(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)
H04L 9/08 (2006.01)

(45) 공고일자 2007년04월09일
(11) 등록번호 10-0703805
(24) 등록일자 2007년03월29일

(21) 출원번호 10-2006-0014762
(22) 출원일자 2006년02월15일
심사청구일자 2006년02월15일

(65) 공개번호
(43) 공개일자

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 이재원
경기 용인시 수지구 풍덕천2동 삼성5차아파트 502동 503호

채승철
경기 수원시 영통구 영통동 벽적골9단지아파트 902동 1906호

정경임
경기 성남시 분당구 수내동 파크타운롯데아파트 128동 903호

장영숙
경기 의정부시 호원동 신도6차아파트 602동 1402호

(74) 대리인 김동진
정상빈

(56) 선행기술조사문헌
KR1020050004580 A
KR1020050096040 A
KR1020050094273 A
US20050044391 A1
* 심사관에 의하여 인용된 문헌

심사관 : 이준석

전체 청구항 수 : 총 18 항

(54) 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여사용하는 방법 및 장치

(57) 요약

본 발명은 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법 및 장치에 관한 것으로 본 발명의 일 실시예에 따른 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법은 모바일 디바이스에 일회용 인증 정보를 발급하는 단계, 원격 도메인에 포함된 비권한 디바이스로부터 상기 인증 정보와 함께 원격 인증을 요청받는 단계, 상기 비권한 디바이스에 원격 인증에 필요한 질의를 송신하는 단계, 상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하는 단계, 및 상기 비권한 디바이스의 인증을 승인하는 데이터를 상기 비권한 디바이스에 송신하는 단계를 포함한다.

대표도

도 2

특허청구의 범위

청구항 1.

모바일 디바이스에 일회용 인증 정보를 발급하는 단계;

원격 도메인에 포함된 비권한 디바이스로부터 상기 인증 정보와 함께 원격 인증을 요청받는 단계;

상기 비권한 디바이스에 원격 인증에 필요한 질의를 송신하는 단계;

상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하는 단계; 및

상기 비권한 디바이스의 인증을 승인하는 데이터를 상기 비권한 디바이스에 송신하는 단계를 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 2.

제 1항에 있어서,

상기 비권한 디바이스는 상기 원격 도메인의 대표 디바이스인, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 3.

제 1항에 있어서,

상기 모바일 디바이스의 식별자를 저장하는 단계를 더 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 4.

제 3항에 있어서,

상기 원격 인증을 요청받는 단계 이후에,

상기 인증을 요청하는 메시지 내에 저장된 식별자가 상기 모바일 디바이스의 식별자와 동일한지 확인하는 단계를 더 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 5.

제 1항에 있어서,

상기 원격 인증을 요청받는 단계 이후에,

상기 비권한 디바이스가 디바이스 해지 목록에 포함되는지 확인하는 단계를 더 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 6.

제 1항에 있어서,

상기 모바일 디바이스는 이동이 가능하며, 상기 일회용 인증 정보를 저장할 수 있는 디바이스인, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 7.

제 1항에 있어서,

상기 원격 인증 질의 또는 상기 비권한 디바이스의 인증을 승인하는 데이터는 일회용 인증 정보에 포함된 키로 암호화된, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 8.

모바일 디바이스가 원시 도메인의 대표 디바이스로부터 일회용 인증 정보를 발급받는 단계;

상기 일회용 인증 정보를 사용하여 원격 도메인의 비권한 디바이스에 원격 인증을 요청하는 단계;

상기 비권한 디바이스로부터 원격 인증 승인 결과를 수신하는 단계; 및

상기 비권한 디바이스에 임시 권리 객체를 송신하는 단계를 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 9.

제 8항에 있어서,

상기 원격 인증을 요청하는 단계 이후에,

상기 비권한 디바이스로부터 원격 인증 질의를 수신하는 단계; 및

상기 비권한 디바이스에 원격 인증 응답을 송신하는 단계를 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 10.

제 8항에 있어서,

상기 원격 인증 질의 또는 상기 원격 인증 승인 결과는 상기 인증 일회용 인증 정보에 포함된 키로 암호화된, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 11.

제 8항에 있어서,

상기 일회용 인증 정보를 발급받는 단계 이전에 상기 원시 도메인의 대표 디바이스에 모바일 디바이스의 식별자를 송신하는 단계를 더 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 12.

제 8항에 있어서,

상기 모바일 디바이스는 이동이 가능하며, 상기 일회용 인정 정보를 저장할 수 있는 디바이스인, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 13.

모바일 디바이스로부터 원격 인증을 요청하는 메시지를 수신하는 단계;

상기 메시지에 명시된 원시 도메인의 대표 디바이스 식별자를 포함하는 원격 인증 요청 메시지를 원격 도메인의 대표 디바이스에 송신하는 단계;

상기 원격 도메인의 대표 디바이스로부터 원격 인증에 필요한 질의를 수신하는 단계;

상기 질의에 대한 응답을 상기 원격 도메인의 대표 디바이스에 송신하는 단계; 및

상기 원격 도메인의 대표 디바이스로부터 인증을 승인하는 데이터를 수신하는 단계를 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 14.

