무선 환경에서 안전한 디지털 컨텐츠 유통을 제공하는 시스템 설계 및 구현

이 권 일[†] · 김 봉 선[††] · 신 영 찬[†††] · 류 재 철[††††] · 이 준 석[†††††]

요 약

DRM 기술은 사용 권한이 없는 사용자가 사용자 기기를 이용해 불법으로 디지털 컨텐츠를 사용하는 것을 방지하는 것을 목적으로 한다. 따라서 DRM 시스템을 구성하기 위해서는 기본적인 정보보호 기술들이 이용된다. 이는 무선 DRM의 경우에 있어서도 마찬가지다. 특히 디지털 컨텐츠를 암호화 기술을 이용하여 패키징하고 패키징된 디지털 컨텐츠를 사용하기 위해 필요한 패키징에 사용된 암호화 키를 PDA나 휴대전화기 같은 합법적인 무선 사용자 기기에 안전한 방법으로 배분하는 것이 중요하다. 본 논문은 무선 DRM 표준안인 OMA의 규격을 준수한 무선 디지털 컨텐츠 배분에 사용될 무선 DRM 시스템의 구조를 제안하고 공개키 기법을 사용하여 디지털 컨텐츠 사용권을 배분하는 방식으로 무선 DRM 시스템 각 구성 요소들 사이의 프로토콜을 제안하고 설계 구현하였다.

A Design and Implementation of System to Provide Secure Digital Contents Distribution on Mobile Environment

Kwon Il Lee[†] · Bong Seon Kim[††] · Young Chan Shin[†††]
Jae Cheol Ryou[††††] · Jun Seok Lee[†††††]

ABSTRACT

There is a need for content providers and operators to control the usage of downloaded digital contents. Digital Rights Management(DRM) is the means to control the usage of the digital contents once it has been downloaded. Therefore, appropriate security mechanism is required. The mobile DRM system is same as the general DRM system. We use encryption technology to package digital contents. In case of Mobile DRM system, secure distribution and secure keeping of packaging encryption key is important. In this paper, we design and implement DRM system on the Mobile Environments following on OMA(Open Mobile Alliance) DRM Model. We considered being a secure DRM system to contain appropriate security solution.

키워드 : 무선인터넷(Mobile Internet), DRM, 사용권(Right), 디지털 컨텐츠(Contents)

1. 서 론

정보통신 기술의 발달로 인해 PDA 및 휴대 전화 등을 이용한 무선 인터넷의 사용이 급속도로 확산되고 있다. 인터넷 사용자들이 빠른 속도로 장소에 제약을 받지 않는 무선 인터넷 서비스로 옮겨가기 시작했다. 최근 무선 인터넷 사업자들은 무선 인터넷을 통한 동영상 서비스 등 다양한 컨텐츠를 제공하고 있으며 무선 인터넷용 영화가 별도로 제작되고 있는 것이 현실이다. 무선 환경에서 디지털 컨텐츠의 사용 요구가 증가함에 따라 무선 컨텐츠 제공자들은 이미 무선 환경에 맞는 DRM(Digital Rights Management) 시스템을 제공하고 있으며, 보다 안전하고 효율적인 DRM 서비스 제공을 위한 솔루션을 연구, 개발 중에 있다.

대부분의 DRM 시스템들이 유선 인터넷 환경에서의 디지털 컨텐츠 보호에 초점을 맞추고 있다[1-9]. 무선 인터넷 환경에서 유통되는 디지털 컨텐츠를 보호하기 위해서는 유선 DRM 시스템의 기본 개념을 도입하더라도 무선 환경에 적합한 디지털 컨텐츠 보호 기술을 개발 사용하여야 한다. 무선 환경은 유선 환경에 비해 데이터 전송 속도, 컨텐츠가 실행되는 단말의 자원 등에서 많은 제약사항이 존재한다. 또한 다른 무선 DRM 시스템 들과의 호환성 및 상호 운영성 등을 고려하여 설계 개발되어야 한다.

현재 무선 DRM의 표준을 제정하고 있는 단체로는 3GPP (3rd Generation Partnership Project)[10]와 OMA(Open

† 정 회 원 : 대덕대학 컴퓨터인터넷정보계열 교수
†† 정 회 원 : 삼성전자
††† 준 회 원 : 충남대학교 대학원 컴퓨터과학과
†††† 종신회원 : 충남대학교 컴퓨터과학과 교수
††††† 정 회 원 : 한국전자통신연구원 책임연구원
논문접수 : 2003년 12월 8일, 심사완료 : 2004년 3월 5일

Mobile Alliance)[11-15]가 있다. 이들은 각각 몇 가지의 DRM 방식을 표준으로 제시하고 있다. 3GPP의 경우 별도의 무선 DRM 표준 제정을 중단하고 OMA의 표준안을 따르기로 결정하였다.

DRM 기술은 사용권한이 없는 사용자가 사용자 단말을 이용해 불법으로 디지털 컨텐츠를 사용하는 것을 방지하는 것을 목적으로 한다. 따라서 DRM 시스템을 구성하기 위해서는 기본적으로 정보 보호 기술들이 이용된다. 특히 암호화 기술을 이용하여 디지털 컨텐츠를 패키징하는 기술, 패키징된 디지털 컨텐츠와 컨텐츠 사용권을 합법적인 사용자 단말로 안전하게 배포하는 기술 등이 요구된다.

본 논문은 무선 DRM 표준안인 OMA의 규격에 따르는 무선 DRM 시스템 구조를 제안하고 이를 설계 구현하였다.

본 논문은 구성은 다음과 같다. 2장에서 무선 DRM 시스템 관련 표준화 동향을 살펴보고 3장에서 본 논문에서 제안한 시스템 구성에 대해 설명하였다. 그리고 4장에서 본 논문에서 제안한 무선 DRM 시스템의 설계 및 구현 내용에 대해 설명하고, 5장에서 구현 및 시험 결과를 기술하였다. 마지막으로 6장에서 결론을 기술하였다.

2. 관련 연구

본 장에서는 무선 DRM의 실질적인 표준안인 OMA DRM에 대해 기술한다.

2.1 OMA(Open Mobile Alliance) DRM

OMA에서는 무선 DRM에 관련된 구체적인 규격을 제시하고 있다. OMA는 WAP[16, 17] 기반에서 작동하는 무선 통신에 적용하는 응용으로서 무선 DRM을 규정한다. 그리고 DRM 컨텐츠 형식인 DCF(DRM Content Format)[13], XML[20] 기반으로 한 메타데이터인 DD(Download Descriptor) 형식, ODRL(The Open Digital Rights Language) v1.1에 기반한 DRM 사용권 형식[14] 등을 제시하고 있다.

OMA DRM은 DRM 사용권과 컨텐츠를 분배하는 방식으로 다음과 같은 3가지를 정의하고 있다.

