(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년04월19일
(11) 등록번호 10-1135145
(24) 등록일자 2012년04월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/24 (2006.01) *G06Q 30/00* (2006.01)
(21) 출원번호 10-2007-0024318
(22) 출원일자 2007년03월13일
심사청구일자 2007년03월13일
(65) 공개번호 10-2007-0109804
(43) 공개일자 2007년11월15일
(30) 우선권주장
60/799,652 2006년05월12일 미국(US)
(56) 선행기술조사문헌
KR1020000029092 A*
KR1020050115151 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
김여진
경기도 수원시 팔달구 인계로166번길 48-21, 샤르망 오피스텔 507 (인계동)
오윤상
서울 강남구 도곡2동 개포한신아파트 8동 703호
(뒷면에 계속)
(74) 대리인
정상빈, 특허법인가산

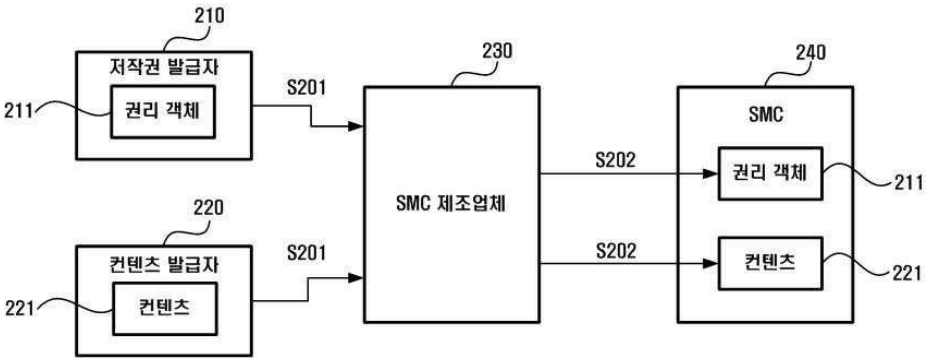
전체 청구항 수 : 총 6 항 심사관 : 계원호

(54) 발명의 명칭 **보안용 멀티미디어 카드, 디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 장치**

(57) 요 약

디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 장치가 제공된다. 디지털 컨텐츠 사용을 위한 권리객체 발급 방법은 컨텐츠 구매 인터페이스를 통해 원하는 컨텐츠가 선택되고 결재되는 단계, 상기 결재된 컨텐츠에 대한 권리객체를 지정된 바인딩 대상키로 암호화하는 단계 및 상기 권리객체를 보안용 멀티미디어 카드(secure multi-media card)에 저장하는 단계를 포함한다.

대 표 도 - 도2



(72) 발명자

심상규

경기도 수원시 영통구 매영로247번길 15, 103동 202호 (원천동, 호산빌리지)

정경임

경기도 성남시 분당구 내정로 186, 롯데아파트 128동903호 (수내동, 파크타운)

김지수

경기 용인시 수지구 상현동 풍산아파트 102동 701호

특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

권리객체 발급 장치가 권리객체를 발급하는 방법에 있어서,

선택된 디지털 컨텐츠에 대한 권한을 나타내는 권리객체를 지정된 바인딩 대상키로 암호화하는 단계; 및

상기 권리객체를 보안용 멀티미디어 카드에 저장하는 단계를 포함하며,

상기 지정된 바인딩 대상키는 멀티미디어 카드키, 사용자 키, 도메인키 및 호스트키 중 하나로부터 선택되어 지정된 키이며, 지정된 바인딩 대상키에 따라 상기 디지털 컨텐츠에 대한 권한을 달리하는, 디지털 컨텐츠 사용을 위한 권리객체 발급 방법.

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

제 3항에 있어서,

상기 보안용 멀티미디어 카드에 저장된 권리객체는 다른 장치로 이동되거나 복사가 가능한, 디지털 컨텐츠 사용을 위한 권리 객체 발급 방법.

청구항 10

호스트가 디지털 컨텐츠 저장 장치와 상호 인증 후 보안 채널을 형성하고, 상기 호스트가 상기 디지털 컨텐츠 저장 장치로부터 디지털 컨텐츠에 대한 권한을 나타내는 권리객체를 전송받는 단계; 및

상기 호스트가 상기 디지털 컨텐츠 저장 장치로부터 전송받은 권리객체를 지정된 바인딩 대상키로 복호화하여 상기 디지털 컨텐츠의 재생에 필요한 정보를 제공하는 단계를 포함하며,

상기 지정된 바인딩 대상키는 멀티미디어 카드키, 사용자 키, 도메인키 및 호스트키 중 하나로부터 선택되어 지정된 키이며, 지정된 바인딩 대상키에 따라 상기 디지털 컨텐츠에 대한 권한을 달리하는, 디지털 컨텐츠 사용을 위한 권리객체 발급 방법.

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

선택된 디지털 컨텐츠에 대한 권한을 나타내는 권리객체를 지정된 바인딩 대상키로 암호화하고 상기 권리객체를 보안용 멀티미디어 카드에 저장하는 암호화 처리부; 및

상기 보안용 멀티 미디어 카드와 통신하는 통신 인터페이스부를 포함하며,

상기 지정된 바인딩 대상키는 멀티미디어 카드키, 사용자 키, 도메인키 및 호스트키 중 하나로부터 선택되어 지정된 키이며, 지정된 바인딩 대상키에 따라 상기 디지털 컨텐츠에 대한 권한을 달리하는, 디지털 컨텐츠 사용을 위한 권리객체 발급 장치.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

제 15항에 있어서,

상기 보안용 멀티미디어 카드에 저장된 권리객체는 다른 장치로 이동되거나 복사가 가능한, 디지털 컨텐츠 사용을 위한 권리객체 발급 장치.

청구항 21

보안용 멀티미디어 카드와 상호 인증 후 보안 채널을 형성하고, 상기 보안용 멀티 미디어 카드로부터 디지털 컨텐츠에 대한 권한을 나타내는 권리객체를 전송받는 통신 인터페이스부; 및

상기 보안용 멀티미디어 카드로부터 전송된 권리객체를 바인딩 대상키로 복호화하여 상기 디지털 컨텐츠의 재생에 필요한 정보를 제공하는 컨텐츠 제공부를 포함하며,

상기 지정된 바인딩 대상키는 멀티미디어 카드키, 사용자 키, 도메인키 및 호스트키 중 하나로부터 선택되어 지정된 키이며, 지정된 바인딩 대상키에 따라 상기 디지털 컨텐츠에 대한 권한을 달리하는, 디지털 컨텐츠 사용을 위한 권리객체 발급 장치.