제 13항에 있어서,

상기 원격 인증에 필요한 질의를 수신하는 단계 이후에, 상기 질의를 모바일 디바이스에 송신하는 단계; 및,

상기 질의에 대한 응답을 상기 모바일 디바이스로부터 수신하는 단계를 더 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 15.

제 13항에 있어서,

상기 인증을 승인하는 데이터를 수신하는 단계 이후에,

상기 모바일 디바이스에 상기 인증을 승인하는 데이터를 송신하는 단계; 및

상기 모바일 디바이스로부터 임시 권리 객체를 수신하는 단계를 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 16.

비권한 디바이스로부터 원격 인증을 요청하는 메시지를 수신하는 단계;

상기 메시지에 명시된 원시 도메인의 대표 디바이스에 원격 인증을 요청하고 상기 원격 도메인의 대표 디바이스로부터 원격 인증에 필요한 질의를 수신하는 단계;

상기 질의를 상기 비권한 디바이스에 송신하고, 상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하는 단계;

상기 질의에 대한 응답을 상기 원시 도메인의 대표 디바이스에 송신하는 단계; 및

상기 원시 도메인의 대표 디바이스로부터 인증을 승인하는 인증 승인 데이터를 수신하고, 상기 인증 승인 데이터를 상기 비권한 디바이스에 송신하는 단계를 포함하는, 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법.

청구항 17.

모바일 디바이스에 일회용 인증 정보를 발급하는 인증부;

원격 도메인에 포함된 비권한 디바이스로부터 상기 인증 정보와 함께 원격 인증을 요청받는 수신부;

상기 비권한 디바이스에 원격 인증에 필요한 질의를 송신하는 송신부; 및

상기 송신부 또는 수신부를 통해 송수신되는 데이터를 암호화 또는 복호화하는 암호/복호화부를 포함하며,

상기 수신부는 상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하며,

상기 송신부는 상기 비권한 디바이스의 인증을 승인하는 데이터를 상기 비권한 디바이스에 송신하는, 디바이스.

청구항 18.

제 17항에 있어서,

상기 인증부는 상기 일회용 인증 정보를 저장하고 삭제하는 기능을 갖으며 상기 질의를 암호화하는 키를 포함시키는, 디바이스.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 DRM 컨텐츠를 사용하는 방법에 관한 것으로, 보다 상세하게는 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법 및 장치에 관한 것이다.

디지털 컨텐츠의 자유로운 사용과 컨텐츠의 저작권을 보호하기 위한 방안으로 DRM(Digital Rights Management) 기술이 도입되고 있다. 종래에는 DRM 기술을 컨텐츠에 적용하였으나, 점차 컨텐츠의 소비 또는 사용을 제어하는 권리 객체(Rights Object)에 중점을 두고 연구되고 있다.

DRM에서 추구하는 컨텐츠의 저작권을 충족시키기 위해 권리 객체가 누구에게 귀속되는가에 따라 컨텐츠를 재생할 수 있는지를 제한할 수 있다. 예를 들어 A란 사람이 컨텐츠를 사용할 수 있도록 하는 권리 객체가 존재한다면, 이 권리 객체를 가지고 B란 사람은 해당 컨텐츠를 사용할 수 없다.

DRM에서 도메인 개념을 사용하여 특정 도메인 내의 디바이스들은 한 사람의 소유로 보아 권리 객체를 사용할 수 있도록 하고 있다. 따라서 도메인에 허용된 권리 객체는 해당 도메인 내에서는 사용할 수 있으나, 다른 도메인에서는 사용할 수 없다. 다른 도메인에서 사용하기 위해서는 별도의 권리 객체가 필요하다.

그런데 최근 무선 인터넷의 증가와 휴대용 디지털 기기의 증가로 서로 다른 도메인 사이에 모바일 노드(mobile node)의 이동으로 컨텐츠를 사용하고자 하는 경우가 발생하고 있다. 예를 들어 E도메인 내에 포함된 모바일 노드가 F 도메인으로 이동시, F 도메인 내의 디바이스에서 컨텐츠를 사용하고자 할 경우, E 도메인에서 사용가능한 권리 객체를 어떻게 사용할 것인지가 문제가 되고 있다.

또한 도메인 단위로 권리 객체가 허여되지 않은 경우에도 컨텐츠의 저작권을 침해하지 않는 범위 내에서도 다른 디바이스에서 권리 객체 취득이 용이하지 않기 때문에, DRM 시스템의 확산에 걸림돌이 되고 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 문제점을 개선하기 위해 안출된 것으로, 본 발명은 모바일 디바이스를 이용하여 권한이 없는 도메인 내의 디바이스에서 컨텐츠를 사용하는데 목적이 있다.

본 발명의 또다른 목적은 모바일 디바이스를 매개로 하여 일시적으로 다른 도메인의 디바이스에서 컨텐츠를 사용하도록 하는 것이다.

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

발명의 구성

본 발명의 일 실시예에 따른 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법은 모바일 디바이스에 일회용 인증 정보를 발급하는 단계, 원격 도메인에 포함된 비권한 디바이스로부터 상기 인증 정보와 함께 원격 인증을 요청받는 단계, 상기 비권한 디바이스에 원격 인증에 필요한 질의를 송신하는 단계, 상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하는 단계, 및 상기 비권한 디바이스의 인증을 승인하는 데이터를 상기 비권한 디바이스에 송신하는 단계를 포함한다.

