 참여자에게 정산 정보를 리포팅하는 역할 수행

▣ 구성

◆ 사용자 관리 서브시스템

◆ 과금 관리 서브시스템

◆ 라이센스 서버 서브시스템

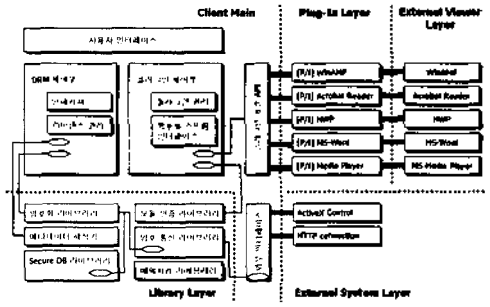
- 컨텐츠 키정보 등록관리 시스템
- 키관리 시스템
- 라이센스 생성 시스템
- 라이센스 발급 관리 시스템

◆ 리포팅 관리 서브시스템

DRM Client

▣ Microsoft Windows 환경에서 동작

▣ Microsoft Visual C++ 를 이용하여 개발



CA 시스템

▣ 개요

◆ CA는 컨텐츠 유통에 참여하는 유통업자와 클리어링 센터에 공개키에 대한 인증서를 발급함으로써 사용자 인증, 메시지 인증, 전자 서명 기능 제공

▣ 구성

◆ 인증 서버 시스템

- 사용자 등록 관리 서브시스템
- 인증서 발급 관리 서브시스템
- 인증서 처리 서브시스템
- 키관리 서브시스템

◆ 인증 클라이언트 시스템

VoD 스트리밍 방식 콘텐츠 유통

개요

▣ 기술 개요

- ◆ 컨텐츠 패키징 기술을 통해 컨텐츠를 암호화하고 독자적인 라이센스 메카니즘을 통해 스트리밍되는 컨텐츠의 저작권을 보호
- ◆ 스트리밍 서버의 수정 없이 기존 스트리밍 서비스 시스템을 지원
- ◆ 유통되는 컨텐츠를 자유롭게 배포할 수 있게 함으로써 컨텐츠 유통을 활성화

▣ 응용 분야

- ◆ 스트리밍 컨텐츠 서비스 분야
  - ▪ 인터넷 방송, 인터넷 영화관, 사이버 교육
- ◆ 컨텐츠 보호 솔루션 개발업체
- ◆ 보안 분야 업체

특징

▣ 스트리밍 서버에 대한 수정 없이 기존의 스트리밍 시스템 지원

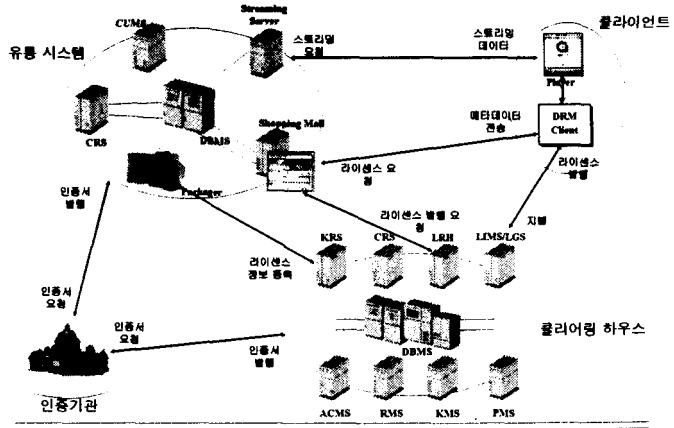
파일 타입	스트리밍 프로토콜	서버
MP4	RTSP	QuickTime Streaming Server Darwin Streaming Server
ASF	MMS/HTTP	Microsoft Media Server