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0012] 본 발명은 디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 장치에 관한 것으로서, 더욱 상세하게는 주로 온라인으로 제공되던 디지털 저작권 관리(Digital Rights Management, 이하 DRM이라 칭함) 컨텐츠를 보안용 멀티미디어 카드(secure multi-media card, 이하 SMC라 칭함)에 저장하여 오프라인을 통해서도 DRM 컨텐츠 유통을 가능하도록 하는 디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 사용 방법, 그리고 이를 실행하는 장치에 관한 것이다.

[0013] DRM은 디지털 컨텐츠의 저작권을 보호하고 디지털 컨텐츠 사용에 대한 정당한 과금을 위해 고안된 기술적 장치로서, 무단 복제 및 배포가 용이한 디지털 컨텐츠를 보호하기 위한 것이다.

[0014] 이를 위해, 종래에는 디지털 컨텐츠에 대한 접근(Access)을 대가를 지불한 사용자에게만 허용하고, 대가를 지불하지 않은 사용자는 디지털 컨텐츠에 접근할 수 없도록 하고 있었으나, 디지털 데이터의 특성상 디지털 컨텐츠는 재사용, 가공, 복제 및 배포가 용이하기 때문에, 대가를 지불하고 디지털 컨텐츠에 접근한 사용자가 이를 무단으로 복제 또는 배포할 경우에는 대가를 지불하지 않은 사용자도 디지털 컨텐츠를 사용할 수 있게 되는 문제점이 있었다.

[0015] 이러한 문제점을 보완하기 위해 DRM은 디지털 컨텐츠를 암호화하여 배포하도록 하고, 암호화된 디지털 컨텐츠를 사용하기 위해서는 권리객체(Right Object; RO)라는 특정 라이센스가 필요하도록 한다.

[0016] 도 1은 종래의 DRM 개념을 나타낸 도면이다.

[0017] 디지털 컨텐츠(이하, 컨텐츠라 칭함)를 사용하려는 사용자(110)는 원하는 컨텐츠를 컨텐츠 발급자(120)로부터 획득할 수 있다.

[0018] 이때, 컨텐츠 발급자(120)가 공급하는 컨텐츠는 암호화된 상태이며, 암호화된 컨텐츠를 사용하기 위해서는, DRM 시스템에서 컨텐츠의 저작권 정보 및 사용자 권리와 같은 정보를 포함하는 소프트웨어 객체인 권리객체가 필요하다.

[0019] 사용자(110)는 일정 대가를 지불하고 권리객체 발급자(130)로부터 컨텐츠를 실행시킬 수 있는 권한이 포함된 권리객체를 획득할 수 있는데, 이때, 권리객체에 포함된 권한은 암호화된 컨텐츠를 복호화시킬 수 있는 컨텐츠 암호화 키(Key)를 포함할 수 있다.

[0020] 이후, 권리객체 발급자(130)는 컨텐츠 발급자(120)에게 권리객체 발행 내역을 보고하게 되는데, 경우에 따라서는 권리객체 발급자(130)와 컨텐츠 발급자(120)가 동일 주체일 수 있다.

[0021] 상술한 과정을 통해 권리객체를 획득한 사용자(110)는 권리객체를 소비하여 컨텐츠를 사용할 수 있게 된다.

[0022] 이때, 권리객체는 권리객체를 통해 컨텐츠를 사용할 수 있는 횟수나 기간 등의 제한 정보 또는 권리객체의 복제

를 허용하는 횟수 등에 관한 제한 정보를 포함하고 있으며, 컨텐츠와 달리 권리객체는 그 재사용이나 복제에 일정 제한이 가해지게 되므로, DRM에 의해서 컨텐츠를 효과적으로 보호할 수 있게 된다.

[0023] 사용자는 이러한 권리객체를 PC, MP3 플레이어, 휴대폰 및 PDA와 같은 멀티미디어 데이터를 실행시키는 호스트에 저장하게 되며, 이에 따라 서로 다른 장치들 간에 디지털 컨텐츠를 공유할 필요성이 증대되었다.

[0024] 그러나, 종래의 DRM 기술을 기반으로 판매되는 DRM 컨텐츠는 특정 장치에 귀속되어 있어 다른 장치에서는 사용할 수 없는 불편함이 있다.

발명이 이루고자 하는 기술적 과제

[0025] 이에 본 발명은, 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 장치를 통해 디지털 컨텐츠와 권리객체를 SMC라는 하드웨어에 미디어 형태로 보유함으로써, 다양한 멀티미디어 장치에서 디지털 컨텐츠를 사용할 수 있게 하는데 그 목적이 있다.

[0026] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 구성 및 작용

[0027] 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 발급 방법은 SMC 제조업체가 컨텐츠 제공자와 저작권 발급자로부터 각기 컨텐츠와 저작권 객체를 제공받는 단계 및 상기 제공받은 저작권 객체를 SMC의 공개키로 암호화하여 상기 SMC에 저장하는 단계를 포함한다.

[0028] 상기 목적을 달성하기 위하여, 본 발명의 다른 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 발급 방법은 사용자에 의해 컨텐츠 구매 인터페이스를 통해 원하는 컨텐츠가 선택되고 결재되는 단계, 상기 결재된 컨텐츠에 대한 권리객체를 지정된 바인딩 대상키로 암호화하는 단계 및 상기 권리객체를 SMC에 저장하는 단계를 포함한다.

[0029] 상기 목적을 달성하기 위하여, 본 발명의 또 다른 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 사용 방법은 컨텐츠 저장 장치와 상호 인증 후 보안 채널을 형성하고, 상기 컨텐츠 저장 장치로부터 권리객체를 전송받는 단계 및 상기 전송받은 권리객체를 바인딩 대상키로 복호화하여 컨텐츠 재생에 필요한 정보를 제공하는 단계를 포함한다.

[0030] 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 발급 장치는 구매하는 컨텐츠의 선택을 입력 받고 상기 선택된 컨텐츠에 대한 결재가 이루어지는 구매 인터페이스부, 상기 결재된 컨텐츠에 대한 권리객체를 지정된 바인딩 대상키로 암호화하고 상기 권리객체를 SMC에 저장하는 암호화 처리부 및 상기 SMC와 통신하는 통신 인터페이스부를 포함한다.