- Forward-Lock : 한 클라이언트 단말에서 실행 가능한 DRM 컨텐츠가 다른 클라이언트 단말로 전송되는 것을 방지하는 것을 말한다.
- Combined Delivery : DRM 컨텐츠와 사용권이 함께 클라이언트 단말로 전송되는 방식. 이 방식은 컨텐츠 암호화를 요구하지 않고 단지 컨텐츠 사용권에 명시된 내용에 의한 컨텐츠 사용 제어가 이루어짐.
- Separate Delivery : DRM 컨텐츠와 사용권이 분리되어 클라이언트 단말로 전송되는 방식으로 컨텐츠는 대칭키 암호 방식을 이용하여 암호화되고 DRM 컨텐츠 형식(DCF)[13]으로 변환되어 클라이언트 단말로 전송됨. 컨텐츠 사용권은 컨텐츠 사용 명세와 동시에 컨텐츠 암호화 키를 이용하여 컨텐츠 사용을 제어.
- Superdistribution : Separate Delivery의 특수한 경우로 하나의 클라이언트 단말에서 다른 클라이언트 단말로 DRM 컨텐츠 전송을 허용하고, 다른 클라이언트 단말을 통해 컨텐츠를 취득한 클라이언트 단말이 컨텐츠 사용을 위해 사용권을 취득하는 방법을 제시하는 것이다.

2.2 OMA(Open Mobile Alliance) DRM 분석

Forward-Lock, Combined Delivery 방식은 디지털 컨텐츠의 암호화를 지원하지 않고 있으므로 컨텐츠의 내용이 통신 선로 상 또는 클라이언트 단말에서 누출될 수 있다. 따라서 본 논문에서 설계, 구현한 무선 DRM 시스템에서는 디지털 컨텐츠의 누출을 방지하기 위해 "Separate Delivery"와 "Superdistribution" 만을 지원한다.

OMA DRM 모델은 무선 DRM 시스템에 관한 구조와 무선 DRM 시스템에서 필요한 기본 데이터 형식을 정의하고 있지만 아래와 같이 보안 측면에서 약점을 가지고 있다.

- OMA DRM 모델은 사용권(right)의 안전한 분배에 관한 해결책을 제시하지 않고 있다.
- OMA DRM 모델은 클라이언트 단말 인증 문제에 대해 다루지 않고 있다.
- OMA DRM 모델은 클라이언트 단말 내의 문서편집기 등과 같은 비인가된 개체들이 사용권(right), DRM 컨텐츠 등과 같은 DRM 개체들로의 접근하는 것을 차단하는 것과 같은 보안 문제에 대해서는 언급하지 않았다.

이 논문은 위와 같은 약점을 해결하는 관점에서 시스템을 설계하였다.

3. 무선 DRM 시스템 구성

3.1 컨텐츠 분배 방식에 따른 시스템 흐름

3.1.1 Separate Delivery

Separate Delivery란 암호화된 컨텐츠와 CEK를 포함한 컨텐츠 사용권을 분리하여 클라이언트 단말에 전송해주는 방식이다. CEK를 소유하지 않은 사용자는 컨텐츠를 사용할 수 없으므로 컨텐츠를 안전하게 보호할 수 있다. 또한 이 방식은 클라이언트 단말에 다운로드된 컨텐츠 사용권이 파기된 이후에도 사용자가 지속적인 서비스를 원하는 경우에는 사용권 발행자에게서 컨텐츠 사용권만을 재발급 받아

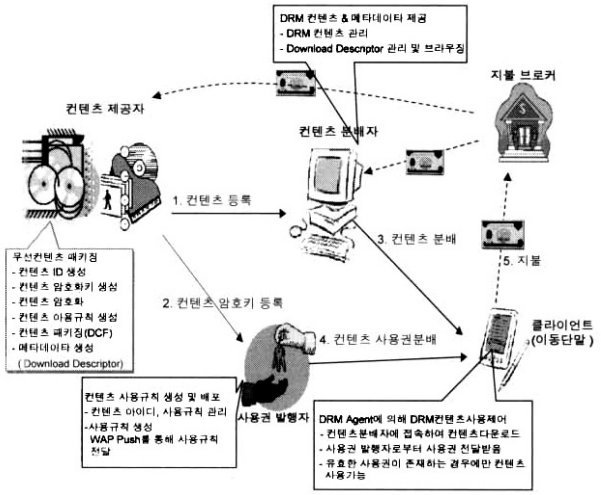
사용할 수 있다.

3.1.2 Superdistribution

Superdistribution 방식은 Separate Delivery 방식을 진보시킨 방법으로 클라이언트 단말들 사이에 DRM 컨텐츠를 전송하는 것을 허용하는 것이다. 클라이언트 단말들 사이에서는 오직 DRM 컨텐츠만 전송되고, 다른 클라이언트 단말로부터 DRM 컨텐츠를 제공받은 단말은 DRM 컨텐츠에 명시된 컨텐츠 분배자를 통해 사용권 발행자에게 사용권을 요청해야 한다.

3.2 시스템 모델

무선 DRM 시스템은 컨텐츠 분배자(Contents Distributor), 사용권 발행자(Right Issuer) 등의 서버와 PDA, 휴대폰 등과 같은 이동 단말인 클라이언트로 구성된다. 컨텐츠 분배자(Contents Distributor)는 이미 패키지된 DRM 컨텐츠를 PDA나 개인용 휴대폰 등과 같은 이동 단말기에 배분하는 포탈 서버이며 사용권 발행자는 이동 단말로 다운로드된 디지털 컨텐츠에 대한 사용권을 발행하는 서버이다. 본 논문에서 구현한 무선 DRM 시스템 모델은 (그림 1)과 같다.



(그림 1) 시스템 모델

- 컨텐츠 패키저(또는 컨텐츠 제공자) : 무선 디지털 컨텐츠 제공자로 디지털 컨텐츠를 가공하여 DRM 컨텐츠를 생성한다.
- 컨텐츠 분배자 : Presentation 서버와 Download 서버로 구성된다. Presentation 서버는 클라이언트 단말들에게 컨텐츠 정보를 알려주는 포탈 서버 역할을 수행하며, Download 서버는 컨텐츠 패키저에 의해 가공된 DRM 컨텐츠를 보관하고 있는 서버이다.
- 사용권 발행자 : 클라이언트에게 컨텐츠 사용권을 발행해 주는 서버이다. 클라이언트 단말은 컨텐츠 분배자에게서 다운로드 받아온 컨텐츠를 사용권 발행자에 의해 발행된 사용권에 의해 사용할 수 있다.
- 클라이언트 단말 : 무선 디지털 컨텐츠를 사용할 PDA, 스마트폰, 휴대폰 등과 같은 이동 단말을 의미한다.