▣ DRM 시스템 적용으로 인한 스트리밍 서비스의 QoS 영향 최소화

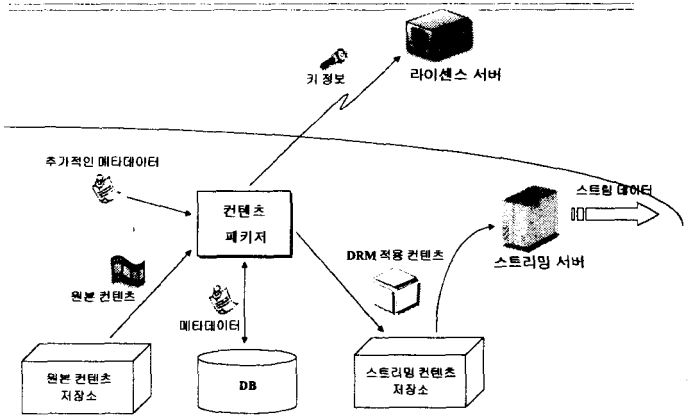
- ◆ 서버: 서버의 성능에 영향을 미치지 않음
- ◆ 클라이언트: 복호화로 인한 지연 최소화

▣ 다운로드형 컨텐츠를 위한 DRM 시스템을 기반으로 함

시스템 구조



패키징



미디어 데이터 암호화

▣ 암호화 알고리즘
- ◆ DES-CBC 알고리즘 사용
- ◆ 암호화된 미디어 데이터의 크기가 변하지 않음

▣ 비디오 데이터
- ◆ 암호화 옵션
  - ▪ 키 프레임 암호화 / 모든 프레임 암호화
  - ▪ 한 프레임에서 일부 영역만 암호화 / 전체 영역 암호화
  - ▪ 암호화될 구간(시간) 지정

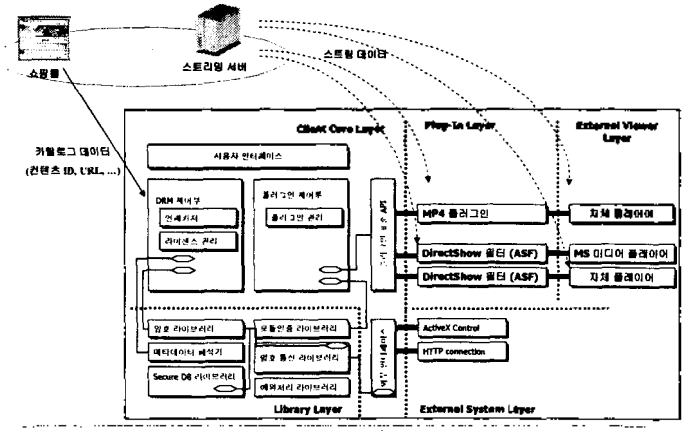
▣ 오디오 데이터
- ◆ 암호화 옵션
  - ▪ 전체 오디오 데이터 암호화
  - ▪ 암호화될 구간(시간) 지정

DRM 클라이언트 시스템

▣ 사용자 시스템에서 DRM-enabled 컨텐츠와 이에 대한 라이센스의 처리 및 관리

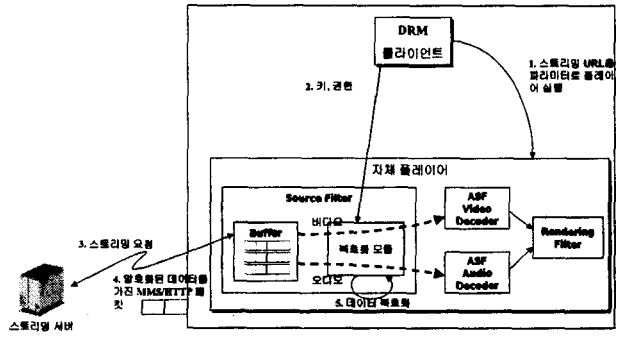
구성요소	설명
DRM 클라이언트	• DRM 정책을 결정하고 전체 프로그램의 동작을 결정 • DRM 제어부와 플러그인 제어부로 구성
플러그인 레이어	• DRM 정책이 외부 뷰어 프로그램에서 제대로 지켜지도록 제어 • 외부 플레이어의 동작을 제어 및 모니터링
외부 뷰어 레이어	• 컨텐츠를 재생하기 위한 응용 프로그램 • DRM 클라이언트와는 독립적이지만 라이센스와 사용규칙에 따라 컨텐츠가 사용될 수 있도록 DRM 클라이언트의 제어를 받음
외부 시스템 레이어	쇼핑몰, 지불중개기관, 라이센스서버 등 DRM 기반 유통시스템과의 통신을 담당