[0031] 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 사용 장치는 SMC와 상호 인증 후 보안 채널을 형성하고, 상기 SMC로부터 권리객체를 전송 받는 통신 인터페이스부 및 상기 전송된 권리객체를 바인딩 대상키로 복호화하여 컨텐츠 재생에 필요한 정보를 제공하는 컨텐츠 제공부를 포함한다.

[0032] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

[0033] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는

[0034] 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다.

[0035] 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0036] 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0037] 이하, 본 발명의 실시예들에 의한 디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 장치를 설명하기 위한 구성도 또는 처리 흐름도에 대한 도면들을 참고하여 본 발명에 대해 설명하도록 한다.

[0038] 이 때, 처리 흐름도 도면들의 각 구성과 흐름도 도면들의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행

될 수 있음을 이해할 수 있을 것이다.

[0039] 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 흐름도 구성(들)에서 설명된 기능들을 수행하는 수단을 생성하게 된다.

[0040] 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 흐름도 구성(들)에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다.

[0041] 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 흐름도 구성(들)에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0042] 또한, 각 구성은 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다.

[0043] 또, 몇 가지 대체 실행예들에서는 구성들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다.

[0044] 예컨대, 잇달아 도시되어 있는 두 개의 구성들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 구성들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0045] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

[0046] 참고로, 본 발명의 실시예에서 사용되는 SMC에 저장되는 권리객체의 형식은 DRM 컨텐츠 사용에 반드시 필요한 정보만으로 구성된 축약 형태이며, 서로 다른 DRM 시스템에서 지원하는 권리객체의 형식으로 쉽게 변환이 가능하다고 가정한다.

[0047] 도 2는 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체의 발급 방법을 도시한 도면이다.

[0048] SMC 제조업체는 컨텐츠를 제공하며 저작권을 보유하고 있는 컨텐츠 발급자와 권리객체를 발급하는 저작권 발급자로부터 각각 컨텐츠와 권리객체를 제공 받는다(S201).

[0049] 이후, SMC 제조업체는 제공받은 권리객체를 SMC의 키(Key)로 암호화하여 디지털 컨텐츠와 함께 SMC에 저장한다(S202).

[0050] 이때, 암호화하는 키는 공개키 암호화(Public-Key Cryptography) 방식과 대칭키 암호화(Symetric-Key Cryptography) 방식을 사용할 수 있다.

[0051] 공개키 암호화 방식은 비대칭 암호화라고도 하며, 이는 데이터를 암호화하는데 사용되는 암호키와 데이터를 복호화하는데 사용되는 암호키가 서로 다른 암호키로 구성되는 암호화 방식이다.

[0052] 공개키 암호화 방식에서 암호키는 공개키와 개인키의 쌍으로 이루어진다.

[0053] 공개키는 비밀로 보관될 필요가 없고 다른 장치에게 손쉽게 알려질 수 있으며, 개인키는 특정 장치만이 알고 있어야 한다.

[0054] 대칭키 암호화 방식은 비밀키 암호화라고도 하며, 이는 데이터를 암호화하는데 사용되는 암호키와 데이터를 복호화하는데 사용되는 암호키가 동일한 암호키로 구성되는 암호화 방식이다.

[0055] S202에서 사용되는 암호화 키는 상술한 공개키 암호화 방식 및 대칭키 암호화 방식 중 어느 하나를 사용할 수 있으며, 본 발명의 실시예로만 한정하지 않는다.

[0056] 참고로, 데이터(본 발명에서는 권리객체 및 컨텐츠 중 하나 이상을 포함한다)를 특정 대상의 키로 암호화하는 것을 바인딩(Binding)이라 하며, 바인딩 된 데이터는 해당 특정 대상을 통해서만 복호화가 가능하다.

[0057] 특정 대상에 의한 바인딩의 실시예는 **도 3을** 통해 상세히 설명하도록 한다.

[0058] 또한, SMC에 바인딩된 권리객체는 사용자가 임으로 다른 장치에 이동하거나 복제하여 사용할 수 없으며, 바인딩

변경 권한이 부여된 경우 소정의 절차를 거쳐 바인딩 대상을 변경할 수 있다.

[0059] S202 후, SMC 제조업체는 컨텐츠와 해당 권리객체가 저장된 SMC를 상품화하여 시장에 공급한다(S203).

[0060] 도 3은 본 발명의 다른 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체의 발급 방법을 도시한 도면이다.

[0061] 도 3의 실시예에서는, 사용자가 보유한 SMC(340)가 온라인 호스트(330)에 삽입되어 있고, 온라인 호스트(330)는 저작권 발급자(310) 및 컨텐츠 발급자(320)로부터 하나 이상 다수의 컨텐츠(321) 및 해당 컨텐츠에 대한 권리객체(311)를 제공받는다고 가정하도록 한다.

[0062] 여기에서 호스트는 권리객체에 포함된 권한에 따라 DRM 컨텐츠를 재생하는 장치로서 SMC 접속부를 포함하고 있으며, 온라인 호스트는 네트워크에 접속하여 저작권 발급자로부터 권리객체를 발급 받을 수 있는 SMC 지원 호스트이다.

[0063] 참고로 온라인 호스트(330)의 예로는 PC, 휴대폰, PDA, PMP 및 키오스크(Kiosk) 등이 있으며, 키오스크를 온라인 호스트(330)로 사용할 경우, SMC 구입과 도 3을 통해 설명하는 권리객체의 발급이 동시에 수행될 수 있다.

[0064] 먼저, 사용자는 온라인 호스트(330)가 제공하는 컨텐츠 구매 인터페이스를 통해 원하는 컨텐츠(321)를 선택하고 결재한다(S301).

[0065] 이때, 온라인 호스트가 제공하는 컨텐츠 구매 인터페이스는 사용자의 선택을 위해 하나 이상 다수의 컨텐츠 목록을 디스플레이하는 디스플레이부(미도시) 및 컨텐츠의 선택을 입력 받는 입력부(미도시) 중 하나 이상을 포함할 수 있으며, 컨텐츠의 결재를 위해 결재 시스템(미도시)과 유무선 네트워크로 연결될 수 있다.

[0066] S301 후, 결재된 컨텐츠(321)에 대한 권리객체(311)를 온라인 호스트(330)에서 지정된 바인딩 대상키로 암호화한다(S302).

