

디지털 방송 콘텐츠 보호 기술

2001. 06. 01.



방송기술연구소
방송미디어연구부

홍진우 (jwhong@etri.re.kr)

목 차

1. 필요성
2. 요소기술
 - 2.1 접속 제어(Access Control)
 - 2.2 사용 제어(Usage Control)
 - 2.3 내용 제어(Content Control)
3. 관련 기술 동향 분석
4. 결론

디지털 콘텐츠 보호의 필요성

ETRI

■ 서비스 환경의 변화(예 : 디지털 방송 환경)

- ◆ 미디어의 유연성, 양방향성 증대
 - ◆ 방송과 인터넷의 결합, 전자상거래 연동
 - ◆ 통신과 방송의 융합
 - 다양한 뉴미디어의 등장으로 방송 사업의 경쟁
 - ◆ 방송의 소비 형태 변화
 - 고품질 정보의 무한 반복 재현, 가공재생, 저장에 의한 시공간 초월
 - 정보 창조자로서의 역할
- 단순 시청형 → 정보 선택형 → 정보 요구형 → 정보 창조형

⇒ 이러한 변화는 결국 디지털 정보(콘텐츠)의 다양화, 차별화, 고품질화, 접근 용이성 등으로 귀착 → 디지털 콘텐츠의 중요성 대두

디지털 콘텐츠 보호의 필요성

ETRI

↓ 디지털 정보의 특성

- 디지털화된 정보에 접근이 용이함.
- 복제가 쉬울 뿐 아니라 이에 따른 비용 역시 비싸지 않음.
- 복제된 디지털 정보는 정보의 손실 없이 원본과 동일함.
- 복제된 디지털 정보의 재사용 및 조작이 쉬움.
- 복제된 디지털 정보의 배포(네트워크나 하드디스크와 같은 저장 장치를 통해)가 쉽고 빠름
- 방송과 통신(인터넷)의 융합으로 하나의 콘텐츠가 다매체에 다수 사용

⇒ 이러한 특성은 디지털 콘텐츠의 보호를 어렵게 하는 요인.

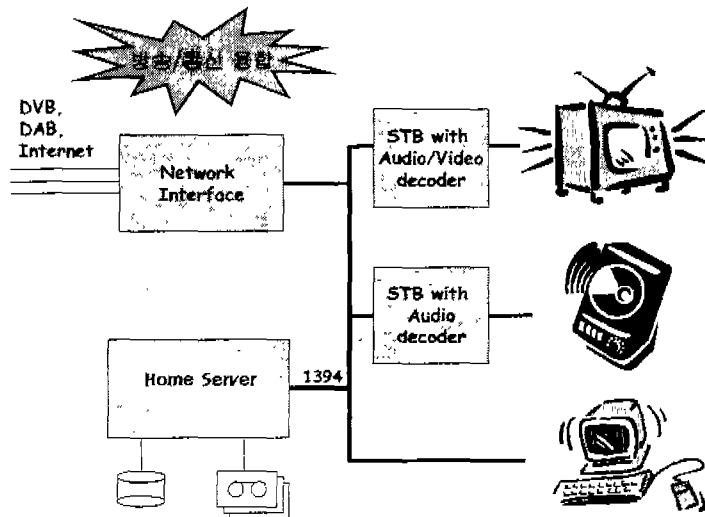
디지털 콘텐츠 보호의 필요성

↓ 예상되는 문제점

▶ 디지털 콘텐츠의 불법 복제 및 배포

- : 디지털 방송이 시작되면 대용량의 Set-top Box가 설치되고 이를 통해 저장된 대용량의 디지털 데이터의 불법복사 및 배포가 가능.
- : 인터넷 방송의 경우에는 주로 개인용 PC를 이용하게 되므로 더욱 더 손쉽게 불법복사가 가능하고, 네트워크를 통해 이를 배포할 수 있게 됨.
- : 현재 Set-top Box나 개인용 PC 등의 입출력 단자의 간단한 조작을 통해 손쉽게 디지털 데이터의 획득이 가능한 실정임.
- : 방송은 24시간 계속해서 양적으로나 질적으로 가장 많은 콘텐츠를 생산하고 있음. 향후 디지털 방송이 시작되어 고품질의 멀티미디어 콘텐츠를 방송을 통해 획득하고, 이를 불법으로 유통시킬 경우 멀티미디어 산업 전반에 엄청난 영향을 미치게 될 것임.

