(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년01월02일
(11) 등록번호 10-1100391
(24) 등록일자 2011년12월22일

(51) Int. Cl.
G11B 20/10 (2006.01)
(21) 출원번호 10-2004-0039662
(22) 출원일자 2004년06월01일
심사청구일자 2009년05월26일
(65) 공개번호 10-2005-0114442
(43) 공개일자 2005년12월06일
(56) 선행기술조사문헌
JP2002073421 A*
JP2003264590 A*
WO2003083746 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
이병래
경기도 용인시 수지읍 상현리 만현마을 성원상떼빌 306동 10 4호
김태성
서울특별시 동작구 상도1동 215-1 고이빌라트 202호
(뒷면에 계속)
(74) 대리인
정상빈, 특허법인가산

전체 청구항 수 : 총 19 항 심사관 : 변성철

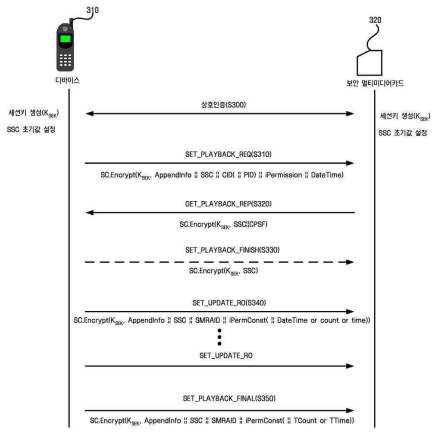
(54) 휴대형 저장장치와 디바이스간에 디지털 저작권 관리를이용한 콘텐츠 재생방법 및 장치와, 이를 위한 휴대형저장장치

(57) 요 약

휴대형 저장장치와 디바이스간에 디지털 저작권 관리를 이용한 콘텐츠를 재생하는 방법 및, 이를 위한 휴대형 저장장치를 제공한다.

휴대형 저장장치를 이용한 콘텐츠 재생방법은 DRM으로 보호되는 휴대형 저장장치에 콘텐츠에 대한 재생권리의 전송을 요청하는 단계와, 상기 휴대형 저장장치로부터 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리를 수신하는 단계, 및 상기 재생권리를 이용한 상기 DRM으로 보호되는 콘텐츠의 재생이 완료되면 재생이 완료되었음을 상기 휴대형 저장장치에 알리는 단계를 포함한다.

대 표 도 - 도3



(72) 발명자

정경임

경기도 성남시 분당구 정자동 88번지 느티마을 주공3단지 31 0동 2402호

오윤상

서울특별시 강남구 도곡2동 타워팰리스아파트 C-2901

김신한

서울특별시 성북구 동소문동4가 103-3

특허청구의 범위

청구항 1

암호화된 디지털 콘텐츠를 재생하기 위한 라이센스에 해당하는 별도의 재생권리를 요구하는 DRM으로 보호되는 휴대형 저장장치에 콘텐츠에 대한 상기 재생권리의 전송을 요청하는 단계;

상기 휴대형 저장장치로부터 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리를 수신하는 단계;

상기 재생권리를 이용한 상기 DRM으로 보호되는 콘텐츠의 재생이 완료되면 재생이 완료되었음을 상기 휴대형 저장장치에 알리는 단계; 및

상기 휴대형 저장장치에 상기 재생권리의 업데이트 명령을 전송하여, 상기 DRM으로 보호되는 콘텐츠를 관리하는 단계를 포함하되,

상기 재생권리의 업데이트 명령은 상기 휴대형 저장장치에 저장된 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리의 일부를 갱신하기 위한 데이터를 포함하는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 2

제1항에 있어서,

상기 휴대형 저장장치에 전송하는 데이터 및 상기 휴대형 저장장치로부터 전송되는 데이터는 대칭키 암호화방식으로 암호화된 데이터인 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 3

제1항에 있어서,

상기 휴대형 저장장치에 전송하는 데이터 및 상기 휴대형 저장장치로부터 전송되는 데이터에는 전송 시퀀스를 알려주는 전송 시퀀스 카운터가 포함되어 있는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 4

제3항에 있어서,

상기 전송 시퀀스 카운터의 초기값을 상기 휴대형 저장장치와 디바이스의 상호인증과정에서 얻은 난수들을 이용하여 설정하는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 5

제1항에 있어서,

상기 재생권리는 상기 DRM으로 보호되는 콘텐츠를 재생하기 위한 라이센스에 해당하는 권리객체에 포함된 정보들 중에서 상기 DRM으로 보호되는 콘텐츠의 재생을 위한 소정의 정보들을 포함하는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 6

제5항에 있어서,

상기 DRM으로 보호되는 콘텐츠는 암호화된 콘텐츠이고, 상기 재생권리는 상기 암호화된 콘텐츠를 복호화할 수 있는 콘텐츠 암호화 키를 포함하는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 7

제1항에 있어서,

상기 재생권리의 업데이트 명령의 상기 데이터는 상기 DRM으로 보호되는 콘텐츠의 재생으로 인해 소비한 한정사항(횟수, 시간)에 대한 정보를 포함하는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

제1항에 있어서,

상기 콘텐츠의 재생이 완료되면 재생이 완료되었음을 알릴 때, 상기 DRM으로 보호되는 콘텐츠의 재생으로 인해 소비한 총한정사항(총횟수, 총시간)에 대한 정보를 함께 알려주는 휴대형 저장장치를 이용한 콘텐츠 재생방법.

청구항 13

디바이스로부터, 암호화된 디지털 콘텐츠를 재생하기 위한 라이센스에 해당하는 별도의 재생권리를 요구하는 DRM으로 보호되는 콘텐츠에 대한 상기 재생권리의 전송을 요청받는 단계;

상기 요청에 따라 상기 디바이스에 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리를 전송하는 단계; 및

상기 디바이스에서 상기 DRM으로 보호되는 콘텐츠를 재생한 후, 상기 DRM으로 보호되는 콘텐츠를 재생하기 위한 라이센스에 해당하는 권리객체에 소비된 한정사항 정보를 갱신하기 위한 업데이트 명령을 수신하는 단계를 포함하되,

상기 업데이트 명령은 휴대형 저장장치에 저장된 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리의 일부를 갱신하기 위한 데이터를 포함하는 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 14

제13항에 있어서,

상기 디바이스에 전송하는 데이터 및 상기 디바이스로부터 전송되는 데이터는 대칭키 암호화 방식으로 암호화된 데이터인 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 15

제13항에 있어서,

상기 디바이스에 전송하는 데이터 및 상기 디바이스로부터 전송되는 데이터에는 전송 시퀀스를 알려주는 전송 시퀀스 카운터가 포함되어 있는 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 16

제15항에 있어서,

상기 전송 시퀀스 카운터의 초기값을 상기 디바이스와 휴대형 저장장치의 상호인증과정에서 얻은 난수들을 이용하여 설정하는 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 17

제13항에 있어서,

상기 재생권리는 상기 DRM으로 보호되는 콘텐츠에 대한 권리객체에 포함된 정보들 중에서 상기 DRM으로 보호되는 콘텐츠의 재생을 위한 소정의 정보들을 포함하는 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 18

제17항에 있어서,

상기 DRM으로 보호되는 콘텐츠는 암호화된 콘텐츠이고, 상기 요청받은 재생권리는 상기 암호화된 콘텐츠를 복호화할 수 있는 콘텐츠 암호화 키인 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 19

제13항에 있어서,

상기 수신된 업데이트 명령에는 상기 DRM으로 보호되는 콘텐츠의 재생으로 인해 소비한 한정사항(횟수, 시간)에 대한 정보를 포함하는 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

제13항에 있어서,

상기 디바이스로부터 재생 기능 완료를 수신하는 단계를 더 포함하며, 상기 재생 기능 완료에는 권리객체의 사용총계의 무결성을 체크하기 위해 상기 수신된 권리객체의 업데이트 명령을 재확인하기 위한 정보를 포함하는 디바이스에 콘텐츠 재생권리를 보내는 방법.

청구항 24

디바이스와의 연결을 위한 인터페이스;

적어도 하나 이상의 암호화된 권리객체들을 저장하고 있는 권리객체 저장모듈;

세션키 생성과 대칭키 방식의 암호화와 공개키 방식의 암호화를 수행하는 암호화 모듈; 및

DRM 동작을 수행하는 DRM 에이전트 모듈을 포함하며,

상기 권리객체들은 암호화된 디지털 콘텐츠를 재생하기 위한 라이센스에 해당하고,

상기 DRM 에이전트 모듈은 상기 인터페이스를 통해 디바이스로부터 특정 콘텐츠에 대한 재생권리를 전송을 요청받으면 상기 권리객체 저장모듈에 저장된 권리객체들 중에서 상기 콘텐츠에 대한 권리객체를 찾고, 상기 권리객체에 포함된 상기 콘텐츠를 재생하는데 필요한 정보를 상기 암호화 모듈을 이용하여 암호화하고 상기 인터페이스를 통해 상기 디바이스에 보내도록 하는 과정을 수행하되,

상기 디바이스에서 DRM으로 보호되는 콘텐츠를 재생한 후, 상기 DRM 에이전트는 소비된 한정사항 정보를 갱신하기 위해 업데이트 명령에 기초하여 상기 권리객체를 업데이트 시키는 과정을 더 수행하고,

상기 업데이트 명령은 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리의 일부를 갱신하기 위한 데이터를 포함하는 휴대형 저장장치.

청구항 25

삭제

청구항 26

휴대형 저장장치와 연결을 위한 인터페이스;

암호화된 디지털 콘텐츠를 재생하기 위한 라이센스에 해당하는 별도의 재생권리를 요구하는 DRM으로 보호되는 적어도 하나 이상의 콘텐츠를 저장하고 있는 콘텐츠 저장모듈;

세션키 생성과 대칭키 방식의 암호화와 공개키 방식의 암호화를 수행하는 암호화 모듈; 및

DRM 동작을 수행하는 DRM 에이전트 모듈을 포함하며,

상기 DRM 에이전트 모듈은 상기 인터페이스를 통해 상기 콘텐츠 저장모듈에 저장된 DRM으로 보호되는 어느 한 콘텐츠에 대한 재생권리를 상기 휴대형 저장장치에게 요청하고, 상기 휴대형 저장장치로부터 암호화된 재생권리를 수신하고, 상기 암호화 모듈을 이용하여 상기 수신된 암호화된 재생권리를 복호화하고, 암호화된 콘텐츠를 재생하기 위해 상기 복호화 된 재생권리에 포함된 콘텐츠 암호화 키를 얻되,

콘텐츠 재생이 끝난 후 상기 DRM 에이전트는 상기 휴대형 저장장치에 권리객체 업데이트를 요청하기 위해 업데이트 명령을 전송하는 단계를 더 수행하고,

상기 업데이트 명령은 상기 DRM으로 보호되는 어느 한 콘텐츠에 대한 재생권리의 일부를 갱신하기 위한 데이터를 포함하는 휴대형 저장장치를 이용한 콘텐츠 재생장치.

청구항 27

삭제

청구항 28

제1항 내지 제7항, 제12항 내지 제19항, 및 제23항 중 어느 한 항의 방법을 수행하는 컴퓨터로 읽을 수 있는 프로그램을 기록한 기록매체.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0010] 본 발명은 디지털 저작권 관리에 관한 것으로서, 보다 상세하게는 휴대형 저장장치와 디바이스간에 디지털 저작권 관리를 이용한 콘텐츠를 재생하는 방법 및 장치와, 이를 위한 휴대형 저장장치에 관한 것이다.