[0067] 이때, 바인딩 대상은 저작권 발급자(310)의 정책에 따라 바인딩 대상이 지정될 수 있고, 사용자가 결재 후 바인딩 대상을 지정할 수도 있다.

[0068] 본 발명의 실시예에 따른 바인딩 대상은 카드, 사용자, 도메인 및 호스트가 있으며, 상세한 설명은 아래와 같다.

[0069] (1) SMC 바인딩 : 권리객체가 SMC의 키로 암호화 되어있어, 해당 SMC 이외의 장치로 권리객체를 이동하거나 복제하는 경우 컨텐츠의 사용이 불가능하다.

[0070] 단, 해당 SMC를 소지한 사람이면 누구나 SMC에 바인딩된 권리객체를 소비할 수 있다.

[0071] (2) 사용자 바인딩 : 권리객체가 사용자의 키로 암호화 되어있어, 타인은 사용이 불가능하며, 사용자는 자신이 보유한 다양한 장치들에서 바인딩된 권리객체를 소비할 수 있다.

[0072] (3) 도메인 바인딩 : 권리객체가 도메인 키로 암호화 되어있어 해당 도메인에 가입되지 않은 장치에서는 사용이 불가능하며, 도메인 내의 모든 장치에서는 해당 도메인에 바인딩된 권리객체를 소비할 수 있다.

[0073] (4) 호스트 바인딩 : 권리객체가 호스트 키로 암호화 되어있어 해당 호스트 이외의 장치로 권리객체를 이동시킬 경우 사용이 불가능하며, 해당 호스트를 소유한 사람이라면 누구나 호스트에 바인딩된 권리객체를 소비할 수 있다.

[0074] 이때, 권리객체의 이동 및 복제는 해당 권한이 있는 경우에 가능하며, 만일 제 1 장치에서 제 2 장치로 권리객체를 이동하는 경우, 제 1 장치에 저장된 권리객체는 완전히 제거된 상태가 되어 해당 권리객체는 제 2 장치에만 존재하게 된다.

[0075] 참고로, S302에서 권리객체(311)를 바인딩하는 주체가 저작권 발급자(310)인 경우, 권리객체(311)는 저작권 발급자(310)가 지정한 바인딩 대상키로 암호화되어 온라인 호스트(330)에 전송되고, 만일 S302에서 권리객체(311)를 바인딩하는 주체가 온라인 호스트(330)인 경우, 권리객체(311)가 저작권 발급자(310)로부터 온라인 호스트(330)에 발급되면 온라인 호스트(330)에서 지정한 바인딩 대상키로 암호화된다.

[0076] S302 후, 암호화된 권리객체(311)는 해당 컨텐츠(321)와 함께 온라인 호스트(330)에 전송된다(S303).

[0077] S303 후, 권리객체(311)와 컨텐츠(321)는 SMC(340)로 이동되어 저장된다(S304).

[0078] 이때, 권리객체(311)는 온라인 호스트(330)에서 SMC(340)로 이동되기 위한 권한을 포함할 수 있으며, 특정 SMC

에만 이동될 수 있도록 제한될 수 있다.

[0079] S304 후, 사용자는 SMC(340)를 온라인 호스트로(330)부터 회수하여 컨텐츠(321) 및 해당 권리객체(311)를 바인딩 대상에 맞게 사용할 수 있다.

[0080] 도 4는 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체의 사용 방법을 도시한 도면이다.

[0081] 참고로, 사용자가 보유한 SMC(410)에 컨텐츠(412) 및 권리객체(411)가 저장되어 있고, 사용자는 이를 사용하기 위해 SMC(410)를 호스트(420)에 삽입한다고 가정하도록 한다.

[0082] SMC(410)가 호스트(420)에 삽입되면, 호스트(420)와 SMC(410)는 상호 인증 후 보안 채널을 형성한다(S401).

[0083] 이때, SMC(410)와 호스트(420)간 상호 인증은 바인딩 대상으로 인증이 가능하다.

[0084] 예를 들어, SMC(410)에 저장된 권리객체(411)가 사용자 키로 바인딩 되어 있다면, S401에서 사용자 키를 통해 상호 인증이 가능하며, 본 발명의 실시예에 따른 상호 인증 방법을 바인딩 대상으로만 한정하지 않는다.

[0085] 여기에서 보안 채널은 장치간 인증 후 형성되는 전송 채널로서 전송 데이터의 암호화 및 무결성 등을 보장한다.

[0086] S401 후, 호스트(420)가 SMC(410)에 권리객체(411)를 요청하면, SMC(410)는 권리객체(411)의 정보를 호스트(420)에 전송한다(S402).

[0087] 이때, 호스트(420)에 전송되는 권리객체(411)의 정보는 컨텐츠(412)를 사용할 수 있는 권한, 해당 컨텐츠(412)에 대한 사용 제한 정보, 권리객체(411)의 복제 제한 정보, 권리객체(411)의 ID 및 컨텐츠(412)의 ID와 같은 정보를 포함한다.

[0088] 이하, 권리객체(411)의 정보에 대해 좀 더 상세히 설명하도록 한다.

[0089] 컨텐츠(412)를 사용할 수 있는 권한은 컨텐츠(412)를 복호화할 수 있는 컨텐츠 암호화 키(Content Encryption Key; 이하 CEK라 함)를 포함하며, CEK는 장치(본 발명에서는 호스트(420))가 이용하고자 하는 컨텐츠(412)를 복호화하는 키 값으로, 호스트(420)는 권리객체(411)가 저장된 저장장치(본 발명에서는 SMC(410))로부터 권리객체(411)를 전송 받고, 전송된 권리객체(411)에서 CEK를 추출하여 컨텐츠를 복호화 함으로써 보호된 컨텐츠를 사용할 수 있다.

[0090] 사용 제한 정보는 컨텐츠(412)를 실행시키기 위해 권리객체(411)를 소비할 수 있는 한도를 나타내는 정보로서, 사용 제한의 종류에는 사용 날짜 제한, 사용 횟수 제한, 사용 기간 제한, 사용 기한 제한 등이 있다.

[0091] 한편, 복제 제한 정보는 권리객체(411)를 복사하거나 이동시킬 수 있는 횟수나 한도를 제한하는 정보로서, 복제 제한 정보는 복사 제한 정보 및 이동 제한 정보를 포함할 수 있다.