Example of Home Network in Broadcasting



디지털 콘텐츠 보호의 필요성

ETRI

예상되는 문제점

불법 복제된 디지털 콘텐츠의 재가공 및 배포

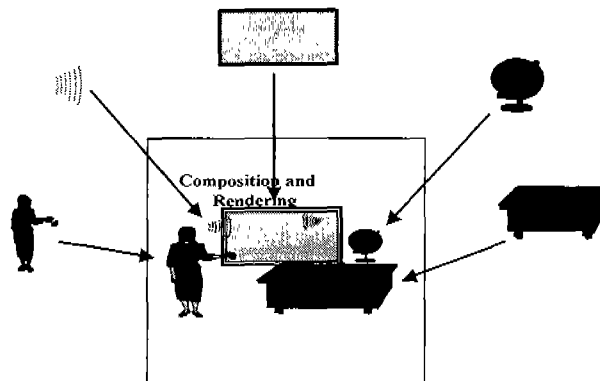
: 불법 복제된 디지털 데이터는 디지털 데이터의 속성 상 손쉽게 재가공될 수 있음. 특히, 향후 디지털 데이터는 MPEG-2, 4, 7 기반의 멀티미디어 데이터가 될 것이고, 이들은 멀티미디어 편집 소프트웨어나 간단한 신호처리적인 조작을 통해 재가공되어 불법적으로 유통될 수 있음.

: 이와 같은 재가공된 디지털 콘텐츠는 소유권이 누구에게 있는지 불분명하게 되므로 새로운 저작권 시비를 불러일으킬 수 있게 됨.

디지털 콘텐츠 보호의 필요성

ETRI

예상되는 문제점(재가공의 예)



< AV Objects로부터 재가공된 디지털 데이터 >

Preliminary for digital broadcast

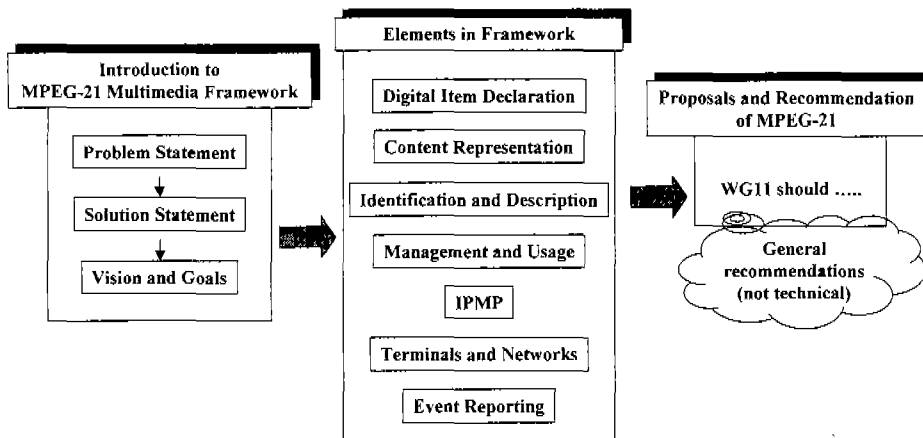
ETRI

↓ 디지털 콘텐츠 보호 및 관리를 위한 프로젝트 및 표준화 동향

- 콘텐츠 식별 기술(ISBN, URI, URN, DOI...)
 - ▶ 콘텐츠에 유일한 식별자를 부여(similar to barcode)
- 메타데이터 기술(INDECS, XrML, ODRL...)
 - ▶ 콘텐츠 타입 정보, 저작권 정보, 및 사용 권리에 대한 명세 체계
- IPMP 관련 기술(CAS, TALISMAN, OKAPI, OPIMA, cIdf, TV-Anytime, MPEG 4/7/21...)
 - ▶ 식별 기술과 메타데이터 기술 등을 기반으로 저작권 보호 및 관리를 할 수 있는 시스템