본 발명의 다른 실시예에 따른 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법은 모바일 디바이스가 원시 도메인의 대표 디바이스로부터 일회용 인증 정보를 발급받는 단계, 상기 일회용 인증 정보를 사용하여 원격 도메인의 비권한 디바이스에 원격 인증을 요청하는 단계, 상기 비권한 디바이스로부터 원격 인증 승인 결과를 수신하는 단계, 및 상기 비권한 디바이스에 임시 권리 객체를 송신하는 단계를 포함한다.

본 발명의 또다른 실시예에 따른 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법은 모바일 디바이스로부터 원격 인증을 요청하는 메시지를 수신하는 단계, 상기 메시지에 명시된 원시 도메인의 대표 디바이스 식별자를 포함하는 원격 인증 요청 메시지를 원격 도메인의 대표 디바이스에 송신하는 단계, 상기 원격 도메인의 대표 디바이스로부터 원격 인증에 필요한 질의를 수신하는 단계, 상기 질의에 대한 응답을 상기 원격 도메인의 대표 디바이스에 송신하는 단계, 및 상기 원격 도메인의 대표 디바이스로부터 인증을 승인하는 데이터를 수신하는 단계를 포함한다.

본 발명의 또다른 실시예에 따른 원격 도메인의 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법은 비권한 디바이스로부터 원격 인증을 요청하는 메시지를 수신하는 단계, 상기 메시지에 명시된 원시 도메인의 대표 디바이스에 원격 인증을 요청하고 상기 원격 도메인의 대표 디바이스로부터 원격 인증에 필요한 질의를 수신하는 단계, 상기 질의를 상기 비권한 디바이스에 송신하고, 상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하는 단계, 상기 질의에 대한 응답을 상기 원시 도메인의 대표 디바이스에 송신하는 단계, 및 상기 원시 도메인의 대표 디바이스로부터 인증을 승인하는 인증 승인 데이터를 수신하고, 상기 인증 승인 데이터를 상기 비권한 디바이스에 송신하는 단계를 포함한다.

본 발명의 일 실시예에 따른 디바이스는 모바일 디바이스에 일회용 인증 정보를 발급하는 인증부, 원격 도메인에 포함된 비권한 디바이스로부터 상기 인증 정보와 함께 원격 인증을 요청받는 수신부, 상기 비권한 디바이스에 원격 인증에 필요한 질의를 송신하는 송신부, 및 상기 송신부 또는 수신부를 통해 송수신되는 데이터를 암호화 또는 복호화하는 암호/복호화부를 포함하며, 상기 수신부는 상기 질의에 대한 응답을 상기 비권한 디바이스로부터 수신하며, 상기 송신부는 상기 비권한 디바이스의 인증을 승인하는 데이터를 상기 비권한 디바이스에 송신한다.

기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 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. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다

이하, 본 발명의 실시예들에 의하여 디바이스에서 DRM 컨텐츠를 로밍하여 사용하는 방법 및 장치를 설명하기 위한 블록도 또는 처리 흐름도에 대한 도면들을 참고하여 본 발명에 대해 설명하도록 한다. 이 때, 처리 흐름도 도면들의 각 블록과 흐름도 도면들의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수 있음을 이해할 수 있을 것이다. 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 블록(들)에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 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 블록(들)에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑제되는 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 블록(들)에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

또한, 각 블록은 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실행예들에서는 블록들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

본 명세서에서 원격 도메인(external domain, remote domain)은 권리 객체를 발급받은 도메인이 아닌 도메인을 의미한다.

도 1은 본 발명의 일 실시예에 따른 원격 도메인의 디바이스에서 권리 객체를 로밍 형식으로 사용하는 경우를 보여주는 도면이다.

DRM 도메인 컨텐츠는 발급 대상 도메인의 도메인 키를 공유하고 있는 디바이스들에서만 재생이 가능하도록 권리 발급자가 권리 객체를 도메인 키로 암호화하여 발급한다. 도메인 컨텐츠를 다른 원격 도메인 디바이스에서 재생하기 위해서 원격 도메인을 원시 도메인에 인증하고, 원시 권리객체를 변환하여 원격 도메인을 위한 임시 권리 객체를 발급하는 과정이 도 1에 도시되어 있다. 이 과정에 대해 권리 발급자의 추가적인 액션 또는 발급이 개입되지 않는다.

도 1에서 컨텐츠의 발급 대상인 원시 도메인(100)에 원시 도메인 디바이스들(110, 112)이 속해 있고, 이들 중 원시 도메인 대표디바이스(110)는 원시 도메인을 관리한다. 원시 도메인 디바이스에 저장된 컨텐츠 객체(104)를 원격 도메인(150)의 디바이스(120, 122)에서 사용하려고 한다.

원격 도메인(150)의 대표 디바이스(120)를 원시 도메인의 대표 디바이스(110)에 인증을 수행하여 원시 도메인(100)의 도메인 컨텐츠에 대한 임시 권리객체(108)을 발급함에 있어서 원시 도메인 사용자의 이동 단말(130)을 매개체로 사용한다.