[0092] 권리객체(411)의 복사는 기존의 호스트(420) 또는 제 1 저장장치(이하 원본장치라 칭함)에 권리객체(411)가 남아있는 상태에서 동일한 권리객체(411)를 다른 호스트(미도시) 또는 제 2 저장장치(이하 목적장치라 칭함)에 전송시키는 개념이며, 권리객체(411)의 이동은 원본장치에 있던 권리객체(411)를 목적장치(미도시)로 전송시키면서 원본장치에서는 해당 권리객체(411)를 삭제한다.

[0093] 따라서 사용자는 호스트나 휴대용 저장 장치에 저장된 권리객체를 해당 권리객체에 설정된 복사 제한 횟수 또는 이동 제한 횟수만큼 다른 호스트나 휴대용 저장 장치로 복사 또는 이동시킬 수 있다.

[0094] 권리객체(411)의 ID는 다른 권리객체로부터 자신을 식별하도록 하는 식별자이며, 컨텐츠(412)의 ID는 권리객체(411)를 소비함으로써 실행시킬 수 있는 컨텐츠(412)를 식별하기 위한 컨텐츠(412)의 식별자이다.

[0095] 한편, S402에서, SMC(410)로부터 호스트(420)로 전송된 권리객체(411)의 정보는 호스트(420)에서 바인딩 대상키로 복호화되어 컨텐츠(412) 재생에 필요한 정보를 제공한다(S403).

[0096] 이때, 어떤 바인딩 대상키로 암호화 되었는가에 따라 복호화할 바인딩 대상키가 결정된다.

[0097] 본 발명의 실시예에 따른 바인딩 대상은 카드, 사용자, 도메인 및 호스트가 있으며, 상세한 설명은 아래와 같다.

[0098] (1) SMC 바인딩 : 권리객체가 SMC의 키로 복호화된다.

[0099] (2) 사용자 바인딩 : 호스트는 입력된 사용자 정보를 기반으로 사용자의 키를 생성하거나, 소정의 저장소에서 사용자의 키를 전송받아 권리객체를 복호화한다.

[0100] (3) 도메인 바인딩 : 도메인에 가입된 호스트의 경우, 해당 도메인 키로 권리객체를 복호화한다.

[0101] (4) 호스트 바인딩 : 현재 SMC와 접속된 호스트가 권리객체를 바인딩한 호스트와 일치하는 경우, 해당 호스트 키로 권리객체를 복호화한다.

[0102] S403 후, 복호화된 권리객체를 통해 획득한 컨텐츠 키로 해당 컨텐츠를 복호화하여 사용한다(S404).

[0103] 도 5는 본 발명의 실시예에 따른 디지털 컨텐스 사용을 위한 권리객체 발급 장치의 구성을 도시한 블록도이다.

[0104] 본 발명의 실시예에 따른 DRM 장치(500)는 컨텐츠, 권리객체 및 권리객체의 상태 정보를 저장하고 저작권 권한 및 제약에 따라 컨텐츠를 사용할 수 있도록 지원해주는 SMC(501), 구매하는 컨텐츠의 선택을 입력 받고, 선택된 컨텐츠에 대한 결재가 이루어지는 구매 인터페이스부(502), 결재된 컨텐츠에 대한 권리객체를 지정된 바인딩 대상키로 암호화하고 권리객체를 SMC(501)에 저장하는 암호화 처리부(503) 및 SMC(501)와 통신하는 통신 인터페이스부(504)를 포함한다.

[0105] 본 발명의 실시예에 따른 도 5 내지 후술하는 도 6에서 도시된 구성요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성요소를 의미하며, 어떤 역할들을 수행한다.

[0106] 그렇지만 구성요소들은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0107] 따라서, 일 예로서 구성요소는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다.

[0108] 구성요소들과 해당 구성요소들 안에서 제공되는 기능은 더 작은 수의 구성요소들로 결합되거나 추가적인 구성요소들로 더 분리될 수 있다.

[0109] 도 5에 도시된 장치(500) 중 SMC(501)는 컨텐츠, 권리객체 및 권리객체의 상태 정보를 저장하고 저작권 권한 및 제약에 따라 컨텐츠를 사용할 수 있도록 지원하는 카드로서 메모리 카드와 스마트 카드를 포함한다.

[0110] 여기에서 권리객체의 상태 정보는 권리객체의 소비 정도를 나타내는 정보로서, 권리객체 내에 포함될 수도 있고, 권리객체를 저장하고 있는 장치가 권리객체와 함께 별도의 정보로서 관리할 수도 있다.

[0111] 예를 들어, 권리객체에 사용 기한 정보가 10시간으로 설정되어 있고, 호스트가 컨텐츠를 사용하기 위해 권리객체를 소비한 시간이 4시간인 경우, 권리객체의 상태 정보는 호스트가 지금까지 권리객체를 소비한 시간(4시간) 또는 앞으로 호스트가 권리객체를 소비하여 해당 컨텐츠를 사용할 수 있는 시간(6시간)에 대한 정보를 나타낸다.

[0112] 구매 인터페이스부(502)는 구매하는 컨텐츠의 선택을 사용자로부터 입력 받고, 선택된 컨텐츠에 대한 결재가 이루어진다.

[0113] 이를 위해, 구매 인터페이스부(502)는 별도의 입력부(미도시)를 포함할 수 있으며, 컨텐츠에 대한 결재를 위해 별도의 결재 시스템(미도시)과 연결될 수 있다.

[0114] 암호화 처리부(503)는 구매 인터페이스부(502)에서 결재된 컨텐츠에 대한 권리객체를 지정된 바인딩 대상키로 암호화하고 암호화된 권리객체를 통신 인터페이스부(504)를 통해 SMC(501)에 저장한다.

[0115] 통신 인터페이스부(504)는 SMC(501)와 접촉하여 데이터를 송수신하는 통신이 가능하도록 소정의 접촉 단자를 포함할 수 있으며, SMC(501)와 접촉하지 않고도 무선으로 데이터를 송수신할 수 있도록 소정의 무선 통신장치를 포함할 수 있다.

[0116] 이때, 바인딩 대상은 저작권 발급자의 정책에 따라 바인딩 대상이 지정될 수 있고, 사용자가 결재 후 바인딩 대상을 지정할 수도 있다.

[0117] 본 발명의 실시예에 따른 바인딩 대상은 카드, 사용자, 도메인 및 호스트가 있으며, 상세한 설명은 아래와 같다.

[0118] (1) SMC 바인딩 : 권리객체가 SMC의 키로 암호화 되어있어, 해당 SMC 이외의 장치로 권리객체를 이동하거나 복사하는 경우 컨텐츠의 사용이 불가능하다.