MPEG-21 멀티미디어 프레임워크

ETRI



디지털 콘텐츠 보호를 위한 요소 기술

ETRI

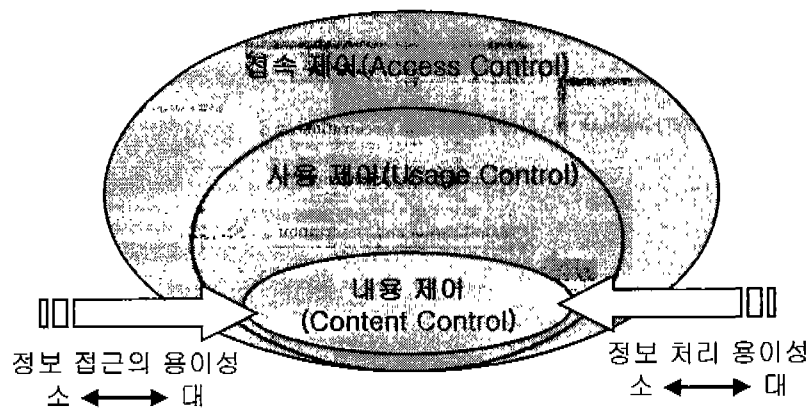
- 접속 제어(Access Control)
 - Protection by Authentication

- 사용 제어(Usage Control)
 - Protection by Scrambling/Encryption

- 내용 제어(Content Control)
 - Protection by Watermarking

디지털 콘텐츠 보호를 위한 요소 기술

ETRI



* 내용 제어(Content Control, ex. watermark)는 “last line of defense”.

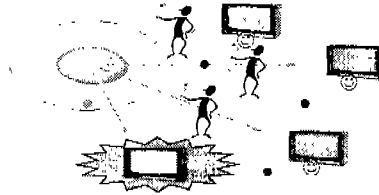
디지털 콘텐츠 보호를 위한 요소 기술

ETRI

↓ 접속 제어(Access Control)

- 소유권을 가지지 않은 사용자의 콘텐츠에 대한 접근을 막는 방법

- : 주로 인증 기술을 이용하여 접근 방어 → 저작권 보호는 불가
- : 일단 인증키가 풀린 디지털 콘텐츠의 경우에는 제어할 방법이 없음
- : 권한이 있는 사용자가 이를 불법으로 배포하고자 할 경우에도 이를 제어하기가 불가능함.



< Access Control : 콘텐츠에 접속할 수 있는 권한(Key)이 있어야만 함 >

ETRI Proprietary

우선방송기술연구소 방송미디어연구부 음향기술연구팀

13

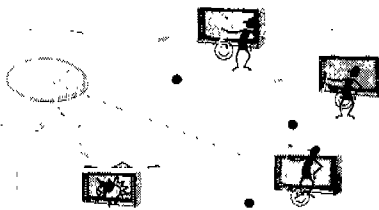
디지털 콘텐츠 보호를 위한 요소 기술

ETRI

↓ 사용 제어(Usage Control)

- 정당하지 않은 사용자의 콘텐츠에 대한 사용을 막는 방법

- : 주로 인터넷에서 많이 이용되는 방법으로 암호화 키(Key)나 디지털 서명 등을 이용하여 콘텐츠의 사용 행위(Play, 복사 등)의 조절
- : 현실적으로 복사, 배포 등의 콘텐츠의 사용과 관련된 모든 행위를 제어하기가 어려움.
- : 실제 구현에 있어서의 문제점 : Bad acceptability, no standard agreement, etc.