4. 무선 DRM 시스템 설계 및 구현

본 장에서는 논문에서 제안하고 설계한 무선 DRM 시스템에 대해 기술한다. 본 논문에서 설계 구현한 시스템은 다음과 같은 개념에 기반을 두고 있다.

- 무선 클라이언트와 각 서버들 사이에서 전송되는 메시지들의 기밀성을 보장받아야 하는 경우는 WTLS[19]를 이용한 Secure Channel 상에서 통신한다.
- 클라이언트 단말 인증에 RSA를 기반으로 한 공개키 시스템을 사용한다.
- 컨텐츠 분배자와 사용권 발행자는 동일 주체에 의해 운영된다. 따라서 컨텐츠 분배자와 사용권 발행자 사이의 전송은 안전하다.
- OMA DRM의 Separate delivery와 Superdistribution[9]을 지원한다.

4.1 주요 데이터

4.1.1 CPF(Contents Package Format)

디지털 컨텐츠를 DRM 컨텐츠로 패키징하기 위해 CPF 형식을 정의하여 사용하였다. CPF 형식은 OMA DRM에서 정의한 DCF 형식에서 superdistribution을 지원하기 위해서 컨텐츠 분배자의 URI를 표시할 영역을 추가 확장하였다. CPF는 아래와 같은 영역으로 구성된다.

- 디지털 컨텐츠의 데이터 유형(예. mp3, avi)
- 디지털 컨텐츠 식별자(Contents ID : CID)
- 암호화에 대한 세부 정보(예 : 암호 알고리즘)
- DRM 컨텐츠 사용권 발급 서비스에 관한 정보
- 컨텐츠 분배자 URI(superdistribution 지원을 위해 확장된 영역)

4.1.2 Download Descriptor(DD)

DD는 DRM 컨텐츠에 관한 정보를 담고 있는 메타 데이터이다. 클라이언트 단말의 download 에이전트는 DD에 정의된 컨텐츠의 속성을 기반으로 DRM 컨텐츠를 다운로드 할 것인지를 결정한다. 이 데이터는 XML[20] 문법을 기반으로 작성되며 아래와 같은 영역으로 구성된다.

- DRM 컨텐츠의 MIME 타입
- DRM 컨텐츠 식별자(Contents ID : CID)
- DRM 컨텐츠 크기

- DRM 컨텐츠 이름

4.1.3 Usages

DRM 컨텐츠의 사용규칙 목록을 명세하기 위하여 XML [20] 문법을 기반으로 Usages 자료를 정의하여 사용하였다. Usages는 사용자가 선택할 수 있는 usage들의 목록을 가지고 있다. Usages 자료의 구성은 다음과 같다.

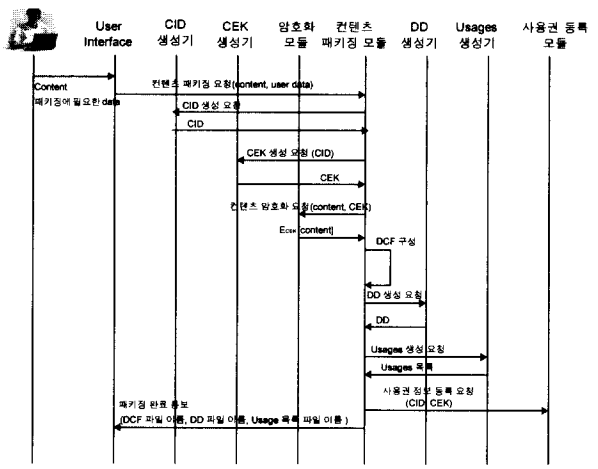
- CID
- 사용규칙 목록

4.1.4 Right

DRM 컨텐츠 사용 제어를 위한 사용규칙을 표현하기 위해 ODRL(Open Digital Rights Language)[21]의 mobile profile인 OMA REL(Rights Expression Language) [14]을 사용하여 right를 정의하였다. Right는 아래와 같은 내용을 포함하고 있다.

- CID, version 등과 같은 데이터
- 사용권
  - 사용규칙 및 제약 사항
  - CEK(Content Encryption Key)

4.2 컨텐츠 패키저(Contents Packager)



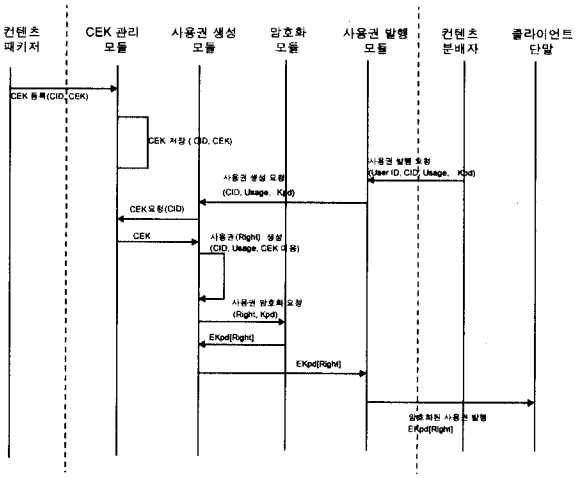
(그림 2) 컨텐츠 패키징 처리 과정

컨텐츠 패키저는 컨텐츠를 암호화하여 DRM 컨텐츠로 패키징하고 메타 데이터인 DD를 생성하는 역할을 담당한다. 사용자가 사용자 인터페이스를 통해 컨텐츠 패키저에게 컨텐츠의 패키징을 요청한다. 사용자 인터페이스는 사용자의 입력을 가지고 컨텐츠 패키징 모듈에게 컨텐츠 패키징을 요청하고, 컨텐츠 패키징 모듈은 CID 생성기에 컨텐츠 ID 생성을 요청해 CID를 생성하고 CEK 생성기를 통해 컨텐츠 암호화에 이용할 키인 CEK를 얻어온다. 그리고 사용자로부터 전달받은 컨텐츠와 컨텐츠 암호화 키인 CEK로 컨텐츠를 암호화한 후 DRM 컨텐츠로 패키징한다. 그리고 DD 생성기를 통해 DD를 생성하고, usages 생성기를 통해 usages를 만든다. DRM 컨텐츠와 DD, usages는 컨텐츠 분배자에게 제공되고, CEK는 사용권 발행자에게 등록한다. (그림 2)에 컨텐츠 패키저의 처리 과정을 도시하였다.