[0119] 단, 해당 SMC를 소지한 사람이면 누구나 SMC에 바인딩된 권리객체를 소비할 수 있다.

[0120] (2) 사용자 바인딩 : 권리객체가 사용자의 키로 암호화 되어있어, 타인은 사용이 불가능하며, 사용자는 자신이 보유한 다양한 장치들에서 사용자 바인딩된 권리객체를 소비할 수 있다.

[0121] (3) 도메인 바인딩 : 권리객체가 도메인 키로 암호화 되어있어 해당 도메인에 가입되지 않은 장치에서는 사용이 불가능하며, 도메인 내의 모든 장치에서는 해당 도메인에 바인딩된 권리객체를 소비할 수 있다.

[0122] (4) 호스트 바인딩 : 권리객체가 호스트 키로 암호화 되어있어 해당 호스트 이외의 장치로 권리 객채를 이동시킬 경우 사용이 불가능하며, 해당 호스트를 소유한 사람이라면 누구나 호스트에 바인딩된 권리객체를 소비할 수 있다.

[0123] 참고로, 권리객체의 이동 및 복사는 해당 권한이 있는 경우에 가능하며, 만일 제 1 장치에서 제 2 장치로 권리객체를 이동하는 경우, 제 1 장치에 저장된 권리객체는 완전히 제거된 상태가 되어 해당 권리객체는 제 2 장치에만 존재하게 된다.

[0124] 만일, 권리객체를 바인딩하는 주체가 저작권 발급자인 경우, 권리객체는 암호화 처리부(503)를 통해 저작권 발급자가 지정한 바인딩 대상키로 암호화되고 온라인 호스트에 전송된다.

[0125] 또한, 권리객체를 바인딩하는 주체가 온라인 호스트인 경우, 권리객체가 온라인 호스트에 발급되면 암호화 처리부(503)를 통해 온라인 호스트에서 지정한 바인딩 대상키로 암호화된다.

[0126] 도 6은 본 발명의 다른 실시예에 따른 디지털 컨텐스 사용을 위한 권리객체 사용 장치의 구성을 도시한 블록도이다.

[0127] 본 발명의 다른 실시예에 따른 DRM 장치(600)는 컨텐츠, 권리객체 및 권리객체의 상태 정보를 저장하고 저작권 권한 및 제약에 따라 컨텐츠를 사용할 수 있도록 지원해주는 SMC(601), SMC(601)와 상호 인증 후 보안 채널을 형성하고, SMC(601)로부터 권리객체를 전송받는 통신 인터페이스부(602) 및 전송된 권리객체를 바인딩 대상키로 복호화하여 컨텐츠 재생에 필요한 정보를 제공하는 컨텐츠 제공부(603)를 포함한다.

[0128] 도 6에 도시된 장치(600) 중 SMC(601)는 도 5에 도시된 장치(500)의 SMC(501)와 동일하므로 설명을 생략하도록 한다.

[0129] 통신 인터페이스부(602)는 SMC(601)와 상호 인증 후 보안 채널을 형성하고, SMC(601)로부터 권리객체를 전송받는다.

[0130] 이를 위해 통신 인터페이스부(602)는 SMC(601)와 접촉하여 데이터를 송수신하는 통신이 가능하도록 소정의 접촉단자를 포함할 수 있으며, SMC(601)와 접촉하지 않고도 무선으로 데이터를 송수신할 수 있도록 소정의 무선 통신장치를 포함할 수 있다.

[0131] 도 6에 도시된 장치(600)는 통신 인터페이스부(602)를 통해 SMC(601)와 보안 채널을 형성하고 권리객체를 전송받는다.

[0132] 여기에서 보안 채널은 장치간 인증 후 형성되는 전송 채널로서 전송 데이터의 암호화 및 무결성 등을 보장한다.

[0133] 컨텐츠 제공부(603)는 SMC(601)에서 통신 인터페이스부(602)를 통해 전송된 권리객체를 바인딩 대상키로 복호화하여 컨텐츠 재생에 필요한 정보를 제공한다.

[0134] 이때, 컨텐츠 제공부(603)는 전송된 권리객체가 어떤 바인딩 대상키로 암호화 되었는가에 따라 복호화할 바인딩 대상키를 결정한다.

[0135] 본 발명의 실시예에 따른 바인딩 대상은 카드, 사용자, 도메인 및 호스트가 있으며, 상세한 설명은 아래와 같다.

[0136] (1) SMC 바인딩 : 권리객체가 SMC의 키로 복호화된다.

[0137] (2) 사용자 바인딩 : 호스트는 입력된 사용자 정보를 기반으로 사용자의 키를 생성하거나, 소정의 저장소에서 사용자의 키를 전송받아 권리객체를 복호화한다.

[0138] (3) 도메인 바인딩 : 도메인에 가입된 호스트의 경우, 해당 도메인 키로 권리객체를 복호화한다.

[0139] (4) 호스트 바인딩 : 현재 SMC와 접속된 호스트가 권리객체를 바인딩한 호스트와 일치하는 경우, 해당 호스트 키로 권리객체를 복호화한다.

[0140] 컨텐츠 제공부(603)는 복호화된 권리객체를 통해 획득한 컨텐츠 키로 해당 컨텐츠를 복호화하여 사용자가 사용할 수 있도록 한다.

[0141] 이상과 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

발명의 효과

[0142] 상기한 바와 같은 본 발명의 디지털 컨텐츠 사용을 위한 권리객체 발급 방법 및 장치에 따르면 다음과 같은 효과가 하나 혹은 그 이상 있다.

[0143] 컨텐츠와 권리객체를 SMC라는 하드웨어에 미디어 형태로 보유하여, 디지털 컨텐츠 미디어의 소장 가치 및 컨텐츠 관리의 편의성을 제공하며, 다양한 멀티미디어 장치에서 컨텐츠를 사용할 수 있도록 하는 장점이 있다.

[0144] 또한, 주로 온라인으로 판매되던 DRM 컨텐츠를 오프라인을 통해 구매할 수 있도록 함으로써, 인터넷에 익숙하지 않은 소비자 층을 흡수하여 디지털 컨텐츠 시장을 확대할 수 있는 장점도 있다.