DRM 클라이언트 시스템 구조



DirectShow 필터를 이용한 방법 - ASF

▣ MMS와 HTTP 프로토콜 모두 지원



PDA 폰에서 무선 DRM 솔루션

2003. 6. 18.

컨텐츠유통기술연구팀

유선과 무선 DRM에 차이점 및 특성

▣ 차이점
- ◆ 표준화
  - ■ 유선 : MPEG-21 주도
  - ■ 무선 : OMA (Open Mobile Alliance)주도
- ◆ 무선 단말기에서 제공할 수 있는 컨텐츠 타입의 제약 존재
  - ■ 컨텐츠 Viewer 제약 및 보안의 문제점
- ◆ 유통 시스템, 플리어링 하우스와 단말기 사이의 통신 프로토콜
  - ■ 무선에서는 WAP과 Push Proxy 서버를 이용

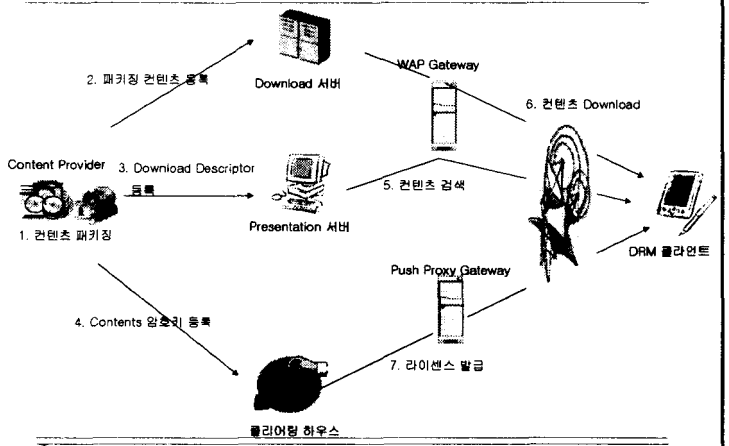
▣ 특성
- ◆ 단말기의 제약으로 Light하게 프로그램 작성
  - ■ 암호화 프로그램, 메타데이타 정보등
- ◆ 단말기 환경에 대한 보안의 중요성이 낮음
  - ■ 핸드폰인 경우 단말기에서 컨텐츠 유출 가능성이 낮음
- ◆ 요금 정책

개요

▣ 기술 개요
- ◆ OMA 표준을 준한 무선 DRM 시스템
  - ■ 3GPP (3rd Generation Partnership Project)
    - ETSI(유럽), ARIB/TTC(일본), TI(북미), TTA(한국)이 결성한 단체
    - 2003년 3월 DRM 오픈 및 요구사항에 관한 명세서 발표 수 OMA에서 진행하는 것으로 결론
- ◆ 폰 PDA 지원
- ◆ Download 방식의 지원
- ◆ Superdistribution 지원

▣ 응용 분야
- ◆ 무선 컨텐츠 서비스 분야
- ◆ 컨텐츠 보호 솔루션 개발업체
- ◆ 보안 분야 업체

시스템 구조



시스템 중요 기능

▣ 컨텐츠 유통 시스템
- ◆ 패키징 기능
  - DRM Content Format (DCF) 표준 준수
- ◆ OMA 표준에 준하는 Download Descriptor 생성 기능

▣ 클리어링 하우스
- ◆ OMA에 명시한 Right Expression Language (REL) 지원 라이센스 생성

▣ DRM 클라언트
- ◆ PDA의 고유 정보와 공개키/비밀키를 이용한 컨텐츠 보호