원시 도메인의 사용자는 원시 도메인 대표 디바이스(110)에서 발급 받은 일회용 인증정보(106)를 자신의 이동 단말(130)에 저장한 뒤 원격 도메인(150)으로 이동하여, 원격 도메인 대표 디바이스(120)에 접속하여 일회용 인증정보(106)를 이용

하여 원시 도메인 대표디바이스(110)에 인증을 수행하여, 원시 도메인의 컨텐츠에 대한 사용 승인을 받고, 임시 도메인 권리객체(108)를 발급 받고, 컨텐츠 객체(104)를 전송 받아, 원격 도메인 디바이스(122)에서 임시 도메인 권리객체(108)를 소비하여 컨텐츠를 재생한다.

사용자는 원시 도메인(100)에서 이동 단말(130)에 일회용 인증정보를 저장한 다음 원격 도메인(150)으로 이동하여 원격 도메인 디바이스(122)에서 원시 도메인 컨텐츠를 재생하기 위하여 원격 도메인 대표 디바이스(120)에 일회용 인증정보(106)를 전송하고 원격 도메인 대표 디바이스(120)은 원거리 통신을 통해 원시 도메인 대표디바이스(110)와 인증을 거쳐 이동 단말(130)에 인증 결과를 전송하여 임시 권리객체(108)을 발급 받는 것을 특징으로 한다. 도 1의 이동 단말(130)은 모바일 기기, 휴대폰, PDA, 노트북 외에도, 저장매체를 포함하는 메모리 카드도 포함된다.

도 2는 본 발명의 일 실시예에 따른 원격 도메인에서 원시 도메인의 컨텐츠를 이용하기 위한 순서를 보여주는 도면이다. 도 2에서 '||' 표시는 메시지에 부가하거나 파라메터의 값으로 송신하는 것을 의미한다.

원시 디바이스(도 1의 112)에 저장된 컨텐츠 객체(104)를 원격 도메인(150)내의 디바이스(122)에서 재생하기 위한 인증 매체로 이동 단말(130)을 사용하는 과정이 제시된다. 이동 단말(130)은 원시 대표디바이스(110)에 자신의 식별자(ID_3)와 함께 일회용 인증정보 요청 메시지(REQ_SEED)를 전송한다(S201). 원시 대표디바이스(110)에서 이동 단말(130)로 근접 통신 매체를 통해 일회용 인증정보(SEED)와 비밀키(K_3)를 전송하고, ID_3와 K_3, SEED를 자신의 저장 공간에 저장한다(S202). 이때, 근접 통신 매체를 이용하여 전송하기 때문에 별도의 보안 채널이 필요하지 않을 수 있으나 필요에 따라 보안 채널을 설정한 후 전송한다. 한편, 근접 통신 매체에서, 무선 네트워크 통신도 가능하지만, USB와 같이 접촉을 통해 데이터를 송수신할 수 있다.

사용자는 이동 단말을 휴대한 상태로 원격 도메인(150)으로 이동하여 원격 디바이스(122)에 근접 통신 매체를 통하여 원격 인증 의뢰 메시지(REQ_AUTH)와 자신의 식별자(ID_3), 원시 대표디바이스(110)의 식별자(ID_1)를 전송한다(S203). 이를 수신한 원격 디바이스(122)는 전송 받은 원격 인증 의뢰 메시지에 자신의 ID(ID_4)를 추가하여 자신의 대표디바이스(120)에 전송한다(S204).

원격 대표디바이스(120)는 S204에서 전송받은 원시 대표디바이스(110)의 식별자(ID_1)를 참조하여 원격 인증 요청 메시지를 전송한다(S205). 원시 대표디바이스(110)는 S205에서 전송받은 인증 요청 메시지를 해석하여 ID_3가 S202 단계에서 자신의 저장공간에 저장한 식별자와 일치하는지 확인하고, 디바이스 해지 목록(Certificate Revocation List)에 포함되어 있는지 여부를 확인하는 등 인증 확인에 필요한 절차를 거친다. 그리고 확인이 완료하면 인증 질의를 비밀키 K_3로 암호화하여 원격 대표디바이스(120)로 전송한다(S206). 이때, 인증 질의는 S202 단계에서 생성한 SEED 값을 의사 난수 함수의 시작값(seed)으로 입력하여 생성한 n 번째 난수를 비교하기 위하여 n 값을 인증 질의 값으로 사용할 수 있다.

원격 대표디바이스(120)는 S206 단계에서 원시 대표디바이스(110)로부터 수신한 암호화된 인증 질의를 원격 디바이스(122)로 전송한다(S207). 원격 디바이스(122)는 S207 단계에서 수신한 암호화된 인증 질의를 근접 통신 매체를 통하여 이동 단말(130)으로 전송한다(S208).