[0011] 최근에 디지털 저작권 관리(Digital Rights Management; 이하, "DRM"이라 함)에 관한 연구가 활발하며, DRM을 적용한 상용 서비스들이 도입되었거나 도입중에 있다. DRM이 되입되어야 하는 이유는 디지털 데이터가 갖는 여러가지 특성으로부터 도출할 수 있다. 디지털 데이터는 아날로그 데이터와는 달리 손실이 없이 복제가 가능하다는 특성과, 재사용 및 가공이 용이한 특성과, 쉽게 제3자에게 배포할 수 있다는 특성을 가지고 있으며, 매우 적은 비용으로 이러한 복제와 배포를 손쉽게 할 수 있다는 특성을 가지고 있다. 그에 반해 디지털 콘텐츠는 그 제작에 많은 비용과 노력 및 시간을 필요로 한다. 따라서 디지털 콘텐츠의 무단 복제 및 배포가 용인될 경우에, 이는 디지털 콘텐츠 제작자의 이익을 침해하게 되고 디지털 콘텐츠 제작자의 창작 의욕은 꺽이게 될 것이고 이는 디지털 콘텐츠 산업의 활성화에 큰 저해요소가 된다.

[0012] 디지털 콘텐츠를 보호하고자 하는 노력은 과거에도 있었으나, 과거에는 주로 디지털 콘텐츠 무단접근 방지에 중점을 두고 있었다. 다시 말하면, 디지털 콘텐츠에 대한 접근(access)은 대가를 지불한 일부 사람에게만 허용되었다. 따라서 대가를 지불한 사람은 암호화되지 않은 디지털 콘텐츠에 접근할 수 있으며, 그렇지 않은 사람은 디지털 콘텐츠에 접근할 수 없었다. 그렇지만 대가를 지불한 사람이 접근한 디지털 콘텐츠를 고의적으로 제3자에게 배포할 경우에 제3자는 대가를 지불하지 않고도 디지털 콘텐츠를 사용할 수 있게 된다. 이러한 문제점을 해결하고자 DRM이라는 개념이 도입되었다. DRM은 어떤 암호화된 디지털 콘텐츠에 대한 접근은 누구에게나 무제한으로 허용하고 있으나, 암호화된 디지털 콘텐츠를 복호화하여 재생시키려면 권리객체(Rights Object)라는 라이센스를 필요하도록 하고 있다. 따라서, DRM을 적용하면 디지털 콘텐츠를 기존과는 달리 효과적으로 보호할 수 있게 된다.

[0013] DRM의 개념은 도 1을 통해 설명한다. DRM은 암호화 또는 스크램블과 같은 방식으로 보호된 콘텐츠(이하에서는 암호화된 콘텐츠로 언급한다)와 보호된 콘텐츠에 접근할 수 있도록 하는 권리객체들을 어떻게 취급할 것인지에 대한 것이다.

[0014] 도 1을 참조하면, DRM에 의해 보호되는 콘텐츠에 접근하기를 원하는 사용자들(110, 150)과 콘텐츠를 공급하는 콘텐츠 공급자(Contents Issuer)(120)와 콘텐츠에 대한 접근할 수 있는 권리를 포함하고 있는 권리객체를 발행하는 권리객체 발행기관(Rights Issuer)(130), 및 인증서를 발행하는 인증기관(140)이 도시된다.

[0015] 동작을 살펴보면, 사용자A(110)는 원하는 콘텐츠를 콘텐츠 공급자(120)로부터 얻을 수 있는데, DRM으로 보호된 암호화된 콘텐츠를 얻는다. 사용자A(110)는 암호화된 콘텐츠를 재생시킬 수 있는 라이센스는 권리객체 발행기관(130)으로부터 받은 권리객체로부터 얻을 수 있다. 권리객체가 있는 사용자A(110)는 암호화된 콘텐츠를 재생시킬 수 있게 된다. 한번 암호화된 콘텐츠를 자유롭게 유통시키거나 배포할 수 있기 때문에, 사용자A(110)는 사용자B(150)에게 암호화된 콘텐츠를 자유롭게 전달할 수 있다. 사용자B(150)는 전달받은 암호화된 콘텐츠를 재생시키기 위해서는 권리객체를 필요로 하게 되는데, 이러한 권리객체는 권리객체 발행기관(130)으로부터 얻을 수 있다. 한편, 인증기관(Certification Authority)은 콘텐츠 공급자(120)와 사용자A(110) 및 사용자B(150)가 정당한 사용자임을 나타내는 인증서(Certificate)를 발행한다. 인증서는 사용자들(110, 150)의 디바이스를 제작할 때부터 디바이스내에 넣을 수 있으나, 인증서의 유효기간이 만료된 경우에 인증기관(140)으로부터 인증서를 재발급받을 수 있다.

[0016] 이와 같이 DRM은 디지털 콘텐츠를 제작하거나 공급하는 자들의 이익을 보호하여 디지털 콘텐츠 산업을 활성화시키는데 도움이 될 수 있다. 그렇지만 도시된 바와 같이 모바일 디바이스를 사용하는 사용자A(110)와 사용자B(150) 사이에서 권리객체나 암호화된 콘텐츠를 교환하는 것은 가능하지만 현실적으로 불편한 감이 없지 않다. 디바이스들간의 권리객체 또는 암호화된 콘텐츠의 이동을 편리하게 할 필요가 있는데, 휴대형 저장장치를 사용하는 경우에 디바이스들간의 권리객체와 암호화된 콘텐츠의 이동을 편리하게 할 수 있다. 즉, 휴대형 저장장치에 권리객체를 두고 디바이스는 이를 이용하여 DRM으로 보호된 콘텐츠에 접근할 수 있게 하는 방법이 필요하다.

발명이 이루고자 하는 기술적 과제

[0017] 본 발명의 목적은 휴대형 저장장치를 이용하여 디바이스가 DRM으로 보호되는 콘텐츠를 재생(Playback)할 수 있도록 하기 위한 휴대형 저장장치와 디바이스간의 동작방법과, 이러한 동작을 하는 휴대형 저장장치와 디바이스를 제공하는 것이다.

[0018] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해되어질 수 있을 것이다.

발명의 구성 및 작용

[0019] 상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 휴대형 저장장치를 이용한 콘텐츠 재생방법은 DRM으로 보호되는 휴대형 저장장치에 콘텐츠에 대한 재생권리의 전송을 요청하는 단계와, 상기 휴대형 저장장치로부터 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리를 수신하는 단계, 및 상기 재생권리를 이용한 상기 DRM으로 보호되는 콘텐츠의 재생이 완료되면 재생이 완료되었음을 상기 휴대형 저장장치에 알리는 단계를 포함한다.

[0020] 상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 디바이스에 콘텐츠 재생권리를 보내는 방법은 디바이스로부터 DRM으로 보호되는 콘텐츠에 대한 재생권리의 전송을 요청받는 단계와, 상기 요청에 따라 상기 디바이스에 상기 DRM으로 보호되는 콘텐츠에 대한 재생권리를 전송하는 단계, 및 상기 DRM으로 보호되는 콘텐츠에 대한 권리객체의 업데이트 명령을 수신하는 단계를 포함한다.

[0021] 상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 휴대형 저장장치는 디바이스와의 연결을 위한 인터페이스와, 적어도 하나 이상의 암호화된 권리객체들을 저장하고 있는 권리객체 저장모듈와, 세션키 생성과 대칭키 방식의 암호화와 공개키 방식의 암호화를 수행하는 암호화 모듈, 및 DRM 동작을 수행하는 DRM 에이전트 모듈을 포함하며, 상기 DRM 에이전트 모듈은 상기 인터페이스를 통해 디바이스로부터 특정 콘텐츠에 대한 재생권리를 전송을 요청받으면 상기 권리객체 저장모듈에 저장된 권리객체들 중에서 상기 콘텐츠에 대한 권리객체를 찾고, 상기 권리객체에 포함된 상기 콘텐츠를 재생하는데 필요한 정보를 상기 암호화 모듈을 이용하여 암호화하고 상기 인터페이스를 통해 상기 디바이스에 보내도록 하는 과정을 수행한다.

[0022] 상기 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 콘텐츠 재생장치는 휴대형 저장장치와 연결을 위한

인터페이스와, DRM으로 보호되는 적어도 하나 이상의 콘텐츠를 저장하고 있는 콘텐츠 저장모듈와, 세션키 생성과 대칭키 방식의 암호화와 공개키 방식의 암호화를 수행하는 암호화 모듈, 및 DRM 동작을 수행하는 DRM 에이전트 모듈을 포함하며, 상기 DRM 에이전트 모듈은 상기 인터페이스를 통해 상기 콘텐츠 저장모듈에 저장된 DRM으로 보호되는 어느 한 콘텐츠에 대한 재생권리를 상기 휴대형 저장장치에게 요청하고, 상기 휴대형 저장장치로부터 암호화된 재생권리를 수신하고, 상기 암호화 모듈을 이용하여 상기 수신된 암호화된 재생권리를 복호화하고, 콘텐츠 암호화 키를 얻는 휴대형 저장장치를 이용한다.

[0023] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다.

[0024] 설명에 앞서 본 명세서에서 사용하는 용어의 의미를 간략히 설명한다. 그렇지만 용어의 설명의 본 명세서의 이해를 돕기 위한 것으로서 명시적으로 본 발명을 한정하는 사항으로 기재하지 않은 경우에 본 발명의 기술적 사상을 한정하는 의미로 사용하는 것이 아님을 주의해야 한다.

[0025] -공개키 암호화(Public-key Cryptography)

[0026] 비대칭 암호화라고도 하며, 이는 데이터를 복호화하는데 사용된 키가 데이터를 암호화한 키와 서로 다른 암호화를 의미한다. 공개키라고도 불리는 암호화키는 비밀로 보관될 필요가 없으므로 암호화키를 안전하지 않은 일반 채널을 통해 교환할 수 있다. 이러한 공개키 암호화 알고리즘은 일반에게 공개되어 있으며, 공개키 암호화는 제3자가 암호화 알고리즘과 암호화키 및 암호화된 문장을 가지고 원문을 알 수 없거나 알기 매우 힘든 특성을 갖는다. 공개키 암호화 시스템의 예로는 Diffie-Hellman 암호시스템, RSA 암호시스템, ElGamal 암호시스템, 및 타원곡선(Elliptic Curve) 암호화 시스템 등이 있다. 공개키 암호화의 경우에 대칭키 암호화보다 약 100~1000배 정도 느리기 때문에 콘텐츠 자체를 암호화하는데 사용되기 보다는 키교환이나 전자서명 등에 사용된다.

[0027] -대칭키 암호화(Symetric-key Criptography)

[0028] 비밀키 암호화라고도 하며, 이는 데이터를 암호화하는데 사용된 키와 데이터를 복호화하는데 사용한 키가 동일한 암호화를 의미한다. 이러한 대칭키 암호화의 예로는 DES가 가장 일반적으로 사용되고 있으며, 최근에는 AES를 채용한 어플리케이션이 증가하고 있다.

[0029] -인증서(Certificate)

[0030] 인증기관(Certification Authority)라는 공인된 기관에서 공개키 암호와 관련하여 사용자들에게 공개키를 인증한 것을 말하며, 인증서는 특정 가입자의 신원과 공개키를 인증기관의 개인키로 서명한 메시지를 의미한다. 따라서, 인증기관의 공개키를 인증서에 적용하면 그 인증서의 무결성을 쉽게 파악할 수 있기 때문에 공격자가 특정 사용자의 공개키를 임의로 변조하는 것을 막아준다.

[0031] -전자서명(Digital Signature)

[0032] 서명자에 의해 문서가 작성되었음을 나타내기 위하여 생성하는 것을 말한다. 이러한 전자서명의 예로는 RSA 전자서명, ElGamal 전자서명, DSA 전자서명, Schnorr 전자서명 등이 있다. RSA 전자서명의 경우에 암호화된 메시지 송신자는 메시지를 자신의 개인키로 암호화하여 송신하고, 수신자는 송신자의 공개키로 암호화된 메시지를 복호화한다. 이러한 경우에 메시지의 암호화는 송신자에 의한 것이라는 것이 증명된다.