[0145] 또한, SMC에 발급되는 권리객체를 DRM 컨텐츠 사용에 필수적인 요소만으로 구성할 경우, 서로 다른 다양한 DRM 지원이 가능하여 디지털 컨텐츠의 재생 영역을 쉽게 확대할 수 있는 장점도 있다.

[0146] 또한, 권리객체에 대한 복제 및 이동에 획일적인 제한을 두지 않고, 컨텐츠 사용에 대한 다양한 정책을 반영할 수 있어 컨텐츠의 사용성을 증가시키는데 도움이 되는 장점도 있다.

[0147] 또한, 저작권 발급자 및 컨텐츠 제공자의 직접 판매가 가능하게 되므로 컨텐츠 시장에 다양성을 제공할 수 있는 장점도 있다.

도면의 간단한 설명

[0001] 도 1은 종래의 DRM 개념을 나타낸 도면이다.

[0002] 도 2는 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체의 발급 방법을 도시한 도면이다.

[0003] 도 3은 본 발명의 다른 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체의 발급 방법을 도시한 도면이다.

[0004] 도 4는 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체의 사용 방법을 도시한 도면이다.

[0005] 도 5는 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 발급 장치의 구성을 도시한 블록도이다.

[0006] 도 6은 본 발명의 실시예에 따른 디지털 컨텐츠 사용을 위한 권리객체 사용 장치의 구성을 도시한 블록도이다.

[0007] <도면의 주요 부분에 관한 부호의 설명>

[0008] 210 : 저작권 발급자 211 : 권리객체

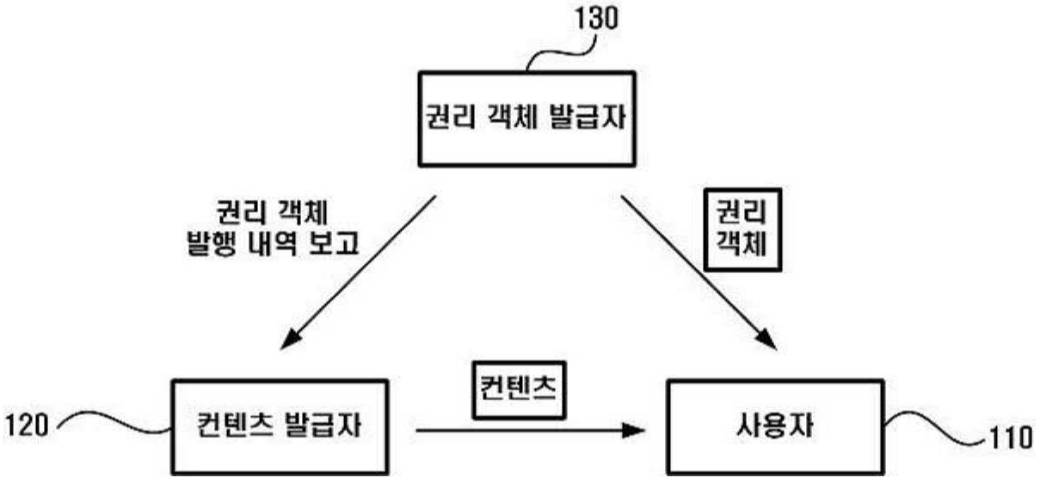
[0009] 220 : 컨텐츠 발급자 221 : 컨텐츠

[0010] 230 : 보안용 멀티미디어 카드(secure multi-media card) 제조업체

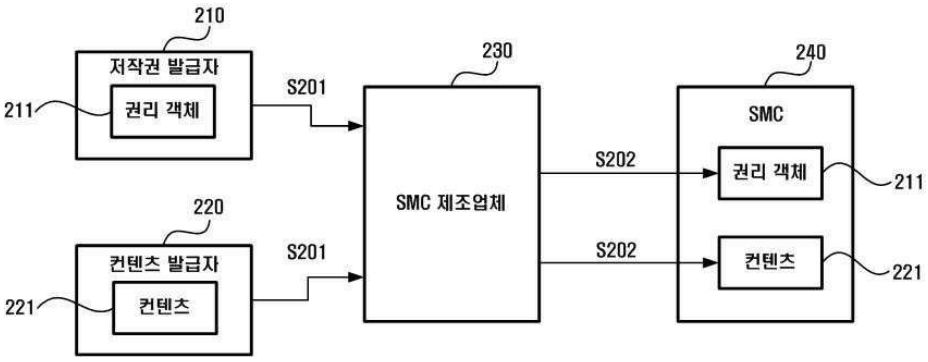
[0011] 240 : 보안용 멀티미디어 카드(secure multi-media card)