이동 단말(130)은 암호화된 인증 질의를 S202 단계에서 전송 받은 비밀키 K3로 복호화하여 질의 값을 얻어내고 사용자에게 질의문을 출력한다. 사용자는 질의문에 대한 응답값(RES)을 입력한다. 이때, S202에서 원시 대표디바이스(110)로부터 수신한 일회용 인증정보 SEED 값을 의사 난수 함수의 초기값(seed)으로 입력하여 생성한 일련의 난수값들을 출력하고, 사용자로부터 n 번째에 해당하는 난수값을 응답값(RES)로 입력받을 수 있다. 이동 단말은 사용자가 입력한 응답값(RES)을 원격 디바이스(122)로 근접 통신 매체를 통하여 전송한다(S209).

원격 디바이스(122)는 S209 단계에서 수신한 사용자의 응답값(RES)을 원격 대표디바이스(120)에 안전하게 전송한다(S210). 그리고, 원격 대표디바이스(120)는 S210에서 수신한 사용자의 응답값(RES)을 원시 대표디바이스(110)에 안전하게 전송한다(S211).

원시 대표디바이스(110)는 S211에서 전송 받은 응답값이 참인 경우 원격 디바이스(122)에서의 컨탠츠 객체(700)의 재생을 허가하여, K3를 키로하여 원격 인증 승인 메시지(GRANT)를 암호화한 후 원격 대표디바이스(120)에 전송한다 (S212). 원격 대표디바이스(120)는 S212에서 수신한 암호화된 승인 메시지를 원격 디바이스(122)에 전송한다(S213).

원격 디바이스는(122)는 S213에서 수신한 암호화된 승인 메시지를 이동 단말에 근접 통신 매체를 통하여 전송한다(S214). 이동 단말은 S214 단계에서 수신한 승인 메시지를 해석하여 승인이 확인되면 원격 디바이스(122)에 임시 도메인 권리객체(108)를 생성하여 임시 비밀키로 암호화 하여 원격 디바이스(122)에 전송한다. 임시 비밀키는 RES 값을 해쉬하여 사용한다(S215).

또는 S212 단계에서 원시 도메인 대표디바이스에서 승인 메시지와 함께 도메인 권리객체를 생성하여 전송할 수도 있다. 이 경우 S214, S215는 생략될 수 있다.

도 2의 과정에서 원격 대표 디바이스(120)가 컨텐츠를 사용하는 경우에는 원격 디바이스(122)에서 진행된 작업이 원격 대표 디바이스에서 진행될 수 있다.

도 2의 과정을 통하여 원시 대표 디바이스로(110)부터 원격 도메인(150)의 인증이 성립된 이후에는 원격 도메인(150)에 속한 적합한 도메인 디바이스들(120, 122 등)은 임시 도메인 권리객체(108)를 공유하여 사용할 수 있다.

도 3은 본 발명의 일 실시예에 따른 홈 네트워크 환경 내에서의 실행 과정을 보여주는 도면이다. 도 3에서 원시 도메인(100)을 관리하는 홈 네트워크 관리자(310)에는 권리 객체를 가지고 있으며 컨텐츠를 다른 디바이스에 송신하는 기능도 함께 가지고 있다. 도 3에서 다른 도메인(원격 도메인(150))에 속하는 제 3자의 노트북(320)에서 사용자의 컨텐츠를 재생하고자 한다. 그런데, 원격 도메인(150)에 소속된 제 3자의 노트북(320)이므로, 사용자의 홈 네트워크 관리자(310)가 소유하는 권리 객체를 직접 사용할 수는 없다. 따라서, 홈 네트워크 관리자(310)에서는 일회용 인증 정보(106)를 모바일 디바이스(330)에 전송한다.

모바일 디바이스(330)(이동 단말)는 일회용 인증 정보를 바탕으로 인증 토큰(108)을 생성하여 원격 도메인(150)에 존재하는 제 3자의 노트북(320)에 전송한다. 제 3자의 노트북(320)은 인증 토큰(108)을 사용하여 원시 도메인(100)의 홈 네트워크 관리자(310)에게 인증을 요구한다. 그리고 도 2에서 살펴본 바와 같은 과정을 통해 인증 과정을 수행하고 임시 권리 객체를 수신한다. 그 결과 사용자는 자신의 도메인 내의 디바이스가 아닌 다른 도메인에 소속된 제 3자의 노트북(320)에서도 자신의 컨텐츠를 사용할 수 있다. 한편, 제 3자의 노트북(320)에 전달되는 권리 객체는 임시 권리 객체이므로, 컨텐츠의 저작권을 해치지 않으면서, 사용의 편의성을 높일 수 있다. 이 과정에서 모바일 디바이스(330)과 제 3자의 노트북(320)과의 거리를 일정 거리 이하로 하여, 홈 네트워크 관리자(310)가 모바일 디바이스(330)의 존재를 바탕으로 노트북(320)에 대해서 인증 과정을 수행할 수 있도록 한다.

도 4는 본 발명의 일 실시예에 따른 디바이스의 구성을 보여주는 도면이다.

본 실시예에서 사용되는 '~부'라는 용어, 즉 '~모듈' 또는 '~테이블' 등은 소프트웨어, FPGA(Field Programmable Gate Array) 또는 주문형 반도체(Application Specific Integrated Circuit, ASIC)와 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 기능들을 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, 드라이버들, 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 내의 하나 또는 그 이상의 CPU들을 재생시키도록 구현될 수도 있다.