[0033] -난수

[0034] 임의성을 갖는 숫자 또는 문자열을 의미하며, 실제로 완전한 랜덤 넘버를 생성하는 것은 고비용을 필요로 하기 때문에 의사랜덤(Pseudo-Random) 번호가 사용되기도 한다.

[0035] -휴대형 저장장치

[0036] 본 발명에서 사용하는 휴대형 저장장치는 플래시 메모리와 같은 읽고 쓰고 지울 수 있는 성질을 갖는 비휘발성 메모리를 포함하고 있으며, 디바이스에 연결이 가능한 저장장치를 의미한다. 이러한 저장장치의 예로는 스마트 미디어, 메모리 스틱, CF카드, XD카드, 멀티미디어카드 등이 있으며, 이하 상세한 설명에서는 멀티미디어카드를 중심으로 설명한다.

[0037] -DRM 에이전트

[0038] 디바이스나 보안 멀티미디어카드 안에서 디바이스의 미디어 객체들을 위한 허가들을 관리하는 엔터티를 말한다.

[0039] 도 2는 본 발명의 일 실시예에 따른 디지털 저작권의 개념을 간략히 설명하는 도면이다.

[0040] 사용자A(210)는 콘텐츠 공급자(220)로부터 암호화된 콘텐츠를 얻을 수 있다. 암호화된 콘텐츠란 DRM으로 보호되는 콘텐츠를 의미하는데, 이를 재생시키기 위해서는 콘텐츠에 대한 권리객체를 필요로 한다. 권리객체란 콘텐츠에 대한 권리에 대한 정의와 한정사항(constraint)을 포함하고 있으며, 권리객체 자신에 대한 권리도 포함하고 있다. 콘텐츠에 대한 권리의 예로는 재생이 될 수 있고, 한정사항의 예로는 재생 횟수, 재생 시간, 재생 기간 등이 될 수 있다. 이 밖에 도 2에 표시되지는 않았으나 권리객체 자신에 대한 권리 중에는 이동이나, 복사 등이 있을 수 있다.

[0041] 암호화된 콘텐츠를 얻은 사용자A(210)는 이에 대한 재생권한을 얻기 위하여 권리객체 발행기관(230)에 권리객체 요청을 한다. 권리객체 발행기관(230)으로부터 권리객체 응답과 함께 권리객체를 받으면 이를 이용하여 암호화된 콘텐츠를 재생시킬 수 있게 된다. 한편, 해당 암호화된 객체를 갖고 있는 사용자B(250)에게 권리객체를 전달하려고 할 때 사용자A(210)는 휴대형 저장장치를 사용하여 전달할 수 있다. 일 실시예로 휴대형 저장장치는 DRM기능을 갖는 보안 멀티미디어카드(260)가 될 수 있는데, 이러한 경우에 사용자A(210)는 보안 멀티미디어카드(260)와 상호인증(Authentication)을 한 후에 권리객체를 보안 멀티미디어카드(260)로 이동시킨다. 사용자A(210)가 암호화된 콘텐츠를 재생시키려면 보안 멀티미디어카드(260)에 재생권리를 요구한 후에 보안 멀티미디어카드(260)로부터 재생권리(콘텐츠 암호화 키)를 받아 암호화된 콘텐츠를 재생시킬 수 있다. 한편, 보안 멀티미디어카드(260)는 사용자B(250)와 인증(Authentication)을 거친 후에 사용자B(250)에게 암호화된 콘텐츠를 재생시킬 수 있도록 한다. 이러한 경우에 보안 멀티미디어카드(260)와 사용자B(250) 사이에는 상호인증이 있어야 한다. 보안 멀티미디어카드(260)에 저장된 권리객체를 이용하여 사용자들(210, 250)이 DRM으로 보호되는 콘텐츠를 재생시키는 과정에 대해서는 도 3을 통해 상술한다.

[0042] 도 3은 본 발명의 일 실시예에 따른 콘텐츠 재생과정을 보여주는 도면이다. 도 3에서 SC.Encrypt(K_{SEK}, A)는 A라는 값을 K_{SEK}으로 대칭키 방식으로 암호화한 것을 의미한다. AppendInfo는 데이터의 길이가 가변적일 수 있을 경우에 뒤에 나오는 데이터에 대한 정보(예를 들면, 데이터 필드의 개수나 길이 등)를 나타낸다.

[0043] 디바이스(310)가 보안 멀티미디어카드(320)에 저장된 권리객체를 이용하여 암호화된 콘텐츠를 재생시킬 수 있다. 권리객체는 디바이스(310) 또는 다른 디바이스로부터 얻을 수도 있고, 제조사에서 보안 멀티미디어카드(320)를 제작할 때 권리객체를 갖도록 제작할 수도 있다.

[0044] 먼저 암호화된 콘텐츠를 재생하기 위해서는 디바이스(310)와 보안 멀티미디어카드(320)는 서로 상호인증을 해야 한다(S300). 상호인증은 상대방의 인증서(Certificate)를 받아 인증서 확인을 통해 상대방이 정당한 장치(또는 프로그램)인지 여부를 판별할 수 있다. 예를 들면 보안 멀티미디어카드(320)는 디바이스(310)로부터 디바이스 인증서($Cert_H$)를 받아 디바이스가 정당한 장치(또는 프로그램)이라는 것을 확인할 수 있고, 디바이스 공개키($PuKey_H$)를 얻을 수 있다. 마찬가지로 디바이스(310)는 보안 멀티미디어카드(320)로부터 보안 멀티미디어카드 인증서($Cert_S$)을 받아 보안 멀티미디어카드가 정당한 장치(또는 프로그램)이라는 것을 확인할 수 있고, 보안 멀티미디어카드 공개키($PuKey_S$)를 얻을 수 있다.

[0045] 인증과정에서 디바이스와 보안 멀티미디어카드 중 어느 하나가 난수를 생성하여 상대방의 공개키로 암호화한 후에 전송하고 이를 세션키(K_{SEK})로 이용할 수 있다. 예를 들면, 디바이스(310)가 난수$_H$를 생성하고 이를 보안 멀티미디어카드 공개키($PuKey_S$)로 암호화한 후에 보안 멀티미디어카드(320)에게 전송한다. 보안 멀티미디어카드(320)는 암호화된 난수$_H$를 보안 멀티미디어카드 공개키($PuKey_S$)에 대응되는 보안 멀티미디어카드 개인 키($PrKey_S$)로 복호화하여 난수$_H$를 얻는다. 양자는 난수$_H$를 세션키(K_{SEK})로 사용할 수 있다.

[0046] 바람직하게는 임의성을 높이기 위해 양자 모두 난수를 생성하여 서로 교환한다. 즉, 상호인증을 통해 디바이스(310)와 보안 멀티미디어카드(320)는 난수$_H$와 난수$_S$을 갖게 된다. 두 난수들을 이용하여 디바이스(310)와 보안 멀티미디어카드(320)는 동일한 세션키(K_{SEK})를 생성한다. 두 난수들을 이용하여 세션키(K_{SEK})를 생성하는 알고리즘은 공개된 알고리즘을 사용할 수 있다.

[0047] 상호인증 과정(S300)을 통해 디바이스(310)와 보안 멀티미디어카드(320)는 세션키(K_{SEK})를 공유하게 되고, 디바이스(310)는 보안 멀티미디어카드(320)의 권리객체를 이용하여 DRM으로 보호되는 콘텐츠를 재생할 수 있다. 한편, 본 발명의 실시예들은 보다 보안성이 우수한 DRM을 위해 전송 시퀀스 카운터(Send Sequence Counter; 이하, SSC라 함)를 사용한다. SSC는 APDU(Application Protocol Data Unit)에 포함되며 APDU가 전송될 때마다 증가

한다. 예를 들면 따라서, 만일 하나 또는 복수의 APDU를 중간에 누군가가 가로챈다면 APDU에 포함된 SSC의 불연속이 발생한다. 또한 누군가가 APDU를 삽입할 경우라도 SSC의 불연속이 발생한다. 이를 좀더 자세히 살펴보면 다음과 같다.

[0048] 디바이스(310)와 보안 멀티미디어카드(320)는 상호인증(S300) 후에 얻은 난수$_H$와 난수$_S$를 조합한 숫자로 SSC를 초기화할 수 있다. 예를 들면 SSC의 크기가 총 2바이트인 경우에 난수$_H$와 난수$_S$의 뒷자리 1바이트씩 결합하여 SSC를 초기화한다. 예를 들면 난수$_H$와 난수$_S$의 맨 뒷자리가 각각 "01010101"와 "11111110"로 끝나는 경우에 SSC는 "0101010111111110"로 초기화한다. SSC의 초기화 값을 난수$_H$와 난수$_S$를 이용하여 얻으므로써 "0000000000000000"으로 초기화한 경우보다 임의성을 높일 수 있고, 따라서 보다 안전한 DRM 과정이 가능하게 된다.

[0049] 디바이스(310)가 보안 멀티미디어카드(320)에 DRM 명령을 할 경우에 APDU에 SSC를 포함시킨다. 만일 DRM 명령에 모두 10개의 APDU가 전송된다면 SSC는 초기값인 "0101010111111110"부터 APDU마다 1씩 증가한다. 그리고 나서 보안 멀티미디어카드(310)는 SSC를 체크하여 정당하지 않은 APDU가 중간에 삽입되거나 원래의 APDU를 누군가 가로챘는지 여부를 판단한다.

[0050] 보안 멀티미디어카드(320)가 디바이스(310)에 DRM 명령을 할 경우에도 APDU에 SSC를 포함시킨다(S140). 일 실시예에 있어서, SSC의 초기 값은 최초에 초기화된 초기값을 사용한다. 예를 들면, DRM 명령에 모두 10개의 APDU가 전송된다면 SSC는 초기값인 "0101010111111110"부터 APDU마다 1씩 증가한다. 다른 실시예에 있어서, SSC의 초기 값은 최종 SSC값을 기준으로 한다. 예를 들면 최종 SSC값이 "1000000000000000"인 경우에 그 다음 APDU의 SSC값은 "1000000000000001"부터 시작한다. 그리고 나서 디바이스(S110)는 SSC를 체크하여 정당하지 않은 APDU가 중간에 삽입되거나 원래의 APDU를 누군가 가로챘는지 여부를 판단한다.

[0051] SSC를 순차적으로 증가시키는 것은 예시적인 것으로서, SSC를 초기값에서부터 순차적으로 감소시키는 경우나 SSC의 증가 또는 감소의 폭이 1이 아닌 경우와 같은 경우도 본 발명의 기술적 사상에 포함되는 것으로 해석해야 한다.

[0052] 이하 본 발명에 따르는 각 실시예에서 특별한 언급이 없더라도 전송하려는 데이터와 전술한 SSC 값이 암호화되어 디바이스와 보안 멀티미디어카드 사이에 전송되는 APDU에 포함될 수 있다.

[0053] DRM으로 보호되는 콘텐츠 재생과정은 S310 내지 S360을 통해 이루어진다.

[0054] 먼저, 디바이스(310)는 재생권리 준비를 요청한다(S310). 디바이스(310)가 SET_PLAYBACK_REQ APDU(Application Protocol Data Unit)를 보안 멀티미디어 카드(320)로 전송하는 것으로 콘텐츠 재생권리 준비를 요청을 할 수 있다. 본 발명의 실시예에 있어서, 요청하는 재생권리는 권리객체(Right Object) 자체가 아니고, DRM으로 보호되는 콘텐츠를 재생시키는데 필요한 간략화된 객체를 의미한다.