4.3 사용권 발행자(Right Issuer)

사용권 발행자는 클라이언트 단말에 컨텐츠 사용권을 발행하는 서버이다. 사용권 발행자는 (그림 3)과 같은 순서로 사용권 발행을 처리한다. 컨텐츠 분배자 또는 superdistribution을 통해 DRM 컨텐츠를 전달받거나 자신이 가진 사용권이 만료된 클라이언트 단말은 DRM 컨텐츠에 명시된 컨텐츠 분배자에게 사용권 발행을 요청한다. 클라이언트 단말의 사용권 발행 요청을 수용한 컨텐츠 분배자는 사용권 발행자의 사용권 발급 모듈에게 사용자 식별자(User ID), CID, 희망하는 usage, 클라이언트 단말의 공개키 Kpd를 가지고 사용권 발급을 요청한다. 사용권 발행 모듈은 사용권 생성 모듈에게 CID와 희망하는 usage, 그리고 Kpd를 전달하여 사용권 생성을 요청한다. 사용권 생성 모듈은 CEK와 CID, usage를 이용하여 right를 생성한 후 이를 Kpd로 암호화 하여 사용권 발행 모듈로 전달한다.

사용권 발행자는 클라이언트 단말에게 발행할 사용권의 URI를 Push한다.



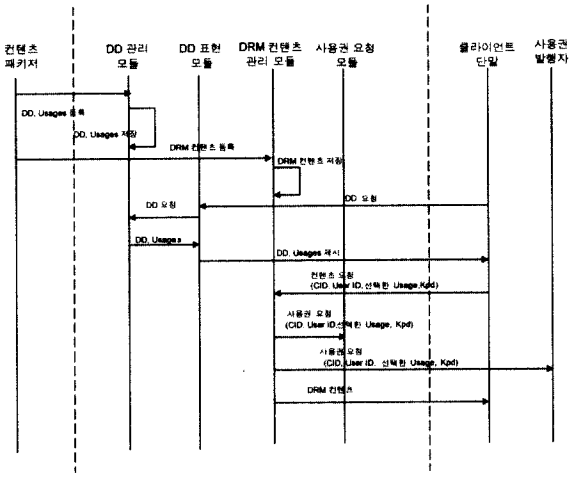
(그림 3) 사용권 발행자 처리 기법

4.4 컨텐츠 분배자(Contents Distributor)

(그림 4)에서와 같이 컨텐츠 분배자는 DD를 관리하는 Presentation 서버와 DRM 컨텐츠를 관리하는 Download 서버로 구성된다. Presentation 서버는 DD와 해당하는 usage 목록을 저장하고 관리하는 기능을 하는 DD 관리 모듈과 사용자로부터 HTTP/WSP 요청을 받아 DD를 보여주는 기

능을 하는 DD 표현 모듈로 구성된다.

Download 서버는 DRM 컨텐츠를 저장하고 관리하며 컨텐츠 제공 요청을 받으면 DRM 컨텐츠를 검색하여 클라이언트 단말로 전송하는 DRM 컨텐츠 관리 모듈과 DRM 컨텐츠 관리 모듈에서 DRM 컨텐츠를 클라이언트 단말로 전송한 후, 사용권 발행자에게 사용권 발급을 요청하는 사용권 요청 모듈로 구성된다.

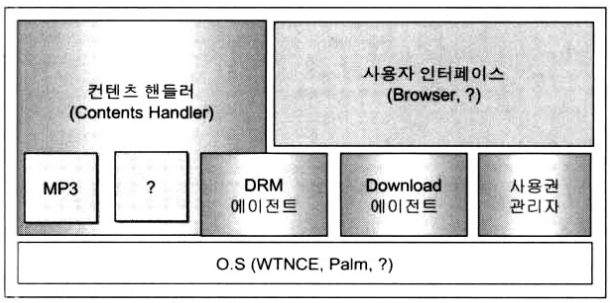


(그림 4) 컨텐츠 분배자 처리 과정

4.5 클라이언트 단말

4.5.1 구성 요소

무선 DRM 클라이언트 구성 요소는 (그림 5)와 같다.



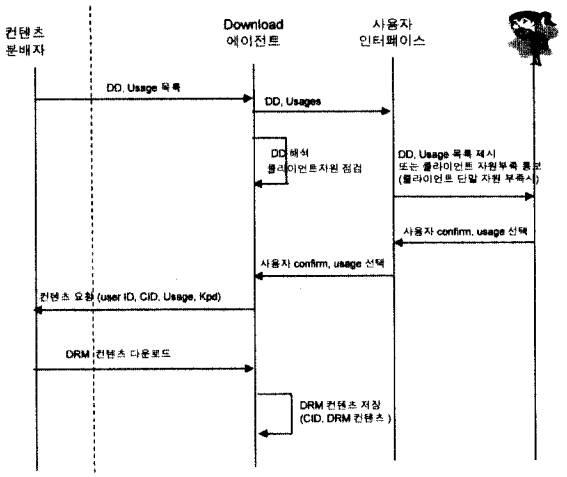
(그림 5) 클라이언트 구성요소

- 사용자 인터페이스 : 무선 인터넷에서 사용하는 웹 브라우저
- 컨텐츠 핸들러 : DRM 컨텐츠를 사용자가 이용할 수 있게 해주는 응용 프로그램이다. DRM 에이전트를 통해서만 DRM 컨텐츠를 동작시킬 수 있다.
- DRM 에이전트 : DRM 컨텐츠 사용을 제어한다. 사용권이 올바른 경우에만 컨텐츠 복호화를 진행하여 사용이 가능하도록 한다. 또한 DRM 컨텐츠를 저장하고 관리하며 DRM 컨텐츠의 암/복호화 기능도 갖는다.
- Download 에이전트 : 사용자에게 DD 정보를 전달하고 DRM 컨텐츠 다운로드시, 클라이언트 단말에 충분한 자원이 있는지에 대한 상태 보고 기능도 포함한다.
- 사용권 관리자 : 사용권 정보를 클라이언트 단말에 안전하게 저장하기 위해 암호화 모듈과 암호화에 사용될 키를 생성하는 기능을 갖는다. DRM 컨텐츠 이용시 사용권 정보를 점검하고 갱신하며 사용권 풀(DB 또는 파일)을 관리한다.

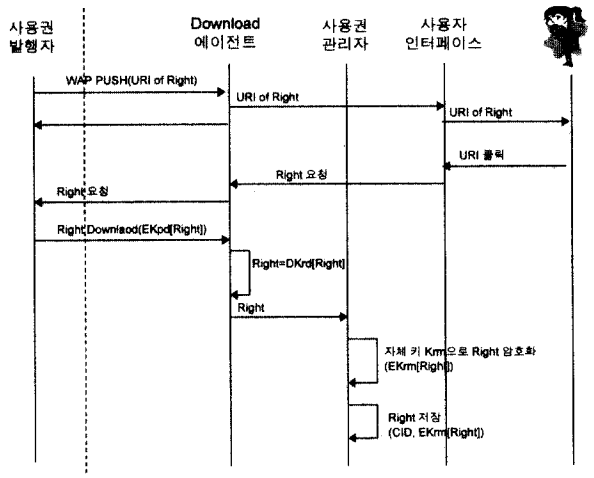
4.5.2 처리 메커니즘

(1) 컨텐츠 설치 과정(컨텐츠 및 사용권 다운로드 및 저장)

DRM 컨텐츠와 자신의 공개키로 암호화된 사용권을 다운로드한 클라이언트의 Download 에이전트는 (그림 6)과 같은 과정을 거쳐 클라이언트에 DRM 컨텐츠와 사용권을 설치한다.