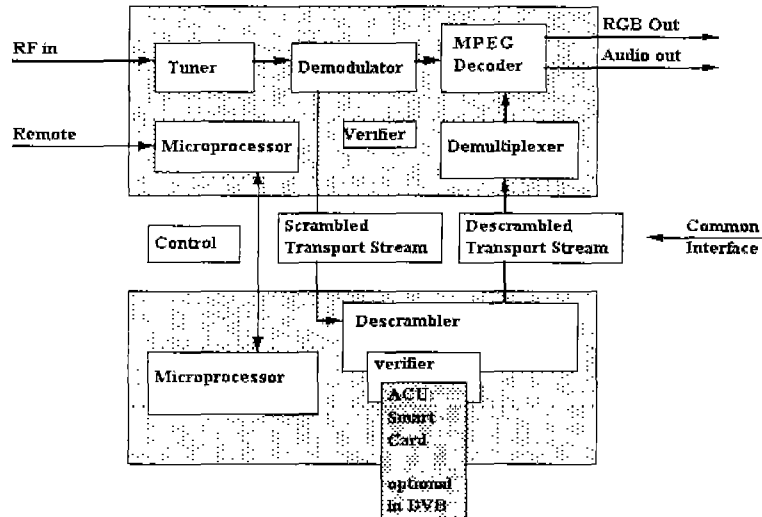
ETRI Proprietary

우선방송기술연구소 방송미디어연구부 음향기술연구팀

14

Example of Usage Control in Broadcasting

ETRI



ETRI Proprietary

무선방송기술연구소 방송미디어연구부 음향기술연구팀

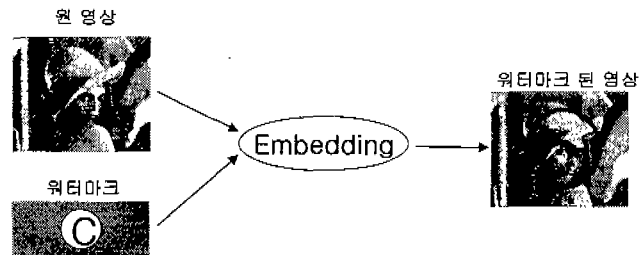
15

디지털 콘텐츠 보호를 위한 요소 기술

ETRI

□ 내용 제어(Content Control)

- ◆ 콘텐츠 내용내에 은닉된 정보로 저작권 정보 및 불법적인 복제를 막는 방법
 - : 지각적으로 감지되지 않는 저작권 정보를 콘텐츠 자체에 삽입
 - : 암호가 풀린 후에도 소유권을 주장할 수 있음.
 - : 의도적인 공격에 살아 남기가 대단히 어려움.