[0055] SET_PLAYBACK_REQ APDU로 전송되는 정보는 콘텐츠 식별자(CID)와 iPermission와 디바이스(310)의 현재 시간(DateTime)이다. 콘텐츠 식별자(CID)는 재생을 원하는 콘텐츠를 가리키고, 현재 시간은 디바이스의 현재 시간을 정의한다. iPermission은 OMA DRM v2.0에 특정된 허가의 인덱스 플래그로서 1바이트의 크기를 갖고, 수출허가는 제외된다. 비트위치가 b0는 재생(Play) 허가를, b1은 디스플레이(Display) 허가를, b2는 실행(Execute) 허가를, b3는 프린트(Print) 허가를 표시하며 b4~b7은 사용하지 않고 예약되어 있다. 각 허가비트는 1일 경우에 설정되고 0인 경우에 설정되지 않는 것으로 표시하며, 복수의 허가들을 동시에 요청할 수도 있다. 이 밖에 서브스크립션 비즈니스 모델에서, 디바이스(310)에 부모 권리객체가 없고 자식 권리객체만 있다면 부모 권리객체 식별자(PID)를 포함하여 보안 멀티미디어카드(320)의 대응되는 부모 권리객체를 찾을 수 있도록 한다.

[0056] 그리고 나서, 디바이스(310)는 보안 멀티미디어카드(320)에게 재생권리 전송을 요구한다(S320). 디바이스(310)가 GET_PLAYBACK_REP APDU를 보안 멀티미디어카드(320)에 보냄으로써 재생권리 전송을 요구할 수 있다. GET_PLAYBACK_REP APDU를 수신한 보안 멀티미디어 카드(320)는 재생권리 준비 요청 단계(S310)에서 지정된 콘텐츠 식별에 해당하는 권리객체가 복수개 있을 때 요청된 재생권리들을 모두 디바이스(310)로 전송한다. 재생권리는 허가 정보(Permission Information)의 형태로 전송되며, 허가 정보 전송 형식은 도 5 내지 도 7을 통해 후술한다.

[0057] 디바이스(310)는 GET_PLAYBACK_REP APDU에 대한 보안 멀티미디어카드(320)의 응답을 받은 후 디바이스측 또는 보안 멀티미디어측의 권리들을 선택한다. 이는 권리객체가 보안 멀티미디어카드나 디바이스 어느 곳에 있을 수도 있고 양자에 모두 있을 수도 있기 때문이다. 만일 디바이스(310)가 보안 멀티미디어카드(320)의 권리객체를

사용하지 않고 자신이 갖고 있는 권리객체를 사용하고자 하는 경우라면 재생 종료 설정을 보안 멀티미디어카드(320)에 알린다(S330). 이를 위해 디바이스(310)는 SET_PLAYBACK_FINISH APDU를 보안 멀티미디어카드(320)로 보낸다.

[0058] 디바이스(310)가 보안 멀티미디어카드(320)의 권리객체를 사용하는 경우라면 권리객체 업데이트 명령을 한다(S340). 디바이스(310)는 SET_UPDATE_RO APDU를 보안 멀티미디어카드(320)에 보냄으로써 권리객체 업데이트 명령은 전달할 수 있다. 이 APDU에는 세가지 다른 데이터 필드를 중 하나를 가질 수 있는데, 각 데이터 필드는 iPermConst 파라미터에 특정된다. iPermConst는 총 8바이트로 구성하며, 재생과 디스플레이와 실행 및 프린트에 각 한 바이트씩 할당되고 4바이트의 예약 바이트를 두어 미래의 사용을 위해 남겨둔다. 각 바이트를 구성하는 비트의 의미는 b0는 횟수(count)를, b1은 시간-횟수(timed count)를, b2는 Datetime을, b3는 Interval을, b4는 Accumulate를 의미하고, 비트값으로 1은 설정을 의미하고 0은 설정되지 않은 것을 의미한다. 그리고 b5 내지 b7은 유보된 비트이다.

[0059] 만일 권리객체에서 데이트타임(datetime)이나 간격(interval)과 같은 한정사항이 소비되는 경우에는 "DateTime" 파라미터가 필요하다. 시간-횟수 한정사항(timed-count constraint)를 소비하는 경우에 디바이스(310)는 시간 횟수 엘리먼트에 특정된 시간이 지난 후에 이 APDU를 전송한다. 한편, 간격 한정사항이 사용되는 경우에 보안 멀티미디어카드(320)는 이 APDU를 수신한 후에 간격 한정사항을 현재시간 한정사항으로 논리적으로 변환시킨다.

[0060] 만일 권리객체에서 횟수(count) 또는 시간 횟수 한정 사항과 같은 것을 소비되는 경우에, 데이터 필드는 "count" 파라미터가 필요하다. 횟수 파라미터는 1을 기본값으로 한다. 일 실시예에 있어서, 횟수 한정사항을 다시 소비해야할 경우라면 디바이스(310)는 SET_UPDATA_RO 명령을 다시 보내기만 하면 된다. 이러한 경우에 S310 및 S320의 과정을 거치지 않으므로 디바이스(310)와 보안 멀티미디어카드(320)간의 통신 오버헤드를 줄일 수 있다.

[0061] 만일 권리객체에서 총 시간(accumulate time) 한정사항을 소비되는 경우에, "time" 필드가 필요하다. Time 파라미터는 10초를 기본값으로 한다. Time 파라미터에 설정된 기간에 따라 디바이스(310)는 주기적으로 SET_UPDATA_RO APDU를 전송한다. 예를 들면 time 파라미터를 60초로 설정한 경우에, 디바이스(310)는 콘텐츠를 재생중에 60초마다 SET_UPDATA_RO APDU를 보안 멀티미디어카드(320)에 전송하여 권리객체가 업데이트될 수 있도록 한다.

[0062] 재생이 끝나고 나면, 디바이스(310)는 재생이 완료되었음을 알린다(S350). 디바이스(310)는 보안 멀티미디어카드(320)에 SET_PLAYBACK_FINAL APDU를 전송함으로써 재생이 완료됨을 알릴 수 있다. 이 APDU는 권리객체의 사용총계의 무결성을 체크하기 위한 정보를 포함하며, 재생 기능이 완료됐다는 것을 알려준다. SMRAID는 권리객체 식별자와 자산 식별자를 포함하고, TCount는 총 횟수의 수를 의미하고 TTime은 총 시간을 의미한다.

[0063] 한편, 도 3에는 도시되어 있지 않지만, 본 발명의 실시예는 보안 멀티미디어카드(320)의 활성화 상태를 체크하는 과정을 포함한다. 이 과정은 주로 datatime 한정사항과 관계된 재생(playback) 절차를 위해 보안 멀티미디어카드(320)가 활성화 상태인지 여부를 체크한다. 일 실시예에 있어서, 디바이스(310)는 자신이 생성한 난수$_H$를 SET_CARD_STATUS 명령에 포함시켜 보안 멀티미디어카드(320)에 보낸다. 이를 수신한 보안 멀티미디어카드(320)는 디바이스(310)의 GET_CARD_STATUS 명령에 따라 자신이 생성한 난수$_S$와 난수$_H$를 함께 세션키(K_{SEK})로 암호화하여 전송한다. 예를 들면 "난수$_H$||SC.Encrypt(KSEK, 난수 $_H$||난수$_S$)" 형태로 전송할 수 있다. 디바이스(310)는 세션키(K_{SEK})로 이를 복호화함으로써 보안 멀티미디어카드(320)가 활성중인 것을 확인할 수 있다.

[0064] 도 4는 본 발명의 일 실시예에 따른 콘텐츠 재생에 사용되는 권리객체의 형식(Secure Multimedia card Right object Format; 이하 SMRF라 함)을 보여주는 도면이다.

[0065] SMRF는 크게 권리(Right) 필드(410)와, 자산(Asset) 필드(430)와, 허가(Permission) 필드(450)의 세 필드로 구성되며, 여러 자산(Asset) 필드와 허가(Permission) 필드를 가질 수 있다. 따라서, 자산의 개수(Number of asset) 필드(420)는 자산 필드의 개수를 나타내고, 허가의 개수(Number of permission) 필드(440)는 허가 필드의 개수를 나타낸다.

[0066] 권리 필드(410)는 권리객체의 버전 정보(412) 및 권리객체의 식별자 정보(414)를 포함한다. 자산 필드(430)는 권리객체에 의해 그 소비가 지배되는 콘텐츠 데이터에 대한 정보를 포함하며, 허가 필드(450)는 보호되는 콘텐츠 데이터에 대하여 권리객체 발행자(Rights Issuer)에 의해 허용되는 실제 용도나 활동에 관한 정보를 포함한다.

[0067] 자산 필드(430)는 자산을 유일하게 식별하는 자산 식별자(431), 콘텐츠 식별자(또는 부모 권리객체 식별자)(432), 부모 권리객체 식별자의 참조(433), 메시지 개요 인덱스(Message Digest Index) + 메시지 개요 값(Message Digest Value)(434) 및 콘텐츠 암호화 키(Content Encryption Key; 이하 CEK라 함)(435)로 구성된다. 하나의 권리객체는 복수의 자산을 가질 수 있으므로 이러한 경우에 자산의 개수 필드(420)가 자산 필드(430)들의 개수를 표시한다.

[0068] 권리객체가 부모 권리객체(Parent Right Object)인 경우 콘텐츠 식별자 대신 부모 권리객체 식별자(432)를 포함하고, 권리객체가 자식 권리객체(Child Right Object)인 경우 부모 권리객체 식별자에 대한 참조 필드(433)를 포함한다.

[0069] 여기서, 부모 권리객체(Parent Right Object) 및 자식 권리객체(Child Right Object)란 하나의 권리객체로부터 허가와 한정사항을 물려받아(Inherit) 다른 권리객체를 정의하는 개념으로, 부모 권리객체는 DRM 콘텐츠를 위한 허가 및 한정사항을 정의하고 자식 권리객체는 이를 물려받을 수 있다. 자식 권리객체는 콘텐츠를 참조하지만, 부모 권리객체는 콘텐츠 자체를 직접 참조하지 않고 그의 자식 권리객체가 참조한다. 자식 또는 부모 권리객체 내의 허가에 따라 콘텐츠에의 접근이 허용되는 경우, DRM 에이전트는 접근을 부여한 허가의 한정사항뿐만 아니라 부모 및 자식 권리객체의 모든 상위 레벨 한정사항을 적용한다. 이를 통해 권리객체 발행자는 서브스크립션 비즈니스 모델(Subscription business model)을 지원할 수 있다.

[0070] 메시지 개요 인덱스(Message Digest Index) 및 메시지 개요 값(Message Digest Value)(434)은 콘텐츠에 대한 참조의 무결성 보호(Integrity Protection)를 위한 값이다. 메시지 개요 값은 공개된 해쉬 알고리즘, 예를 들면 보안 해쉬 알고리즘1(Security Hash Algoritm1; 이하 SHA1이라 함)에 의해 생성된 값이고, 메시지 개요 인덱스는 메시지 개요 값을 생성하는데 사용된 해쉬 알고리즘의 종류를 나타낸다.

[0071] CEK 필드(435)는 콘텐츠를 암호화하기 위해 사용되는 이진 키 값을 저장한다. CEK는 디바이스가 이용하고자 하는 암호화된 콘텐츠를 복호화하는 키 값으로 디바이스는 보안 멀티미디어카드로부터 이 CEK 값을 전송받음으로써 콘텐츠를 이용할 수 있다.

[0072] 하나의 권리객체는 여러 개의 허가를 가질 수 있으므로 허가의 개수 필드(440)는 허가 필드(450)의 개수가 몇 개인지를 표시한다. 허가 필드(450)는 자산 식별자의 참조의 개수(452), 자산 식별자의 참조(454), 허가정보의 개수(456), 허가정보(458)로 구성된다.

[0073] 하나 이상의 자산 식별자의 참조(454)가 허가정보 필드(458) 전에 올 수 있다. 자산 식별자의 참조는 자산 식별자(431)를 참조한다.