(그림 6) DRM 컨텐츠 다운로드 과정



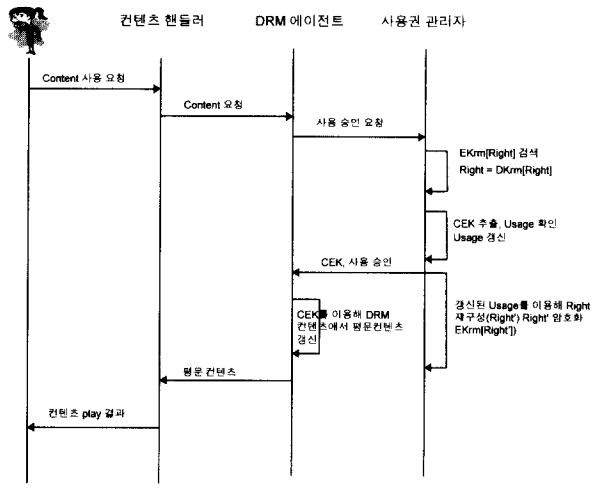
(그림 7) 사용권 다운로드 과정

사용권 다운로드는 (그림 7)과 같은 순서로 이루어진다. 컨텐츠 분배자로부터 사용권 발행 요청을 접수한 사용권 발행자는 사용자의 클라이언트 단말로 사용권의 URI를 보

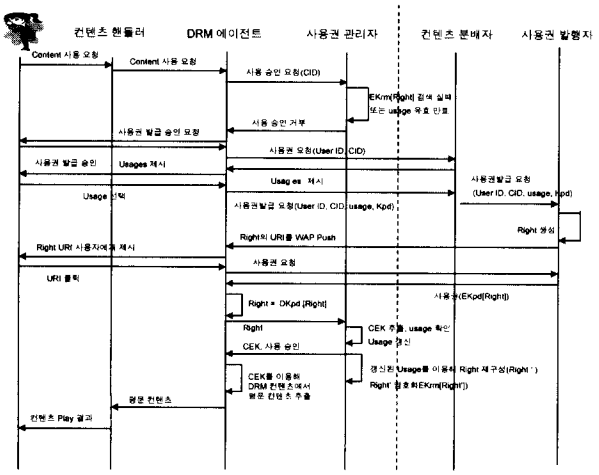
내면 사용자는 사용권 URI를 클릭하여 사용권 발행자로부터 클라이언트 단말의 공개키로 암호화된 사용권을 다운로드 받는다. 다운로드된 컨텐츠의 사용권은 클라이언트 단말의 사용권 관리자가 클라이언트의 단말의 비밀키 Krd를 사용하여 전달받은 사용권을 복호화한 후 클라이언트 단말 자체 암호화 키(Krm)로 사용권을 암호화하여 CID와 함께 저장한다.

(2) 컨텐츠 사용 과정

컨텐츠 핸들러가 컨텐츠를 사용하는 과정은 (그림 8)과 같다. 사용자가 DRM 컨텐츠 사용을 요청하면 컨텐츠 핸들러는 DRM 에이전트에게 DRM 컨텐츠를 요청하여 컨텐츠 실행 승인을 획득한다.



(그림 8) 컨텐츠 사용 과정



(그림 9) 사용권이 파기되거나 없는 경우 재발급 과정

(그림 9)는 해당 컨텐츠 대한 사용권이 존재하지 않는 경우 사용권을 재발급 받는 과정과 superdistribution에서 사용권을 발급받는 과정을 보여준다. DRM 에이전트는 사용자에게 컨텐츠 사용권이 없음을 알리고 사용권 발행 승인을 요청한다. 사용자의 사용권 발행 승인을 취득한 DRM 에이전트는 CID를 사용하여 DRM 컨텐츠에 명시되어 있는 컨텐츠 분배자에게 사용권 발급을 요청한다. 사용권 발급을 요청 받은 컨텐츠 분배자는 사용자에게 해당 컨텐츠의 usages를 제시하고, 사용자는 그 중 하나의 usage를 선택하여 DRM 에이전트를 통해 컨텐츠 분배자에게 사용권을 요청한다.

5. 구현 결과와 평가

5.1 구현 및 시험 환경

본 시스템의 구현 및 시험 환경은 <표 1>과 같다.