도 4에서의 디바이스는 원시 도메인을 관리하는 홈 네트워크 관리자의 기능을 수행하는 디바이스의 구성을 제시하고 있다.

디바이스(400)의 구성은 크게 송신부(410), 수신부(420), 권리객체 저장부(430), 인증부(440), 제어부(450), 그리고, 암호/복호부(460)를 포함하며, 선택적으로 출력부(470)와 입력부(480)를 포함한다. 송신부(410)는 권리 객체를 다른 디바이스에 송신한다. 또한 권리 객체뿐 아니라 인증에 관련된 정보를 송신한다. 수신부(420)는 권리 발행자로부터 권리 객체를 수신하며, 인증시 다른 디바이스가 전송하는 데이터를 수신하여 처리한다.

송신부(410)와 수신부(420)는 독립적으로 존재할 수 있으며, 결합하여 존재할 수 있다. 통상 권리 객체는 물리적 접촉 또는 네트워크에 의해 송수신된다.

권리객체 저장부(430)는 수신한 권리 객체를 저장한다. 저장한 권리 객체는 다른 디바이스에 전송할 수 있으며, 또한 임시 권리 객체를 생성하여 저장할 수 있다. 권리객체 저장부(430)는 이외에도 인증에 필요한 디바이스에 대한 정보를 함께 저장할 수 있다. 예를 들어 해당 권리객체를 수신할 디바이스의 식별자에 대한 정보도 함께 저장할 수 있다.

인증부(440)는 다른 디바이스와의 인증 과정을 처리한다. 전술한 바와 같이, 모바일 단말에서 일회용 인증 정보를 요청하는 경우, 일회용 인증 정보를 발급하는 작업과 원격 인증 요청에 따른 질의 생성, 원격 인증의 승인 등을 처리한다. 따라서, 미리 저장된 디바이스의 식별자를 사용할 수 있으며, 인증을 위한 초기값(Seed)를 생성할 수 있다. 한편, 원격 인증에 성공하면 권리객체 저장부(430)에 저장된 권리 객체를 송신하도록 제어부(450)에 요청할 수 있다.

제어부(450)는 상기의 각 구성요소들이 상호작용 할 수 있도록 제어한다. 한편, 인증 과정에서 발생하는 여러 계산과정들, 예를 들어, 인증 값의 비교, 질의문 생성 등에서 필요로하는 산술적인 과정들을 제어할 수 있다. 암호/복호부(460)는 인증부(440) 또는 송신부(410), 수신부(420)에서 처리하는 데이터의 암호화와 복호화를 담당한다.

출력부(470)와 입력부(480)는 사용자와의 인터페이스를 처리하고 멀티미디어 컨텐츠를 보여주는 기능을 수행한다.

한편 도 4의 구성을 모바일 디바이스의 구성으로 할 수 있다. 이때, 송신부(410) 또는 수신부(420)는 도 3의 원격 도메인에 소속된 제 3자의 노트북과 같은 비권한 디바이스와 물리적 거리를 측정하는 기능을 함께 제공할 수 있다.

도 5는 본 발명의 일 실시예에 따른 디바이스에서 권리 객체를 로밍하여 제공하는 순서도이다. 본 순서도에서 비권한 디바이스는 컨텐츠를 재생하고자 하는 원격 도메인 내의 디바이스로, 도 1, 2의 디바이스(120, 122), 또는 도 3에서의 제 3자의 노트북(320) 등이 비권한 디바이스에 해당한다.

홈 네트워크를 관리하는 디바이스(원시 도메인의 대표 디바이스)는 모바일 디바이스(이동 단말)에 일회용 인증 정보를 발급한다(S510). 일회용 인증 정보를 발급하면서, 모바일 디바이스에 대한 정보를 저장할 수 있다. 일회용 인증 정보를 발급받은 모바일 디바이스는 일회적으로 컨텐츠를 재생하고자 하는 원격 도메인에 소속된 비권한 디바이스에 대해 비권한 디바이스에 원격 인증 의뢰를 요청하면, 비권한 디바이스 측에서 원격 인증 요청을 수행한다. 따라서 디바이스는 원격 도메인 내의 비권한 디바이스 측으로부터의 원격 인증 요청을 수신한다(S520). 이때 원격 도메인 내에 컨텐츠를 재생하고자 하는 디바이스가 대표 디바이스가 아닌 경우, 이러한 원격 인증 요청은 비권한 디바이스에서 원격 대표 디바이스로 전달되어서 원시 대표 디바이스로 전송된다. 이는 도 2의 S204와 S205 과정을 통해 알 수 있다.

수신한 원격 인증 요청에 포함된 모바일 디바이스의 식별자가 S510 단계에서 저장한 모바일 디바이스의 정보와 일치하는지 비교하여, 원격 도메인 내의 비권한 디바이스에 원격 인증 질의를 전송한다(S530). 마찬가지로, 원격 도메인 내의 디바이스가 원격 대표 디바이스를 통해 질의를 전송한 경우에, 도 2dml S206과 S207 단계를 거쳐서 질의가 전송된다.