[0074] 권리객체는 최대 7개의 허가, 즉 재생(Play), 디스플레이(Display), 실행(Execute), 인쇄(Print), 수출(Export), 복사(Copy), 이동(Move) 허가를 가질 수 있다. 재생(Play) 허가는 DRM 콘텐츠를 오디오/비디오 형태로 표현하는 권리를 의미한다. 따라서 DRM 에이전트는 이런 방법으로 표현될 수 없는 콘텐츠, 예를 들면 자바 게임 등에 재생에 따른 접속을 부여하지 않는다.

[0075] 재생 허가는 한정사항(Constraint)을 선택적으로 가질 수 있다. 한정사항이 특정되어 있다면 DRM 에이전트는 해당 한정사항에 따라 재생 권리를 부여하고, 어떠한 한정사항도 특정되어 있지 않다면 DRM 에이전트는 무제한의 재생 권리를 부여한다.

[0076] 디스플레이(Display) 허가는 DRM 콘텐츠를 시각 장치에 표현할 수 있는 권리를 의미한다. 따라서 DRM 에이전트는 gif 또는 jpeg 이미지와 같이 시각 장치를 통해 표현될 수 없는 형식의 콘텐츠에 대하여 디스플레이에 따른 접근을 부여하지 않는다.

[0077] 실행(Execute) 허가는 자바게임 또는 다른 응용프로그램과 같은 DRM 콘텐츠를 실행하는 권리를 의미하고, 인쇄(Print) 허가는 jpeg등의 이미지와 같은 DRM 콘텐츠의 하드카피를 생성할 수 있는 권리를 의미한다.

[0078] 수출(Export) 허가는 DRM 콘텐츠와 상응하는 권리객체들을 OMA DRM 시스템이 아닌 다른 DRM 시스템 또는 콘텐츠 보호 구조로 내보내는 권리를 의미한다. 수출 허가는 한정요소를 필수적으로 갖는다. 한정 요소는 어떤 DRM 시스템 또는 콘텐츠 보호 구조로 DRM 콘텐츠 및 권리객체를 내보낼 수 있는지를 특정한다. 수출 허가에는 이동(Move)과 복사(Copy)의 두가지 모드가 있다. 이동(Move)의 경우 다른 시스템으로 권리객체를 수출하는 경우 현재의 DRM 시스템내의 권리객체를 비활성화하나, 복사(Copy)의 경우 현재의 DRM 시스템내의 권리객체를 비활성화하지 않는다.

[0079] 이동(Move) 허가는 디바이스에서 보안 멀티미디어카드로의 이동과 보안 멀티미디어카드에서 디바이스로의 이동

의 두 가지가 있다. 디바이스에서 보안 멀티미디어카드로의 이동은 디바이스에 있는 권리객체를 보안 멀티미디어카드로 전송하고 디바이스에 있던 원래의 권리객체를 비활성화 시킨다. 보안 멀티미디어카드에서 디바이스로의 이동도 이와 유사하다.

[0080] 복사(Copy) 허가도 디바이스에서 보안 멀티미디어카드로의 복사와 보안 멀티미디어카드에서 디바이스로의 복사의 두 가지가 있다. 디바이스에서 보안 멀티미디어카드로의 복사는 디바이스에 있는 권리객체를 보안 멀티미디어카드로 전송하지만 이동 허가와 달리 디바이스에 있던 원래의 권리객체를 비활성화 시키지 않는다. 보안 멀티미디어카드에서 디바이스로의 복사도 이와 유사하다.

[0081] 허가정보의 개수 필드(456)는 이러한 허가의 개수를 나타내며, 허가정보 필드(458)는 7가지의 허가를 위한 한정사항과 같은 허가에 관한 정보를 특정한다.

[0082] 허가정보 필드(458)는 허가 인덱스(461), 수출 인덱스(462), 한정사항의 개수(463), 한정사항 인덱스 + 한정사항 정보(464)의 필드로 구성된다. 허가 인덱스(461)는 허가의 종류를 나타내는 인덱스로 다음의 표1에 있는 값 중 하나를 갖는다.

표 1

[0083]

허가의 이름	허가 인덱스
전부(All)	0x00
재생(Play)	0x01
디스플레이(Display)	0x02
실행(Execute)	0x03
인쇄(Print)	0x04
수출(Export)	0x05
이동(Move)	0x06
복사(Copy)	0x07

[0084] 수출 인덱스 필드(462)는 허가 인덱스의 값이 수출일 때 사용되는 것으로 복사에 의한 수출과 이동에 의한 수출을 구분하기 위한 인덱스 값이다.

[0085] 각 허가 정보 필드(458)는 다음의 한정사항 중 일부 또는 전부에 관한 정보를 갖는다. 한정사항은 디지털 콘텐츠에 대한 소비를 제한하는 정보로, 한정사항의 종류는 표 2와 같다. 한정사항 인덱스 필드(464)가 표 2에 있는 값 중 하나의 값을 가짐으로써 한정사항의 종류를 나타낸다.

표 2

[0086]

한정사항의 이름	한정사항 인덱스
None	0x00
Count	0x01
Time Count	0x02
Interval	0x03
Accumulated	0x04
Datetime	0x05
Individual	0x06
System	0x07

[0087] 한정사항 인덱스 필드(464)의 값에 따라 한정사항 정보 필드가 갖는 정보의 형식이 달라질 수 있다.

[0088] Count 한정은 횟수 필드를 한정 사항 정보로 하며, 횟수 필드에 기록된 값은 콘텐츠에 부여되는 허가의 횟수를 특정한다. Time count 한정은 횟수 및 타이머 필드를 한정 사항 정보로 하며, 타이머에 의해 한정되는 시간동안 콘텐츠에 부여되는 허가의 횟수를 특정한다.

[0089] Interval 한정은 시간 필드를 한정 사항 정보로 하며, 권리가 DRM 콘텐츠에 대하여 수행될 수 있는 시간의 구간을 특정한다. Accumulated 한정은 권리가 DRM 콘텐츠에 수행될 수 있는 측정된 사용 시간의 최대 구간을 특정한다. DRM 에이전트는 Accumulated 한정 값에 의해 특정된 누적 구간이 경과한 후에는 DRM 콘텐츠에 대한 접속을 허용하지 않는다. Datetime 한정은 두 개의 시간 필드를 한정 사항 정보로 하며, 허가에 대한 시간범위를

특정한다. 시작시간 또는 종료시간을 모두 갖거나 어느 하나를 선택적으로 가질 수 있다. 시작시간이 있으면 특정된 시간/날짜 이후, 종료시간이 있으면 특정된 시간/날짜 이전에 DRM 콘텐츠의 소비가 허용된다.

[0090] Individual 한정은 콘텐츠가 묶여 있는 개인을 특정한다. 즉, 콘텐츠가 묶여 있는 개인의 URI(Uniform Resource Identifier)를 이용하여 특정한다. 따라서 DRM 에이전트는 디바이스와 결합된 사용자 신원이 콘텐츠의 사용이 허용되어 있는 사용자의 신원과 일치하지 않으면 DRM 콘텐츠에 대한 접속을 허용하지 안는다. System 한정은 콘텐츠 및 권리객체가 수출될 수 있는 DRM 시스템 또는 콘텐츠 보호 구조를 특정한다.

[0091] 한편 상호인증을 마친 디바이스와 멀티미디어카드 사이에는 권리객체의 이동이나 복사등이 수행될 수 있으며, 이를 통해 멀티미디어카드도 권리객체를 저장할 수 있다. 멀티미디어카드에 권리객체가 저장된 경우 디바이스는 암호화된 콘텐츠를 재생시키기 위해 멀티미디어카드에게 재생 요청을 할 수 있다. 디바이스가 멀티미디어카드에 저장된 권리객체를 통해 콘텐츠를 재생시키는 경우 권리객체에 설정된 한정 정보등이 업데이트되어야 한다.

[0092] 휴대형 저장장치에 저장된 권리객체의 업데이트는 디바이스에서 이루어 질수 있으며, 종래의 기술에서는(예컨데 휴대형 저장장치가 SD 카드인 경우) 권리객체의 업데이트를 위해 권리객체 전체를 휴대형 저장장치에서 디바이스로 이동시기도 하였다. 권리객체의 업데이트시마다 권리객체 전체를 이동시키는 것은 디바이스와 휴대형 저장장치 사이의 통신에 오버헤드가 되므로, 본 발명 실시예에서는 권리객체의 업데이트시 권리객체를 식별하기 위한 기본 정보 및 권리객체의 허가 정보를 포함하는 데이터 형식을 이동시킬 수 있다.

[0093] 또한 본 발명에 따를 경우, 디바이스가 휴대형 저장장치에 저장된 권리객체의 허가 정보의 확인을 요청하는 경우에도 이러한 데이터 형식을 이동시킴으로써 디바이스와 휴대형 저장장치 사이의 통신에 오버헤드를 줄이고, 필요한 정보만을 신속히 전송시킬 수 있다.

[0094] 도 5 내지 도 7은 각각 본 발명의 실시예에 따른 현재 허가 상태 형식을 보여주는 도면이다.

[0095] 이와 같이 권리객체를 식별하기 위한 기본 정보 및 권리객체의 허가 정보를 포함하는 데이터 포맷을 이하 현재 허가 상태 형식(Current Permission Status Format; 이하, CPSF라 함)라 한다. 허가 상태 형식은 권리객체의 요청받은 모든 허가와 권리객체의 기본적인 정보를 특정한다. 본 발명의 실시예에서 권리객체를 직접적으로 전송하지 않고 이와 같이 CPSF로 전송하므로써 디바이스와 보안 멀티미디어카드 사이의 불필요한 오버헤드를 줄일 수 있다.

[0096] 본 발명의 실시예에 따른 CPSF는 콘텐츠 식별자 필드(510, 610, 710)와, 콘텐츠 암호화 키 필드(520, 620, 720)와, 메시지 개요 인덱스+ 메시지 개요값 콘텐츠 식별자 필드(530, 630, 730)와, 허가 정보 필드(540, 640, 740)을 포함한다.

[0097] 콘텐츠 식별자 필드(510, 610, 710)에는 권리객체를 통해 사용할 수 있는 특정 콘텐츠를 식별할 수 있는 콘텐츠 식별자가 설정된다.

[0098] 콘텐츠 암호화 키 필드(520, 620, 720)에는 암호화된 콘텐츠를 복호화시킬 수 있는 CEK 값이 설정된다. 디바이스는 CEK 값을 전송받음으로써 콘텐츠를 사용할 수 있게 된다.

[0099] 메시지 개요 인덱스+ 메시지 개요값 콘텐츠 식별자 필드(530, 630, 730)에는 메시지 개요 값이 설정되는데 이는 전송되는 데이터의 무결성 보호(Integrity Protection)를 위한 값이다. 메시지 개요 값은 공개된 해쉬 알고리즘(예컨데 보안 해쉬 알고리즘1(Security Hash Algorism1)에 의해 생성될 수 있다.

[0100] 허가 정보 필드(540, 640, 740)에는 권리객체가 지니고 있는 허가 정보가 설정될 수 있다.

[0101] 이러한 CPSF는 권리객체의 타입에 따라 그 내용이 달라질 수 있는데 본 발명의 실시예는 권리객체의 타입은 크게 일반 권리객체(general RO), 자식 권리객체(Child RO) 및 부모 권리객체(Parent RO)의 세가지로 구분한다. 타입 1은 일반 권리객체를, 타입 2는 자식 권리객체를, 타입 3은 부모 권리객체를 나타나낸다.

[0102] 일반 권리객체란 OMA DRM v2.0 REL에서 설명되고 있는 서브스크립션 모델(subscription model 혹은 subscription business model)과 관련이 없는 권리객체를 의미한다.