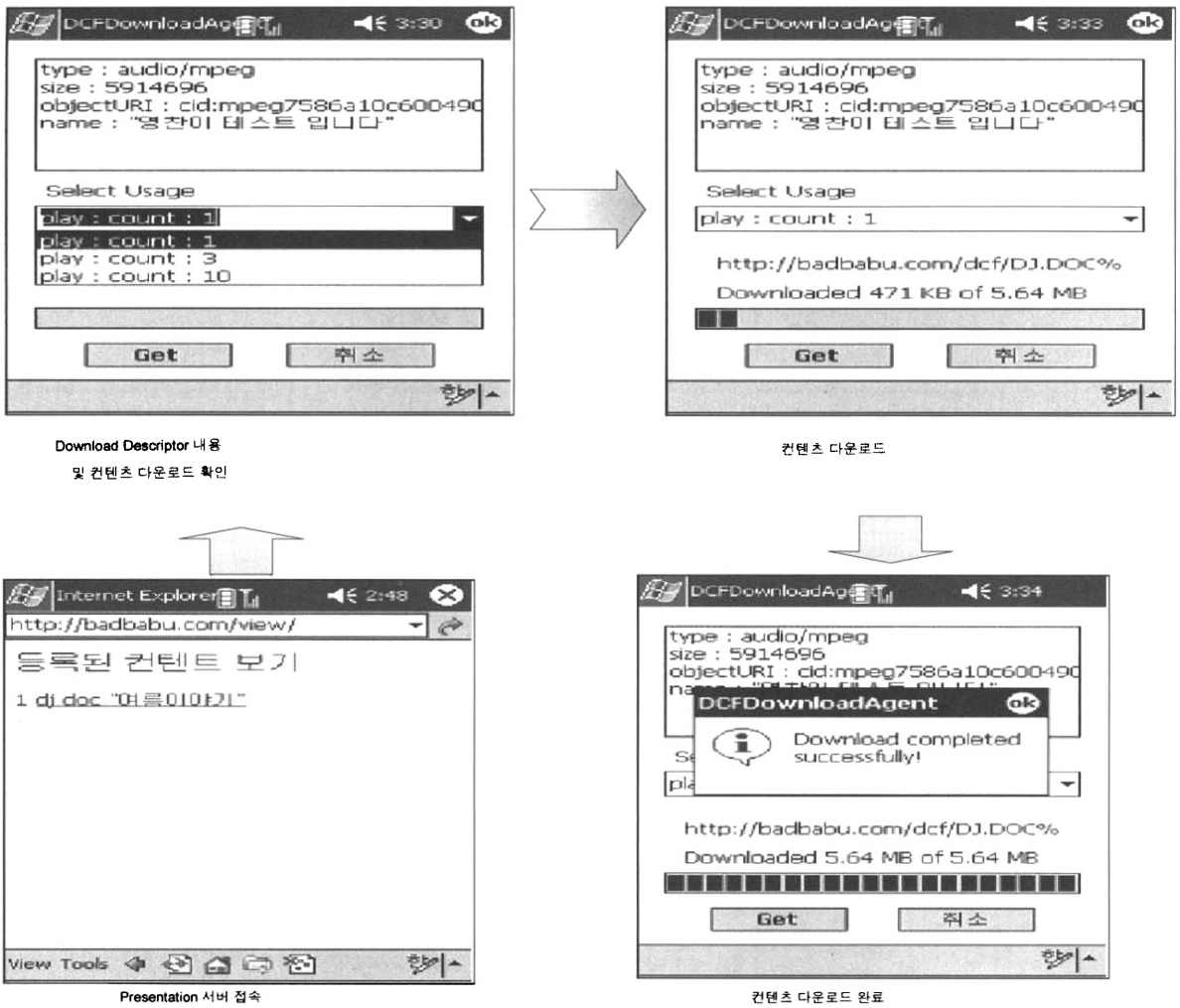
〈표 1〉 개발 환경

구 성 요 소	개 발 환 경
컨텐츠 패키저	• 운영체제 : Windows 98/ME/2000/XP • 개발언어 : XML, C/C++ • User Interface : Windows GUI
컨텐츠 분배자	• 운영체제 : Windows NT (Windows 2000 Professional) • 개발언어 : PHP, C/C++ • Web Server : IIS • Data Base : My SQL • User Interface : Web Browser
사용권 발행자	• 운영체제 : Windows NT (Windows 2000 Professional) • 개발언어 : PHP, C/C++ • Web Server : IIS • Data Base : My SQL • User Interface : WAP Push
DRM 클라이언트	• 플랫폼 : PocketPC 2002 • 운영체제 : WinCE PDA • 컨텐츠 핸들러 : GNU MVP 플레이어

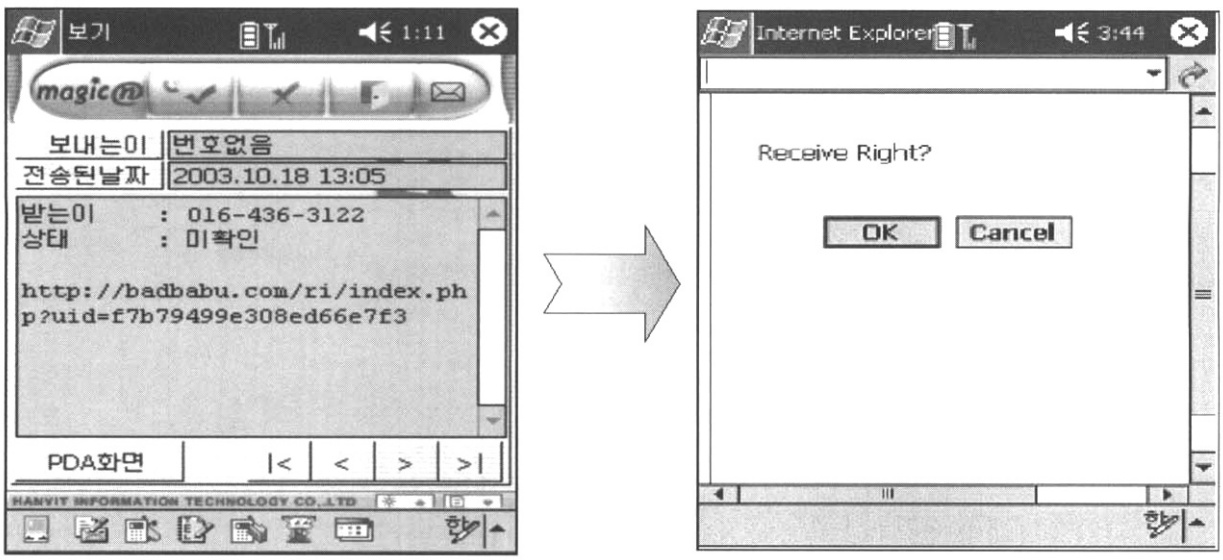
5.2 DRM 시스템 동작

(그림 10)은 클라이언트 단말에서 컨텐츠를 다운로드하는 과정을 보여준다. 사용자가 클라이언트 단말을 통해 컨텐츠 분배자의 URL에 접속하면 컨텐츠 분배자가 제공하는 컨텐츠 목록이 화면에 나타난다. 사용자가 다운로드 하고자 하는 컨텐츠를 클릭하면 원격의 컨텐츠 분배자는 DD와 사용자가 선택해야 하는 usgaes를 클라이언트 단말로 전송한다. 사용자가 자신이 원하는 usage을 선택하면 사용자가 선택한 usage가 컨텐츠 분배자에게 전송됨을 확인할 수 있다. 클라이언트 단말의 모든 요구 사항을 수용한 컨텐츠 분배자 사용권 발행자에게 클라이언트의 요구사항을 전달하고 클라이언트 단말로 컨텐츠를 전송한다.

사용권 발행자는 right의 URI를 클라이언트 단말로 push 해 주고 사용자가 사용권 발행을 승인하면 사용권 발행자는 클라이언트 기기로 사용권을 발행한다. (그림 11)은 right 다운로드 화면을 보여준다.



(그림 10) 컨텐츠 다운로드



(그림 11) 사용권 다운로드

DRM 컨텐츠를 사용하고자 하는 사용자는 컨텐츠 목록에서 사용하기를 원하는 DRM 컨텐츠를 선택한다. DRM 컨텐츠를 실행할 컨텐츠 핸들러가 *.dcf 파일 확장자를 보고 DRM 에이전트를 호출한다. DRM 에이전트는 컨텐츠 핸들러가 이해할 수 있는 형태로 DRM 컨텐츠를 복호화한 후 컨텐츠 핸들러에게 전달하고 컨텐츠 핸들러는 컨텐츠를 실행한다.

5.3 시스템 시험 및 분석

5.3.1 시스템 기능 시험

본 논문에서 설계 구현한 시스템 기능 시험 항목 및 시험 결과는 <표 2>와 같다.