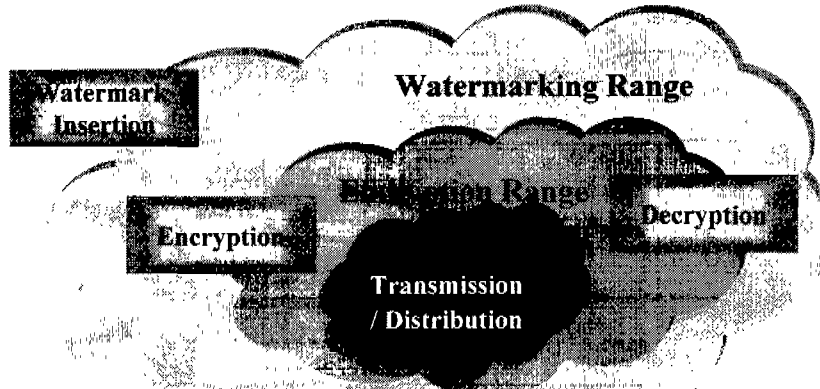
ETRI Proprietary

무선방송기술연구소 방송미디어연구부 음향기술연구팀

16

Encryption vs. Watermarking

ETRI



ETRI Proprietary

무선방송기술연구소 방송미디어연구부 음향기술연구팀

17

디지털 콘텐츠 보호를 위한 요소 기술

ETRI

향후 발전방향

: 강인한 내용 제어(워터마크) 기술 개발

: 각각의 요소 기술들의 결합을 통한 방법으로 발전
⇒ 내용제어, 접속제어 및 사용 제어의 결합

: 복제조절정보(CCI : Copy Control Information)를 워터마크로 삽입하여
워터마크 검출 시 한번 이상 복사되었으며 자동으로 Play가 멈추게 하
거나 접속 권한이 없을 경우 자동으로 Scrambling 기능이 작동되게 함
⇒ Never copy, one copy → no more copy, copy free

: Play 되는 시간정보를 워터마크로 삽입하게 하여 자동으로 과금이 Check
되게 함

: 깨지기 쉬운(Fragile) 워터마크를 이용한 디지털 콘텐츠에 대한 불법적
인 변형 여부의 판별

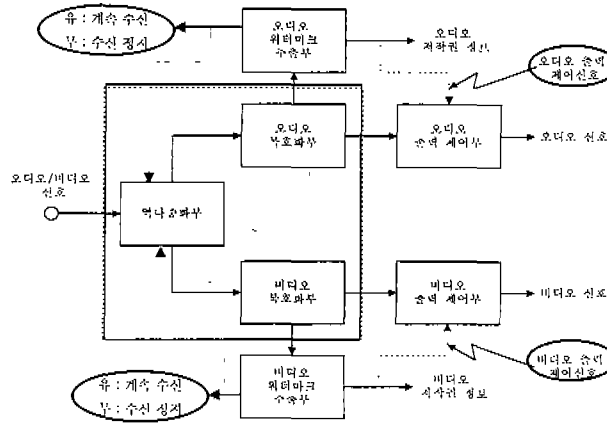
ETRI Proprietary

무선방송기술연구소 방송미디어연구부 음향기술연구팀

18

디지털 콘텐츠 보호를 위한 요소 기술

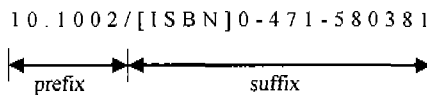
향후 발전방향



< 워터마킹과 접속 제어, 사용 제어의 결합 >

Overview Technology(DOI)

- ↓ 디지털 환경에서 지적 재산을 확인하고, 교환하기 위한 디지털 콘텐츠에 대한 영구 식별자
- ↓ International DOI Forum(IDF)이 주관
- ↓ 식별자에 대한 메타데이터는 별도 요구
- ↓ DOI 구성
 - Prefix : [등록기관번호]. [DOI 등록자 번호]
 - Suffix : 정해진 규칙이 없음, 해당 등록기관의 자율(기존 식별시스템 적용 가능)

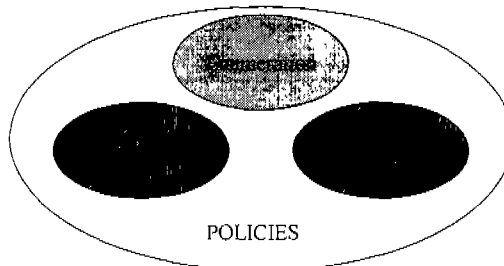


Overview Technology(DOI)

ETRI

✦ DOI 구조

- Enumeration
 - ▶ 식별번호
- Description
 - ▶ DOI는 메타데이터 description으로 <INDECS> 프레임워크를 선택한다.
- Resolution
 - ▶ Handle system으로 DOI를 변환하여 실제적인 data가 있는 곳을 알려줌