[0103] 한편 OMA DRM v2.0 REL에서 설명되고 있는 서브스크립션 모델에 해당하는 권리객체는 자식 권리객체와 부모 권리객체로 나뉠 수 있다. 자식 권리객체는 암호화된 콘텐츠의 사용 권한인 CEK를 포함하고 있고, 부모 권리객체는 허가 요소 및 허가 요소에 대한 한정 사항을 포함하고 있다. 기타 자식 권리객체 및 부모 권리객체에 대한 내용은 OMA DRM v2.0 REL에 상세히 설명되어 있다. 자세한 내용은 OMA DRM에 관한 보다 상세한 내용은

http://www.openmobilealliance.org/에서 얻을 수 있다.

[0104] 도 5은 본 발명의 일 실시예에 따른 일반 권리객체에 대한 CPSF의 구조를 나타낸 도면이다.

[0105] 일반 권리객체를 위한 CPSF 구조에는 도시된 바와 같이 하나 이상의 허가 정보 필드(540)가 포함될 수 있으며, 각 허가 정보 필드를 구성하는 서브 필드를 살펴보면 다음과 같다.

[0106] 먼저 타입 필드(541)에는 권리객체의 타입을 구별하기 위한 정보가 있으며, 각 권리객체 타입은 표 3에 도시된다.

표 3

[0107]

권리객체 유형	식별정보(1byte)
일반 권리객체	0x01
자식 권리객체	0x02
부모 권리객체	0x03

[0108] 권리객체 인덱스 필드(542) 및 자산 인덱스 필드(543)에는 각각 멀티미디어카드 상의 내부 권리객체 식별자 및 내부 자산 식별자가 설정된다. 이러한 내부 권리객체 식별자 및 내부 자산 식별자는 멀티미디어카드에 저장된 각 권리객체 및 자산을 식별하는데 사용될 수 있다.

[0109] 허가 인덱스 필드(544)에는 허가의 종류를 식별할 수 있는 식별 정보가 설정된다. 이러한 허가 인덱스는 앞서 살펴보았듯이 표 1에 표시되어 있다.

[0110] 한정사항의 개수 필드(545)에는 한정사항 정보의 개수가 설정되고, 한정사항 정보 필드(546)는 한정사항 인덱스 필드(547)와 한정사항 필드(548)가 포함된다. 이에 대한 내용은 도 4를 참조하여 앞서 살펴본 바와 같다.

[0111] 도 6은 본 발명의 일 실시예에 따른 자식 권리객체에 대한 CPSF 구조를 나타낸 도면이다.

[0112] 특정한 콘텐츠를 위해 사용될 수 있는 자식 권리객체는 하나 뿐이므로 도시된 CPSF는 하나의 허가정보 필드를 포함한다.

[0113] 도시된 CPSF에서 콘텐츠 식별자 필드(610), 콘텐츠 암호화 키 필드(620) 및 메시지 개요 인덱스+메시지 개요 값 필드(630)에 설정되는 내용은 앞서 살펴보았다.

[0114] 허가 정보 필드(640)의 서브 필드중 타입 필드(641)에는 권리객체의 유형을 식별하는 식별 정보가 포함되어 0x02 값을 갖는다.

[0115] 부모 권리객체 식별자 필드(642)에는 부모 권리객체의 식별 정보가 설정되며, 자식 권리객체 발행자 URL 필드(643)에는 자식 권리객체 발행자의 위치주소(Uniform Resource Location; URL)이 설정될 수 있다.

[0116] 도 7은 본 발명의 일 실시예에 따른 부모 권리객체에 대한 CPSF 구조를 나타낸 도면이다.

[0117] 콘텐츠 식별자 필드(710)는 앞서 설명한 바와 같다. 그러나 OMA DRM v2.0 REL의 서브스크립션 모델을 따르는 부모 권리객체는 콘텐츠 암호화 키 및 메시지 개요 값을 갖지 않으므로 콘텐츠 암호화 키 필드(720) 및 메시지 개요 인덱스 + 메시지 개요 값 필드(730)는 널(null) 값으로 설정될 수 있다.

[0118] 한편 특정 DRM 콘텐츠를 사용하도록 할 수 있는 부모 권리객체는 하나이므로 도시된 CPSF는 하나의 허가정보(740)를 포함할 수 있다.

[0119] 허가 정보 필드(740)의 서브 필드중 타입 필드는 부모 권리객체 식별자 필드(742)에는 부모 권리객체를 식별할 수 있는 식별자가 설정된다.

[0120] 그밖에 허가 인덱스 필드(744), 한정사항의 개수 필드(745) 및 한정사항 정보 필드(746)에 설정 되는 한정사항 인덱스 필드(747)와 한정 사항 필드(748)의 내용은 앞서 살펴본 바와 같다.

[0121] 한편 멀티미디어카드는 동일한 콘텐츠를 재생시킬 수 있는 일반 권리객체와 자식 권리객체를 동시에 저장하고 있고 있거나, 동일한 콘텐츠를 재생시킬 수 있는 일반 권리객체와 부모 권리객체를 동시에 저장하고 있을 수 있다.

[0122] 도 8은 본 발명의 일 실시예에 따른 보안 멀티미디어카드의 블록도이다.

[0123] 본 실시예에서 사용되는 "모듈"이라는 용어는 소프트웨어 또는 FPGA또는 ASIC과 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 모듈은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다. 구성요소들과 모듈들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다. 뿐만 아니라, 구성요소들 및 모듈들은 디바이스 또는 보안 멀티미디어카드 내의 하나 또는 그 이상의 CPU들을 재생시키도록 구현될 수도 있다.

[0124] 이러한 DRM 과정을 수행하기 위하여 보안 멀티미디어카드(800)는 보안기능과 콘텐츠 또는 권리객체를 저장하는 기능과 디바이스와의 데이터 교환을 하는 기능과 DRM 관리기능이 있어야 한다. 이를 위한 보안 멀티미디어카드(800)는 암호화 기능을 갖는 RSA 모듈(840)과 세션키 생성모듈(850)과 AES 모듈(860)을 포함하고 저장 기능을 갖는 권리객체 저장 모듈(830)을 포함하고 디바이스와의 데이터 교환이 가능하도록 하는 인터페이스(810)와 DRM 과정을 수행하기 위하여 각 구성모듈이 DRM 동작을 하도록 제어하는 DRM 에이전트 모듈(820)을 포함한다.

[0125] 인터페이스(810)는 보안 멀티미디어카드(800)가 디바이스와 연결될 수 있도록 한다. 기본적으로 보안 멀티미디어카드(800)가 디바이스와 연결된다는 것은 보안 멀티미디어카드와 디바이스의 인터페이스들이 서로 전기적으로 연결된 것을 의미하지만, 이는 예시적인 것으로서 "연결"이라는 의미는 비접촉 상태에서 무선매체를 통해 서로 통신할 수 있는 상태에 있다는 의미도 포함되는 것으로 해석해야 한다.

[0126] RSA 모듈(840)은 공개키 암호화를 수행하는 모듈로서 DRM 에이전트 모듈(820)의 요청에 따라 RSA 암호화를 수행한다.

[0127] 세션키 생성모듈(850)은 디바이스에게 전달할 난수를 생성하고 디바이스로부터 받은 난수와 자신이 생성한 난수를 이용하여 세션키를 생성한다. 세션키 생성모듈(850)에서 생성한 난수는 RSA 모듈을 통해 암호화되고 인터페이스(810)를 통해 디바이스에게 전달된다.

[0128] AES 모듈(860)은 대칭키 암화화를 수행하는 모듈로서 생성된 세션키를 사용하여 대칭키 암호화를 수행한다. 주로 권리객체로부터 콘텐츠 암호화 키를 받아 이를 세션키로 암호화하는데 사용하며, 이 밖에 디바이스와의 통신과정에서 중요한 정보를 암호화할 때 사용한다. AES 암호화 방식 또한 예시적인 것으로서, DES와 같이 다른 대칭키 암호화를 사용하는 것 또한 가능하다.

[0129] 권리객체 저장 모듈(830)은 권리객체들을 저장한다. 권리객체들은 앞서 살펴본 바와 같이 SMRF 형식으로 권리객체 저장 모듈에 저장되어 있다.

[0130] DRM 에이전트 모듈(820)은 앞서 설명한 구성요소들이 DRM 동작을 하도록 제어한다.

[0131] 도 9는 본 발명의 일 실시예에 따른 디바이스의 블록도이다.

[0132] 이러한 DRM 과정을 수행하기 위하여 디바이스(900)는 보안기능과 콘텐츠 또는 권리객체를 저장하는 기능과 디바이스와의 데이터 교환을 하는 기능과 콘텐츠 제공자나 권리객체 발행기관과 통신할 수 있는 데이터 송수신 기능 및 DRM 관리기능이 있어야 한다. 이를 위한 디바이스(900)는 암호화기능을 갖는 RSA 모듈(940)과 세션키 생성모듈(950)과 AES 모듈(960)을 포함하고 저장 기능을 갖는 콘텐츠 저장 모듈(930)을 포함하고 보안 멀티미디어카드와 데이터 교환이 가능하도록 하는 MMC 인터페이스(910)와 DRM 과정을 수행하기 위하여 각 구성모듈을 제어하는 DRM 에이전트 모듈(920)을 포함한다. 또한 디바이스(900)는 데이터 송수신 기능을 위한 송수신 모듈(960)과 재생되는 콘텐츠를 디스플레이하기 위한 디스플레이 모듈(970)을 포함한다.

[0133] 송수신 모듈(960)은 디바이스(900)가 콘텐츠 발행자나 권리객체 발행기관과 통신할 수 있도록 한다. 디바이스(900)는 송수신 모듈(960)을 통해 권리객체나 암호화된 콘텐츠를 외부로부터 얻을 수 있다.

[0134] MMC 인터페이스(910)는 디바이스(900)가 보안 멀티미디어카드와 연결될 수 있도록 한다. 기본적으로 디바이스(900)가 보안 멀티미디어카드와 연결된다는 것은 보안 멀티미디어카드와 디바이스의 인터페이스들이 서로 전기적으로 연결된 것을 의미하지만, 이는 예시적인 것으로서 "연결"이라는 의미는 비접촉 상태에서 무선매체를 통해 서로 통신할 수 있는 상태에 있다는 것도 의미도 포함되는 것으로 해석해야 한다.

[0135] RSA 모듈(940)은 공개키 암호화를 수행하는 모듈로서 제어 모듈(920)의 요청에 따라 RSA 암호화를 수행한다.

[0136] 세션키 생성모듈(950)은 디바이스에게 전달할 난수를 생성하고 디바이스로부터 받은 난수와 자신이 생성한 난수를 이용하여 세션키를 생성한다. 세션키 생성모듈(950)에서 생성한 난수는 RSA 모듈을 통해 암호화되고 MMC 인터페이스(910)를 통해 디바이스에게 전달된다. 한편, 세션키 생성모듈(950)에서 난수를 생성하는 것은 예시적인 것으로서 이미 존재하고 있는 복수의 난수들 중에 어느 한 난수를 선택하는 것이 가능하다는 것은 앞서 살펴본 바 있다.

[0137] AES 모듈(960)은 대칭키 암호화 모듈로서 생성된 세션키를 사용하여 대칭키 암호화를 수행한다. 주로 권리객체로부터 콘텐츠 암호화 키를 받아 이를 세션키로 암호화하는데 사용하며, 이 밖에 디바이스와의 통신 과정에서 중요한 정보를 암호화할 때 사용한다. AES 암호화 방식 또한 예시적인 것으로서, DES와 같이 다른 대칭키 암호화를 사용하는 것 또한 가능하다.

[0138] 콘텐츠 저장 모듈(930)은 DRM으로 보호되는 콘텐츠들을 저장한다. DRM으로 보호되는 콘텐츠는 콘텐츠 암호화 키로 암호화되어 있다. DRM으로 보호되는 콘텐츠를 재생하기 위해서는 콘텐츠 암호화 키가 있어야 한다. 재생이 끝난 콘텐츠는 다시 콘텐츠 암호화 키로 암호화되어 저장된다.