5.4 시스템 분석

본 논문에서 구현한 무선 DRM 시스템은 OMA DRM의

〈표 2〉 시스템 기능 시험 항목 및 결과

시험 항목	세 부 항 목	시험 시나리오	예상 결과	결 과
DRM 컨텐츠 및 사용권 다운로드 시험	정상적인 다운로드 시험	1. 사용자가 브라우저의 주소 창에 컨텐츠 분배자 주소 입력 2. 사용자가 브라우저에 제시된 컨텐츠 목록 중 하나 선택 3. 컨텐츠 분배자가 클라이언트 기기를 통해 사용자에게 DD와 usages 제시 4. 사용자가 제시된 usages 중 하나 선택 후 GET 버튼 클릭 5. 컨텐츠 분배자로부터 클라이언트 단말로 DRM 컨텐츠가 다운로드 됨 6. 사용권 발행자가 사용권의 URI를 클라이언트 기기로 Push 7. 사용자가 사용권 URI 더블 클릭 8. 사용권이 클라이언트 단말로 다운로드 됨	클라이언트 단말에 다운로드된 DRM 컨텐츠 존재	클라이언트 단말에서 *.dcf 파일 확인
	클라이언트 단말 자원 부족	1. 사용자가 브라우저의 주소창에 컨텐츠 분배자 주소 입력 2. 사용자가 브라우저에 제시된 컨텐츠 목록 중 하나 선택 3. 컨텐츠 분배자가 클라리언트 단말을 통해 사용자에게 DD와 usages 제시 4. 클라이언트 단말이 선택한 DRM 컨텐츠를 설치하기에 자원이 부족함을 사용자에게 경고	클라이언트 단말이 DRM 컨텐츠 설치를 위한 충분한 자원이 없음을 알림	클라이언트 단말에 DRM 컨텐츠 설치 자원 부족 경고창이 뜸
DRM 컨텐츠 실행 시험	정상적인 경우	1. 사용자가 클라이언트 단말에 있는 DRM 컨텐츠 중 하나를 더블 클릭 또는 컨텐츠 핸들러를 실행시켜 컨텐츠 핸들러의 파일 open을 이용하여 DRM 컨텐츠 선택 2. 컨텐츠 핸들러가 선택한 컨텐츠를 실행함	컨텐츠가 실행 된다.	mp3 컨텐츠가 실행됨
	사용권 유효기간 만료, expire, 부재인 경우 (사용자가 사용권 발행 승인)	1. 사용자가 클라이언트 단말에 있는 DRM 컨텐츠 중 하나를 더블 클릭 또는 컨텐츠 핸들러를 실행시켜 컨텐츠 핸들러의 파일 open을 이용하여 DRM 컨텐츠 선택 2. 클라이언트 단말에 사용권 발행 승인 요청 창이 뜸 3. 사용자가 사용권 발행 요청을 승인함 4. 사용자가 제시된 usages 중 하나 선택 후 GET 버튼 클릭 5. 사용자가 사용권 URI를 더블 클릭 6. 클라이언트 단말로 사용권이 다운로드 됨 7. 컨텐츠 핸들러가 컨텐츠를 실행	컨텐츠가 실행 된다.	mp3 컨텐츠가 실행됨
	사용권 유효기간 만료, expire, 부재인 경우 (사용자가 사용권 발행 승인 안함)	1. 사용자가 클라이언트 단말에 있는 DRM 컨텐츠 중 하나를 더블 클릭 또는 컨텐츠 핸들러를 실행시켜 컨텐츠 핸들러의 파일 open을 이용하여 DRM 컨텐츠 선택 2. 클라이언트 단말에 사용권 발행 승인 요청창이 뜸 3. 사용자가 사용권 발행 요청을 거부함 4. 컨텐츠 핸들러가 컨텐츠 실행을 못함	컨텐츠 핸들러가 컨텐츠 실행 오류 메시지 발행	컨텐츠 핸들러가 컨텐츠 실행 오류 메시지 발행

기본을 유지하면서 OMA DRM에서 다루지 않은 보안 구조 및 무선 DRM 시스템의 전체 모델 등을 제시하였다. <표 3>에 OMA DRM 시스템과 본 논문에서 구현한 무선 DRM 시스템을 비교한 것이다. 현재까지 나와 있는 대부분의 무선 DRM 시스템들이 클라이언트 단말에서 하드웨어적으로 "Forward-Lock"을 제공하는 수준에 머무르고 있을 뿐 컨텐츠를 한시적으로 사용할 수 있게 하는 사용권 발급 기능 등을 제공하지 않고 있다.

〈표 3〉 시스템 시험 항목 및 결과

항 목		본 시스템	OMA DRM 시스템
보안 기술	클라이언트 단말(또는 사용자) 인증	클라이언트 공개키 이용	지원하지 않음
	클라이언트 단말 내에 인가되지 않은 개체에 의한 DRM 개체 접근 금지(접근제어)	암호화 기술을 적용하여 클라이언트 기기 내에 안전하게 사용권 보관(단말 자체 키 Krm 사용)	지원하지 않음
	암호 기술	자체 암호 라이브러리 사용	AES
사용권 발행 주체		컨텐츠 분배자(portal)	컨텐츠 제공자
유·무선 연동		고려 사용자 인터페이스 HTML 기반	언급 없음
DRM 컨텐츠		CFP(OMA DCF 확장) (컨텐츠 분배자의 URI 명시)	DCF 형식 제공
패키징 정보(메타 데이터)		OMA 규격 준수	XML 기반 DD 형식 제공
사용권		OMA 규격 준수	ODRL 기반 Right 형식 제공
사용 규칙 목록 형식		XML로 제공	고려하지 않음
별도 player 필요		필요 없음	고려하지 않음

6. 결 론

본 논문에서는 무선 환경에서 유통되는 디지털 컨텐츠의 저작권을 보호하기 위한 DRM 시스템 설계 및 구현하였다. 본 시스템 설계 및 구현시 최우선 고려 사항은 추후의 확장성을 위한 표준안 수용이었다. 현재까지의 대부분의 DRM 시스템이 유선 환경에서의 디지털 컨텐츠를 고려하고 있으며, 무선 디지털 컨텐츠의 유통이 활발해지면서 무선망 사업자들을 중심으로 한 무선 DRM 시스템들이 개발, 적용되고 있는 상태이다.