여기서 모바일 디바이스의 식별자가 함께 포함되어 있으므로, 비권한 디바이스에 대해 인증을 수행해도 되기 때문에, 비권한 디바이스에 원격 인증 질의를 전송하게 된다.

비권한 디바이스가 모바일 단말을 통해 원격 인증 질의에 대한 응답을 받은 후, 비권한 디바이스는 수신한 응답을 다시 원시 도메인의 대표 디바이스에 송신하게 된다. 따라서 원시 도메인의 대표 디바이스는 원격 인증 질의에 대한 응답을 수신하고(S540), 이 응답에 따라 원격 인증 승인을 원격 도메인 내의 비권한 디바이스에 대해 수행한다(S550). 그리고 비권한 디바이스는 이에 따라 모바일 디바이스에 원격 인증 승인을 받았음을 알리고, 임시 권리 객체를 부여받아서 컨텐츠를 소비 또는 사용하게 된다.

도 6A와 6B는 종래의 방식과 본 명세서에서 제시한 방식을 비교하는 도면이다. 도 6A에서 사용자가 원격 도메인(150)의 권한이 없는 디바이스(622)에서 컨텐츠를 재생하기 위해서는 권리 발행자(680)로부터 인증을 수행하고 권리 객체를 수신하는 과정을 수행하였다. 따라서 원시 도메인의 홈 네트워크 관리자(612)의 개입이 존재하지 않았다. 대신, 일회적인 컨텐츠의 재생에도 권리 발행자(680)로부터 인증을 받는 과정을 필요로 하므로 컨텐츠 사용의 편의성이 감소된다.

반면, 본 명세서에서 제시한 방법에 따르는 도 6B의 경우 사용자는 원시 도메인에 소속된 모바일 디바이스(634)에 일회용 인증정보(106)를 저장한다. 그리고 이 모바일 디바이스(634)를 이동시켜서 다른 원격 도메인 내에 존재하는 디바이스(624)의 주변에 근접시킨다. 이때, 제 3의 디바이스(624)와 일정 거리 이하로 다가간 경우에만 모바일 디바이스(634)를 통해 로밍이 가능하도록 정의할 수 있다. 두 디바이스간의 거리 측정은 무선 네트워크 또는 적외선 통신 등을 통해 가능하다. 제 3의 디바이스(624)는 권리 발행자(680)가 아닌 원시 도메인의 대표 디바이스인 홈 네트워크 관리자(614)와 인증을

수행하고, 컨텐츠를 사용할 수 있다. 또한, 컨텐츠를 일시적으로만 재생할 수 있도록 제한을 가하여, 컨텐츠 제공자의 이익을 보호할 수 있다. 한편, 624 디바이스가 원격 도메인(150)의 대표 디바이스인 경우, 원격 도메인 내의 다른 디바이스(628)가 컨텐츠를 사용할 수 있도록 할 수 있다.

도 6에서의 모바일 디바이스(634)는 반드시 휴대폰과 같은 통신 기기에만 한정되지 않는다. 플래시 메모리가 내장된 이동형 저장장치도 가능하며, 노트북, PDA 등 저장 매체를 포함하는 디지털 디바이스도 가능하며, 메모리 카드도 이에 포함된다. 본 명세서에서의 모바일 디바이스(634)는 이동이 용이한 디바이스로, 일회용 인증 정보를 저장하는 저장부를 포함하는 모든 디바이스를 통칭한다.

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. 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

본 발명을 구현함으로써 사용자는 자신이 구입한 컨텐츠를 컨텐츠 발급 대상 도메인 내의 디바이스가 아닌 원격 도메인에 소속된 디바이스에서 발급 대상인 원시 도메인의 대표 디바이스의 도움을 받아 적법하게 인증받을 수 있다.

본 발명을 구현함으로써 원격 도메인에 소속된 디바이스에 적절한 재생 권리를 부여함으로써, 사용자의 편의성을 증대시키며, 또한 컨텐츠의 무분별한 유포를 제한하여 컨텐츠 제공자의 이익을 해치지 않을 수 있다.

도면의 간단한 설명

도 1은 본 발명의 일 실시예에 따른 원격 도메인의 디바이스에서 권리 객체를 로밍 형식으로 사용하는 경우를 보여주는 도면이다.

도 2는 본 발명의 일 실시예에 따른 원격 도메인에서 원시 도메인의 컨텐츠를 이용하기 위한 순서를 보여주는 도면이다.

도 3은 본 발명의 일 실시예에 따른 홈 네트워크 환경 내에서의 실행 과정을 보여주는 도면이다.

도 4는 본 발명의 일 실시예에 따른 디바이스의 구성을 보여주는 도면이다.

도 5는 본 발명의 일 실시예에 따른 디바이스에서 권리 객체를 로밍하여 제공하는 순서도이다.

도 6A와 6B는 종래의 방식과 본 명세서에서 제시한 방식을 비교하는 도면이다.