[0139] 디스플레이 모듈(970)은 권리객체를 통해 재생이 허가된 콘텐츠의 재생되는 모습을 사용자가 시각적으로 볼 수 있도록 디스플레이 한다. 디스플레이 모듈(970)은 TFT LCD와 같은 액정표시장치나 유기EL로 구현될 수 있다.

[0140] DRM 에이전트 모듈(920)은 각 구성요소들이 DRM 동작을 할 수 있도록 제어한다.

[0141] 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 예를 들면, 도 3의 실시예에서 보안 멀티미디어카드는 콘텐츠 암호화 키를 세션키로 암호화하지 않고 디바이스 공개키($PuKey_D$)로 암호화하여 디바이스에게 전달할 수도 있다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구의 범위에 의하여 나타내어지며, 특허청구의 범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

발명의 효과

[0142] 본 발명은 휴대형 저장장치를 이용하여 디바이스가 DRM으로 보호되는 콘텐츠를 재생(Playback)하는 구체적인 과정을 개시하고 있으며, 이에 따라 디바이스는 DRM으로 보호되는 콘텐츠를 재생할 수 있다.

[0143] 또한 본 발명의 실시예는 디바이스가 DRM으로 보호되는 콘텐츠를 재생하기 위하여 휴대형 디바이스와 권리객체 전부를 주고받지 않고 간략화된 일부 정보만을 교환한다. 따라서 이 실시예에 따르면 디바이스와 휴대형 저장장치간의 통신 오버헤드를 줄일 수 있다.

[0144] 또한 본 발명의 실시예에 따르면 디바이스에서 DRM으로 보호되는 콘텐츠의 재생중에 휴대형 저장장치의 상태를 체크할 수 있다.

[0145] 또한 본 발명의 실시예에 따르면 권리객체를 연속적으로 사용하는 경우의 절차를 정의하고 있으므로 연속적인 권리객체의 사용이 가능하다.

[0146] 이 밖에 본 발명의 실시예에 따르면 휴대형 저장장치의 권리객체를 사용하지 않는 경우에 휴대형 저장장치와의 재생절차를 종료하는 프로세스를 종료할 수 있다.

도면의 간단한 설명

[0001] 도 1은 디지털 저작권 관리의 개념을 설명하는 도면이다.

[0002] 도 2는 본 발명의 일 실시예에 따른 디지털 저작권의 개념을 간략히 설명하는 도면이다.

[0003] 도 3은 본 발명의 일 실시예에 따른 콘텐츠 재생과정을 보여주는 도면이다.

[0004] 도 4는 본 발명의 일 실시예에 따른 콘텐츠 재생에 사용되는 권리객체의 형식을 보여주는 도면이다.

[0005] 도 5는 본 발명의 일 실시예에 따른 현재 허가 상태 형식을 보여주는 도면이다.

[0006] 도 6은 본 발명의 다른 실시예에 따른 현재 허가 상태 형식을 보여주는 도면이다.

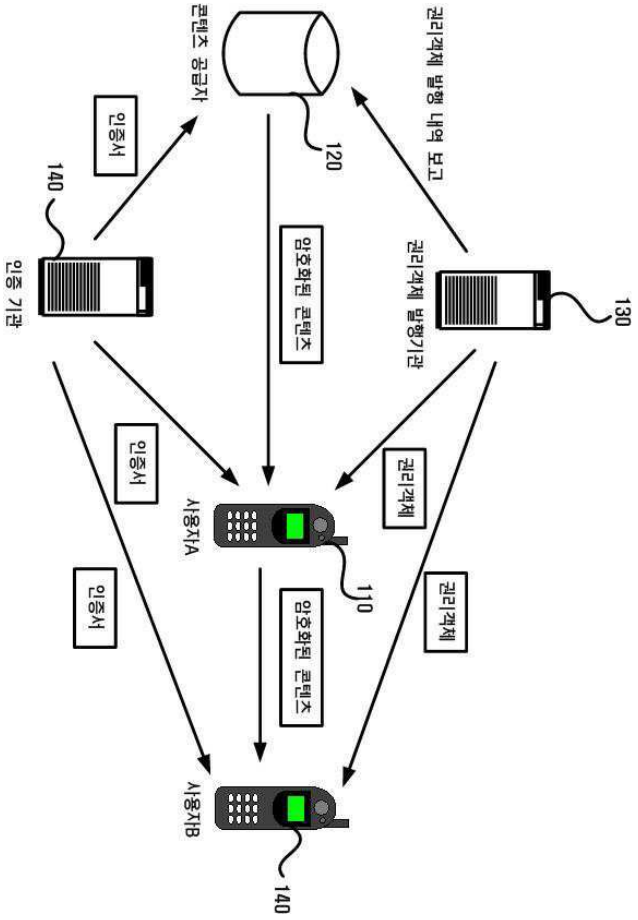
[0007] 도 7는 본 발명의 또 다른 실시예에 따른 현재 허가 상태 형식을 보여주는 도면이다.

[0008] 도 8은 본 발명의 일 실시예에 따른 보안 멀티미디어카드의 블록도이다.

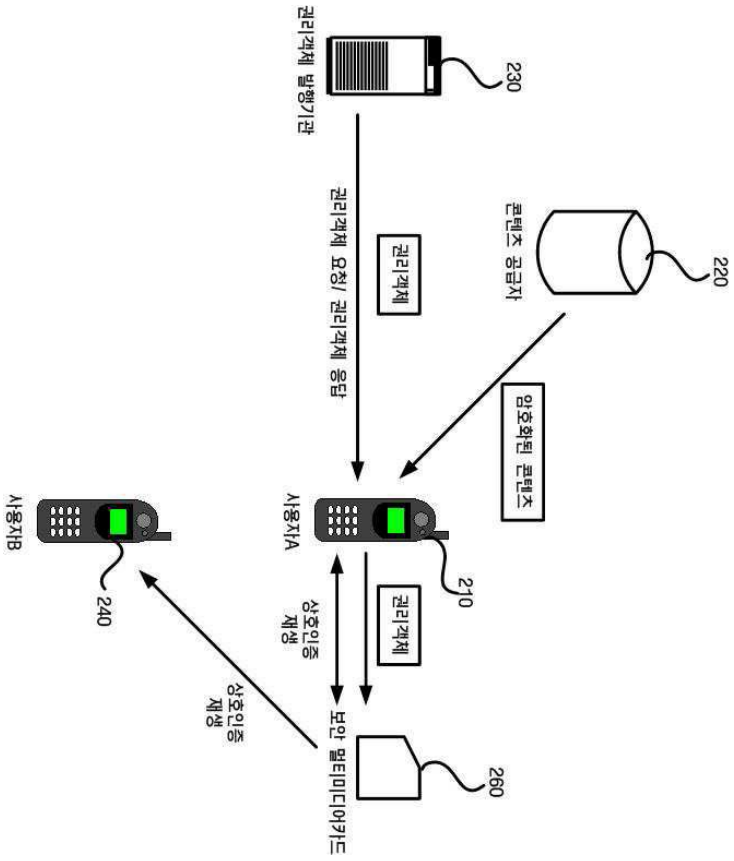
[0009] 도 9는 본 발명의 일 실시예에 따른 디바이스의 블록도이다.