본 논문에서 제시한 DRM 시스템에서는 클라이언트 단말이 컨텐츠 분배자로부터 컨텐츠를 다운로드하고, 해당 컨텐츠에 대한 사용권은 사용권 발행자에 의해 SMS 또는 WAP Push 서비스 형태로 전송 받으므로 사용자 입장에서는 컨텐츠 다운로드 시간을 단축할 수 있다는 장점이 있다. 만약 현재의 대부분의 DRM 시스템의 경우처럼 컨텐츠와 컨텐츠 사용권이 함께 클라이언트 단말로 다운로드된다면 다운로드 시간의 증가로 무선 인터넷의 특징인 disconnection 등의 문제가 발생하여 컨텐츠 다운로드가 중단될 수도 있다. 또한 사용자 입장에서는 다운로드 시간의 증가로 인한 회선 사용료에 대한 부담이 가중되는 문제점이 있다. 무선 컨텐츠와 컨텐츠 사용권을 분리함으로써 얻는 또 하나의 이점은 클라이언트 단말이 불법적으로 다른 클라이언트 단말로 컨텐츠를 전송 사용하는 것을 방지할 수 있다는 점이다. 불법으로 디지털 컨텐츠를 취득한 클라이언트 단말은 컨텐츠에 대한 사용권을 취득하지 않는 한 컨텐츠를 사용할 수 없다. 이 경우에 사용권의 불법적인 전송 문제를 우려할 수 있으나 본 논문에서는 사용권을 클라이언트 단말 내의 사용권 관리자의 비밀키에 의해 암호화해 저장하고 있다. 사용권 관리자의 비밀키는 사용자가 알아낼 수 없도록 사용권 관리자가 초기화 될 때 생성되며 수시로 변경된다.

본 논문에서는 현재 PDA나 이동 전화기 등의 무선 클라이언트 단말의 인증에 관한 자세한 부분에 대해 다루지는 못했다. 그러나 클라이언트 단말의 공개키와 컨텐츠 다운로드 요청시마다 발생하는 클라이언트 단말 고유 식별자에 의한 부분적인 클라이언트 단말 인증 방법을 제공하였다. WPKI[17]와 WIM[16] 등을 이용한 무선 클라이언트 기기를 인증하는 부분을 추후에 연구할 계획이다.

참 고 문 헌

[1] 박복녕, 김태윤, 디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜, 정보과학회논문지, Vol.30, No.2, pp.189-198, Apr., 2003.

[2] 박주상, 윤기송, 박창순, Microsoft의 디지털 저작권 보호 기술 분석 및 향후 시스템 개발 요소, 정보처리학회 2002년 추계학술발표대회, Vol.9, No.2, Oct., 2002.

[3] 박지현, 윤기송, 박창순, DRM 기반 유통시스템을 위한 컨텐츠 패키저 설계, 정보처리학회 2002년 추계학술대회, Vol.9, No.2, Oct., 2002.

[4] 성수련, 정인성, 신용태, 이준석, 정연정, DRM 유통시스템에서의 보안 통신 모듈 설계 및 구현, 정보처리학회 2002년 추계학술발표대회, Vol.9, No.2, Oct., 2002.

[5] 이덕규, 박희운, 이임영, Agent 기반 불법 복제 방지 DRM 모델, 정보과학회 2001년 추계학술대회, Vol.28, No.2, pp. 682-684, Oct., 2001.

[6] 이용효, 황대준, 에이전트 기반의 동적 디지털저작권관리

시스템 설계 및 구현, 정보처리학회논문지D, Vol.8-D, No. 5, pp.613-622, Oct., 2001.
[7] 장성호, 이창열, 이준석, 김정현, 디지털 컨텐츠의 권리관리에 관한 연구, 한국정보처리학회 2002년 추계학술발표대회, Vol.9, No.2, Oct., 2002.
[8] F. Hartung, F. Ramme, Digital rights management and watermarking of multimedia content for m-commerce applications, IEEE Communications Magazine, Vol.38, No. 11, pp.78-84, Nov., 2000.
[9] L. J. Camp, First principles of copyright for DRM design, IEEE Internet Computing, Vol.7, No.3, pp.59-65, May, 2003.
[10] 3GPP, Digital Rights Management Technical Specification, Jan., 2002.
[11] OMA, Digital Rights Management V1.0, Sep., 2002.
[12] OMA, Download Architecture V1.0, June, 2002.
[13] OMA, DRM Contents Format V1.0, Aug., 2003.
[14] OMA, DRM Rights Expression Language, Aug., 2003.
[15] OMA, Generic Content Download Over The Air Specification V1.0, Feb., 2003.
[16] WAP Forum, Wireless Application Protocol Identity Module, Apr., 2001.
[17] WAP Forum, Wireless Application Protocol Public Key Infrastructure Definition Specification, Nov., 1999.
[18] WAP Forum, WAP Push Architectural Overview version 0.8, Nov., 1999.
[19] WAP Forum, Wireless Session Protocol Version 1.0, Sep., 2002.
[20] W3C : Extensible Markup Language (XML), http://www.w3.org/XML/.
[21] W3C : Open Digital Rights Language(ODRL) Version 1.1, http://www.w3.org/TR/2002 /NOTE-odrl-20020919/.

이 권 일

e-mail : kilee@mail.ddc.ac.kr
1988년 충남대학교 계산통계학과(이학사)
1998년 충남대학교 컴퓨터과학과(이학석사)
2002년 충남대학교 컴퓨터과학과 박사수료
1988년~2000년 한국전자통신연구원 선임연구원
2000년~현재 대덕대학 컴퓨터인터넷정보계열 조교수
관심분야 : 유·무선 인터넷보안, 분산처리시스템, 컨텐츠 보호, 인증시스템

김 봉 선

e-mail : iam7998@hotmail.com
2002년 충남대학교 컴퓨터과학과(이학사)
2004년 충남대학교 컴퓨터과학과(이학석사)
2004년 현재 삼성전자
관심분야 : 유·무선 인터넷보안, 디지털 컨텐츠 보호, 인증시스템

신 영 찬

e-mail : badbabu@home.cnu.ac.kr
2003년 충남대학교 컴퓨터과학과(이학사)
2003년 충남대학교 컴퓨터과학과 대학원 석사과정 재학중
관심분야 : 유·무선 인터넷보안, 디지털 컨텐츠 보호, 인증시스템

류 재 철

e-mail : jcryou@home.cnu.ac.kr
1985년 한양대학교 산업공학과(공학사)
1988년 Iowa State University 전산학과 (공학 석사)
1990년 Northwestern University 전산학과 (이학박사)
1991년~현재 충남대학교 정보통신공학부 교수
1993년~1995년 JTC1/SC27 보안기술 전문위원회 위원
1995년~1996년 시스템공학연구소 초빙연구원
1996년~1998년 OSIA Internet-KIG Security WG 위원장
1997년~현재 한국정보보호학회 이사
2001년~현재 국가정보원 정보보호시스템 인증위원회 위원
2003년~현재 한국정보처리학회 논문지편집위원
관심분야 : 스마트 카드 보안, 인증이론 및 시스템, 유·무선 인터넷 보안, 저작권 보호

이 준 석

e-mail : leejs@etri.re.kr
1986년 아주대학교 전산학과(공학사)
1989년 동국대학교 전산학과(공학 석사)
2004년 충남대학교 컴퓨터 과학과(이학박사)
1991년~현재 한국전자통신연구원 책임연구원
관심분야 : 보안, 저작권 보호