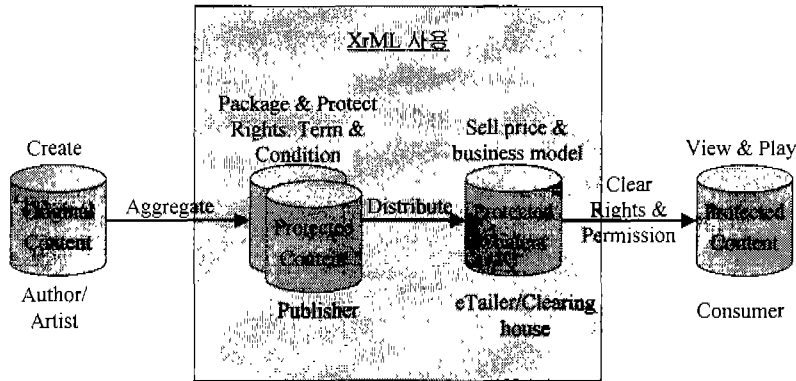
Overview Technology(XrML)

ETRI

- ✦ XrML은 디지털 콘텐츠에 대하여 접근과 사용, 출판과 판매 조건 등을 명세 하기 위한 언어
- ✦ Xerox Palo Alto Research Center(PARC)에 의하여 제안되고 개발됨
- ✦ XML 기반으로 명세에 필요한 element와 attribute를 top down 방식으로 정의
- ✦ 디지털 저작권 명세 사항에 대한 인터페이스 제공
- ✦ 사용권한, 요금과 같은 과금정책 작성을 도와주는 인터페이스 제공
- ✦ 여러 다른 기기와 장비들 간에 균일한 인터페이스 제공

Overview Technology(XrML)

↓ XrML 적용 부분



Overview Technology(CAS)

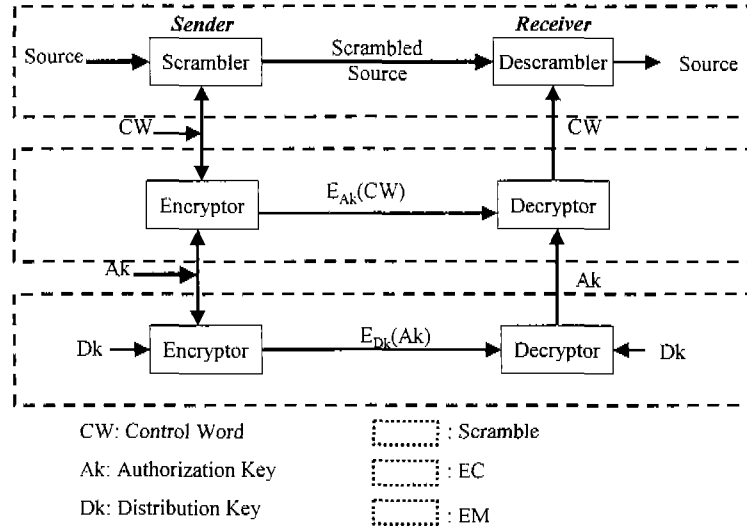
↓ 접속 제어를 위한 시스템

- ▶ 정당한 권리를 갖는 사용자만이 서비스에 접속 할 수 있도록 함

↓ 주로 3부분으로 이루어짐

- ▶ 스크램블링 모듈
 - ▶ 방송 신호를 descrambling 모듈과 키(CW) 없이는 볼 수 없도록 변형시킴
- ▶ Entitlement control
 - ▶ 주기적으로 변하는 CW를 전송하기 위하여 암호화하여 ECM으로 전송
- ▶ Entitlement management
 - ▶ 수신자의 권한 및 인증을 확인하는 부분으로 authorization 키를 분배키로 암호화하여 EMM으로 전송
 - ▶ 분배키는 스마트 카드 또는 안전한 전송 채널을 통하여 수신자에게 전달

Overview Technology(CAS)



Overview Technology(TALISMAN)



- ✦ 'Tracing Authors' rights by Labeling Image Services and Monitoring Access Networks'
- ✦ ACTS programme에 의하여 1995년 9월에 시작하여 3년간 개발됨
- ✦ 유럽 연합 디지털 방송 서비스업자들에게 저작권 보호를 위한 메커니즘을 제공하기 위함
- ✦ 디지털 영상 콘텐츠에 대한 대규모적인 상업적 해적행위와 불법 복제를 막기 위함
- ✦ Common Functional Model
 - MM 유통에 관련된 행위자(actor) 및 행위자들의 기능을 모델링
- ✦ 3가지 보호 메커니즘이 디자인됨