도면

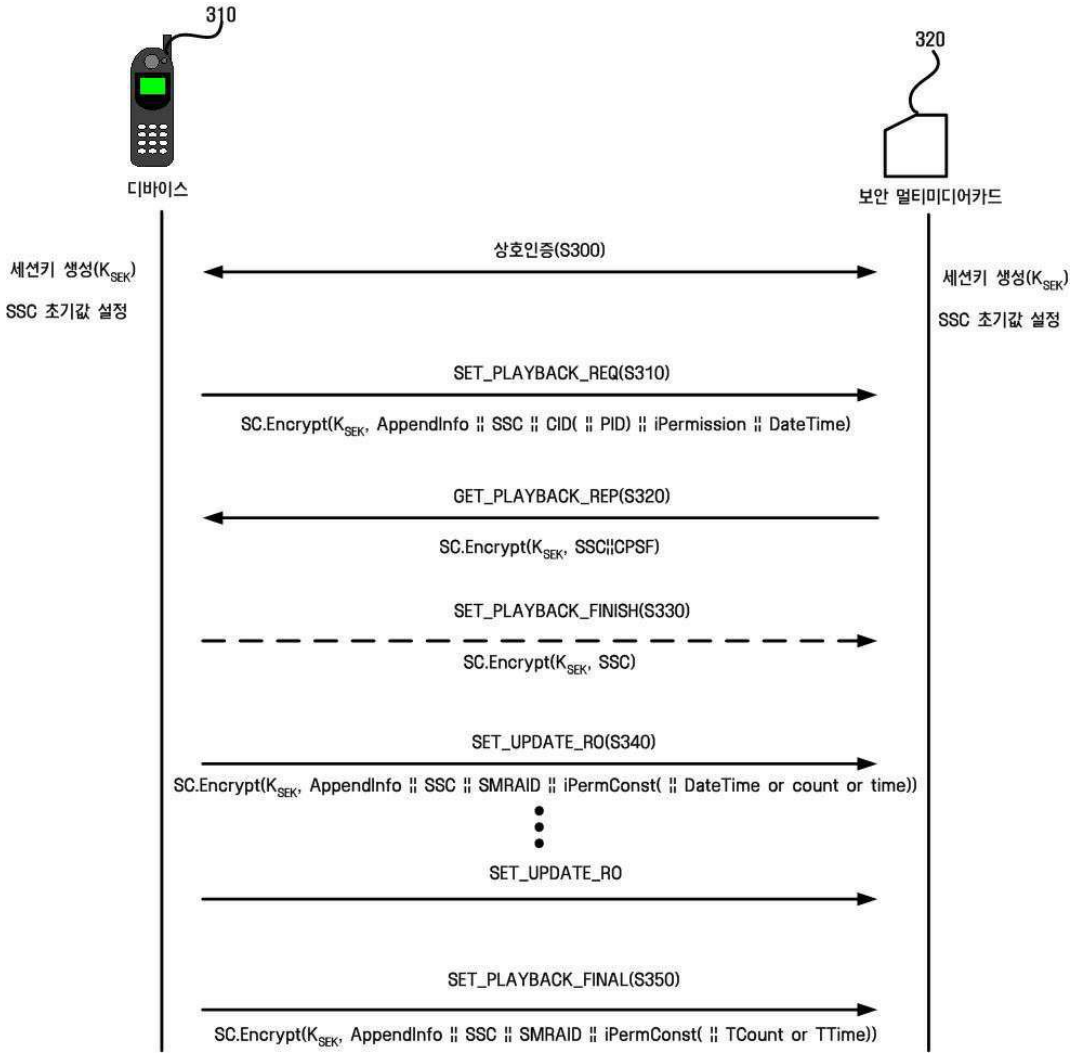
도면1



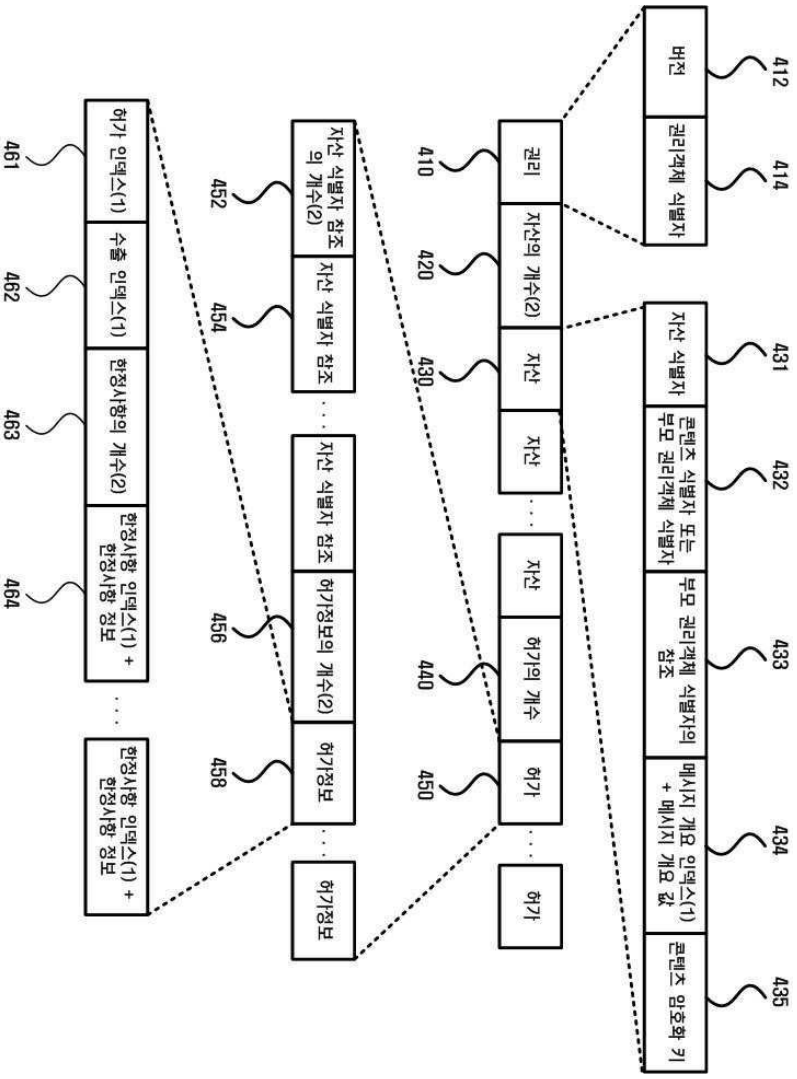
도면2


권리객체 발행기관
230
권리객체 요청 / 권리객체 응답
권리객체
콘텐츠 공급자
220
암호화된 콘텐츠
사용자A
210
상호인증 세션
권리객체
사용자B
240
상호인증 세션
모바일 멀티미디어기기
260

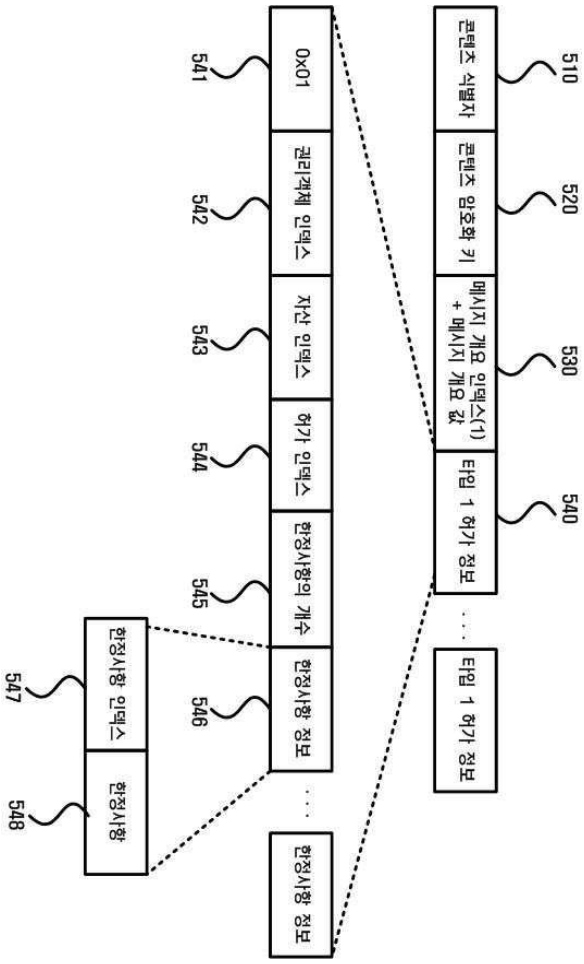
도면3


310
320
디바이스
보안 멀티미디어카드
상호인증(S300)
세션키 생성(K_{SEK})
SSC 초기값 설정
세션키 생성(K_{SEK})
SSC 초기값 설정
SET_PLAYBACK_REQ(S310)
SC.Encrypt(K_{SEK}, AppendInfo ¦¦ SSC ¦¦ CID(¦¦ PID) ¦¦ iPermission ¦¦ DateTime)
GET_PLAYBACK_REP(S320)
SC.Encrypt(K_{SEK}, SSC¦¦CPSF)
SET_PLAYBACK_FINISH(S330)
SC.Encrypt(K_{SEK}, SSC)
SET_UPDATE_RO(S340)
SC.Encrypt(K_{SEK}, AppendInfo ¦¦ SSC ¦¦ SMRAID ¦¦ iPermConst(¦¦ DateTime or count or time))
SET_UPDATE_RO
SET_PLAYBACK_FINAL(S350)
SC.Encrypt(K_{SEK}, AppendInfo ¦¦ SSC ¦¦ SMRAID ¦¦ iPermConst(¦¦ TCount or TTime))

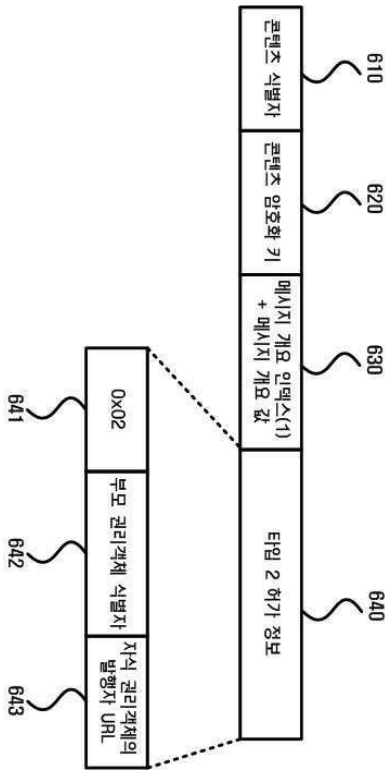
도면4


412
414
버전
권리객체 식별자
410
420
430
권리
자산의 개수(2)
자산
자산
자산
431
432
433
434
435
자산 식별자
콘텍츠 식별자 또는 부모 권리객체 식별자
부모 권리객체 식별자의 참조
메시지 개요 인덱스(1) + 메시지 개요 값
콘텍츠 암호화 키
440
450
자산
허가의 개수
허가
허가
452
454
456
458
자산 식별자 참조의 개수(2)
자산 식별자 참조
자산 식별자 참조
허가정보의 개수(2)
허가정보
허가정보
461
462
463
464
허가 인덱스(1)
수출 인덱스(1)
한정사항의 개수(2)
한정사항 인덱스(1) + 한정사항 정보
한정사항 인덱스(1) + 한정사항 정보

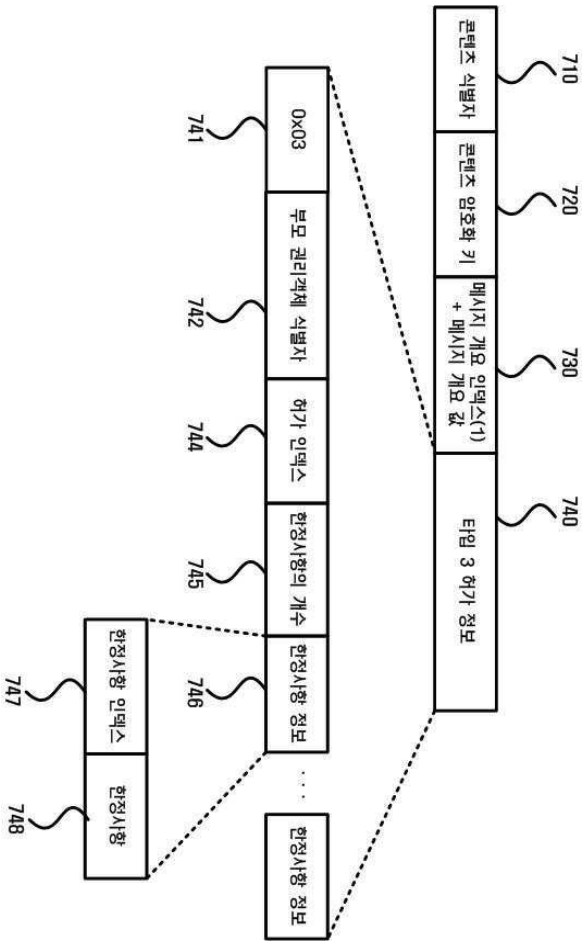
도면5


콘텐츠 식별자
510
콘텐츠 암호화 키
520
메시지 개요 인덱스(1) + 메시지 개요 값
530
타입 1 허가 정보
540
...
타입 1 허가 정보
0x01
541
권리객체 인덱스
542
자산 인덱스
543
허가 인덱스
544
한정사항의 개수
545
한정사항 정보
546
...
한정사항 정보
한정사항 인덱스
547
한정사항
548

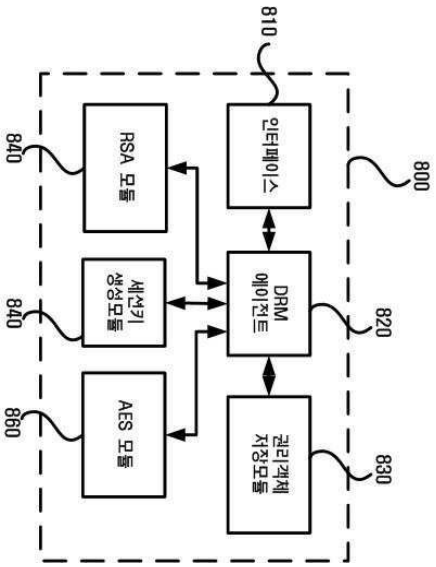
도면6


콘텐츠 식별자
610
콘텐츠 암호화 키
620
메시지 개요 인덱스(1) + 메시지 개요 값
630
타입 2 허가 정보
640
0x02
641
부모 권리객체 식별자
642
자식 권리객체의 발행자 URL
643

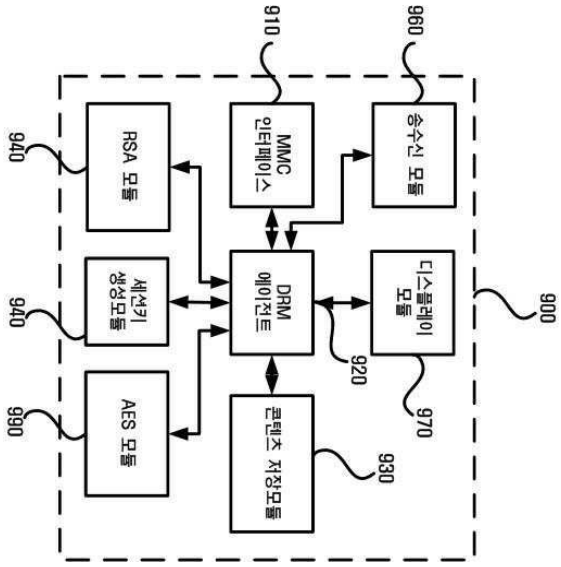
도면7


710
콘텐츠 식별자
720
콘텐츠 암호화 키
730
메시지 개요 인덱스(1) + 메시지 개요 값
740
타입 3 허가 정보
741
0x03
742
부모 권리객체 식별자
744
허가 인덱스
745
한정사항의 개수
746
한정사항 정보
747
한정사항 인덱스
748
한정사항
한정사항 정보

도면8


810
800
인터페이스
DRM 에이전트
820
권리객체 저장모듈
830
RSA 모듈
840
세션키 생성모듈
840
AES 모듈
860

도면9



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 13, 9째줄

【변경전】

상기 휴대형 저장장치

【변경후】

휴대형 저장장치