도면

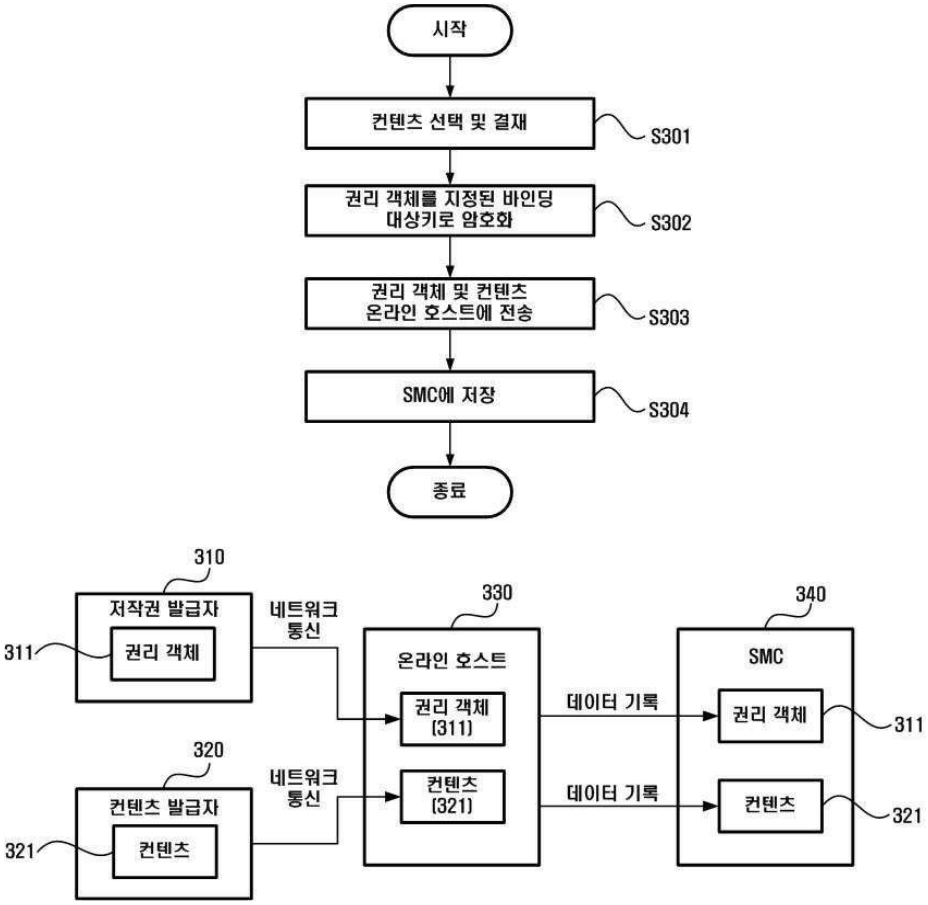
도면1


130
권리 객체 발급자
권리 객체
발행 내역 보고
권리
객체
120
컨텐츠 발급자
컨텐츠
사용자
110

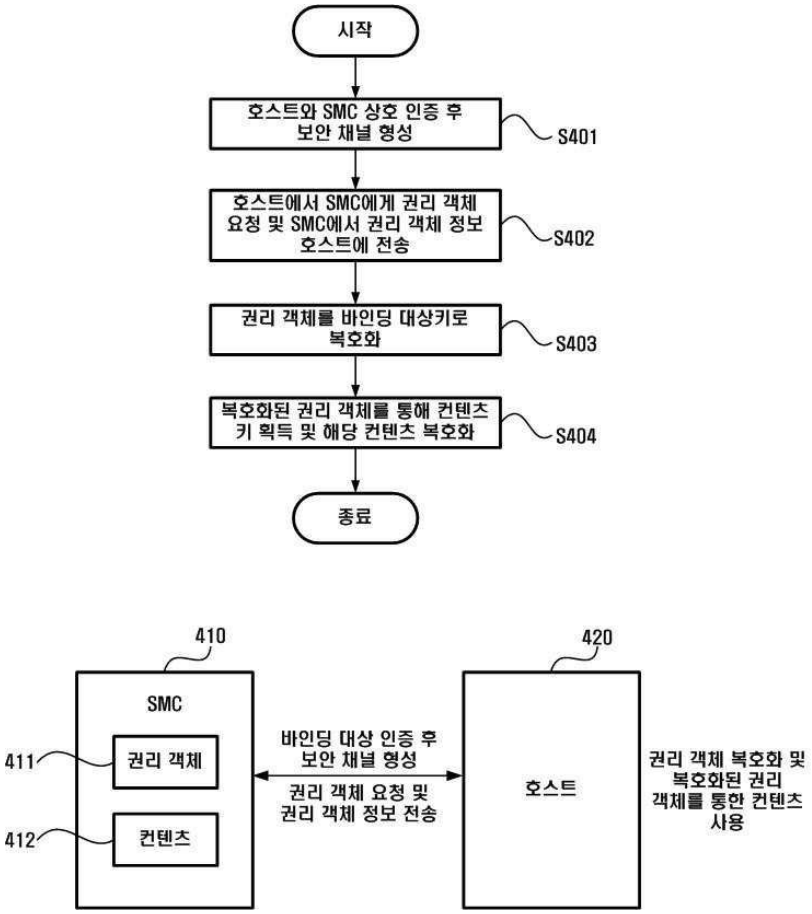
도면2


210
저작권 발급자
211
권리 객체
S201
230
SMC 제조업체
240
SMC
S202
권리 객체
211
220
컨텐츠 발급자
221
컨텐츠
S201
S202
컨텐츠
221

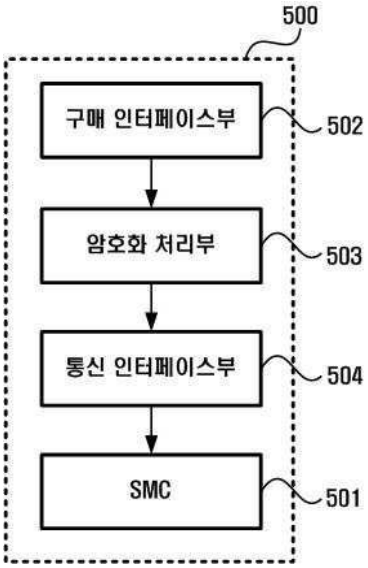
도면3


시작
컨텐츠 선택 및 결재
S301
권리 객체를 지정된 바인딩 대상키로 암호화
S302
권리 객체 및 컨텐츠 온라인 호스트에 전송
S303
SMC에 저장
S304
종료
310
저작권 발급자
311
권리 객체
네트워크 통신
330
온라인 호스트
권리 객체 (311)
컨텐츠 (321)
340
SMC
데이터 기록
권리 객체
311
데이터 기록
컨텐츠
321
320
컨텐츠 발급자
321
컨텐츠
네트워크 통신

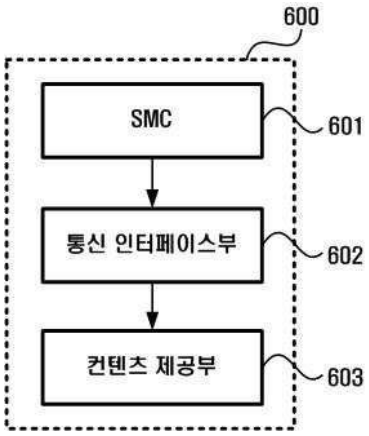
도면4


시작
호스트와 SMC 상호 인증 후 보안 채널 형성
S401
호스트에서 SMC에게 권리 객체 요청 및 SMC에서 권리 객체 정보 호스트에 전송
S402
권리 객체를 바인딩 대상키로 복호화
S403
복호화된 권리 객체를 통해 컨텐츠 키 획득 및 해당 컨텐츠 복호화
S404
종료
410
SMC
411
권리 객체
412
컨텐츠
바인딩 대상 인증 후 보안 채널 형성
권리 객체 요청 및 권리 객체 정보 전송
420
호스트
권리 객체 복호화 및 복호화된 권리 객체를 통한 컨텐츠 사용

도면5


500
구매 인터페이스부
502
암호화 처리부
503
통신 인터페이스부
504
SMC
501

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 21의 7번째 줄

【변경전】

상기 지정된 바인딩 대상키

【변경후】

지정된 바인딩 대상키