Overview Technology(TALISMAN)

ETRI

↓ Labelling

- *integrity*: 디지털 콘텐츠에 불법적인 편집이 일어났는지를 탐지함 (hash or feature extraction)
- *rights clearance*: 라벨 안에 삽입된 ID number로 저작권 침해를 탐지

↓ Watermarking

- 저작권 정보에 대한 증거를 남김
- 64bits의 정보를 삽입

↓ Monitoring

- 라벨과 워터마크를 사용하여 이용되고 있는 콘텐츠를 자동적으로 분석

Overview Technology(OKAPI)

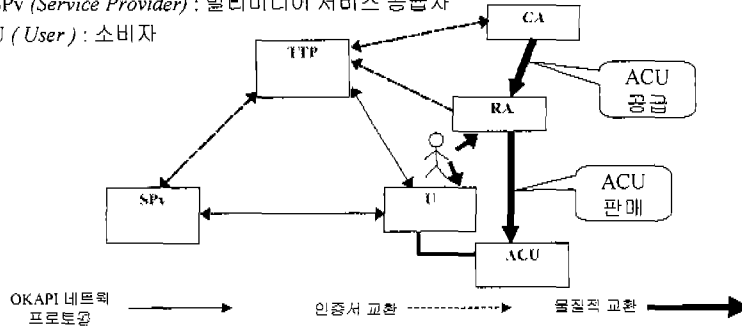
ETRI

- ↓ OKAPI (Open Kernel for Access to Protected Interoperable services)
- ↓ 방송 및 인터넷 환경에서 제한수신(conditional access)을 위한 일관성 있는 통합적인 프로토콜 개발
- ↓ 콘텐츠를 암호화 하는 session key를 공유하기 위한 안전한 프로토콜의 필요로 시작됨
- ↓ Trusted Third Parties(TTPs), 스마트 카드, public-key 암호화 개념에 기반
- ↓ 객체들 사이 인증 시스템으로 SPKI(Simple Public Key Infrastructure)를 사용

Overview Technology(OKAPI)

OKAPI 시나리오

- RA (Registration Authority) : ACU를 U(ser)에게 공급
- ACU (Access Control Unit, or Smart Card) : 멀티미디어 저장, 재생 장치
- CA (Certification Authority) : ACU 제작, 설치, 분배
- TTP (Trusted Third Party) : SPv, CA, User사이의 관계 인증
- SPv (Service Provider) : 멀티미디어 서비스 공급자
- U (User) : 소비자



Overview Technology(OPIMA)

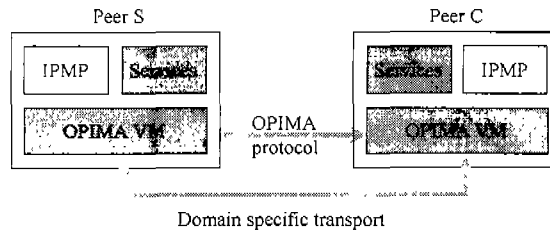
- ✦ 'Open Platform Initiative for Multimedia Access'
- ✦ IEC 산하 ITA program 에서 개발
- ✦ 다중 콘텐츠 보호 장치 하에서 다양한 형태의 콘텐츠나 서비스에 접근을 가능하게 하기 위함
 - 서로 다른 응용, 장비 및 IPMP 시스템간의 일반적인 상호 작용을 가능하게 함
 - Peer-to-peer 구조로 각 peer는 OPIMA Virtual Machine(OVM) 위에서 작동
- ✦ OPIMA 신용장(Credentials)를 사용하여 보호된 콘텐츠가 compartment 간에 안전하게 교환될 수 있도록 함
- ✦ OPIMA 프로토콜 사용
 - SAC(Secure Authenticated Channel)을 설정하고, IPMP 시스템을 OVM으로 다운로드 하도록 하는 프로토콜

Overview Technology(OPIMA)

ETRI

OPIMA 프로토콜

1. Application이 OVM에게 보호된 콘텐츠에 접속하도록 요청
2. OVM이 OS에게 초기 망 접속을 설정하도록 요청
3. 이 접속 상부에 OPIMA SAC가 설정됨
4. 필요한 IPMP 시스템이 OVM에 의해 요청되고 다운로드 된다.



ETRI Proprietary

무선방송기술연구소 방송미디어연구부 융합기술연구팀

31

Overview Technology(cIDf)

ETRI

- ✦ 1999년 Content ID Forum에 의하여 시작
- ✦ 워터마킹 기술을 이용하여 “콘텐츠 ID”를 각 디지털 콘텐츠 안에 삽입.
 - 디지털 콘텐츠의 저작권을 손쉽게 명시
 - 콘텐츠 매매, 재사용 시 저작권 소유자에 적절한 보상
 - 콘텐츠 시장에서 디지털 콘텐츠에 바코드를 부여하므로 콘텐츠에 대한 기록을 남길 수 있는 메커니즘을 제공
 - 불법 복제를 쉽게 검출
- ✦ 계층적 저작권 관리
- ✦ 워터마킹 기술의 체계화 및 표준화 방법 모색
 - 메타-워터마킹 기술

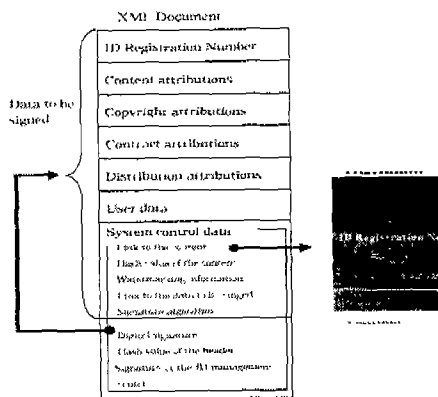
ETRI Proprietary

무선방송기술연구소 방송미디어연구부 융합기술연구팀

32

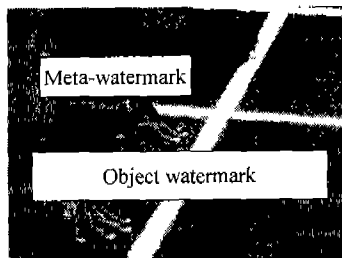
Overview Technology(cIDf)

- ↓ DCD 및 IDCMN을 사용하여 콘텐츠를 Package화 한다.
 - IDCMN(ID Center Management number)
 - ▶ Center No. + work ID + issuing ID + version info
 - DCD(Distribution Content Identifier)



Overview Technology(cIDf)

- ↓ 메타-워터마킹 기술
 - Object-워터마크 와 메타-워터마크를 사용
 - Object 워터마크는 IDCMN(ID Center Management Number)을 삽입하는데 쓰이고 이 방법은 제한이 없음
 - 메타-워터마크는 object 워터마크 방식에 대한 정보를 삽입하는데 쓰이며 이 방식은 표준화됨



결언

ETRI

- ↓ 디지털 방송의 상용화에 따른 양질의 디지털 방송 콘텐츠의 보호 필요성 강조
 - 다양한 양질의 방송 콘텐츠 생산 및 제공
 - 디지털 방송 및 관련 콘텐츠 산업의 활성화

- ↓ 콘텐츠 보호와 개인 프라이버시 보호 사이의 절충 고려
- ↓ 방송망과 인터넷 상에서 모두 적용 가능한 IPMP 시스템 개발 필요
- ↓ 요소 기술들에 대한 지속적인 연구가 필요
- ↓ 기존 IPMP 시스템과의 호환성 문제
- ↓ 불법 복제 및 사용에 대한 도덕적 의식 강조