<도면의 주요 부분에 대한 부호의 설명>

100: 원시 도메인 102: 권리객체

104: 컨텐츠 객체 106: 일회용 인증정보

110: 원시 도메인의 대표 디바이스 112: 원시 도메인의 디바이스

120: 원격 도메인의 대표 디바이스 122: 원격 도메인의 디바이스

150: 원격 도메인 400: 디바이스

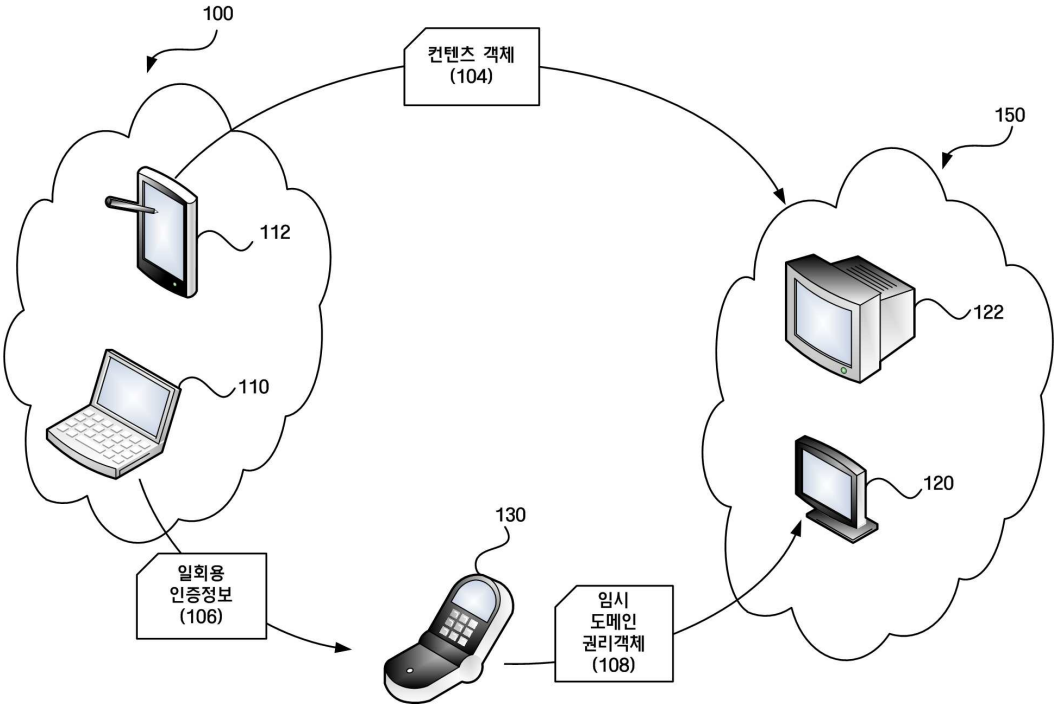
410: 송신부 420: 수신부

430: 권리객체 저장부 440: 인증부

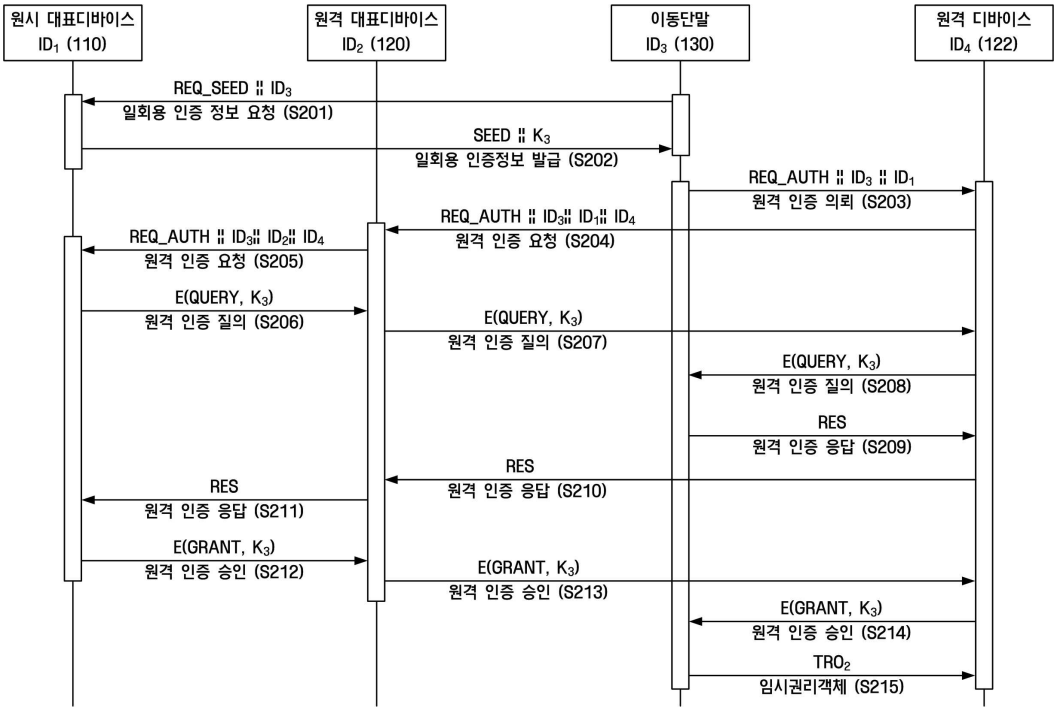
450: 제어부 460: 암호/복호부

도면

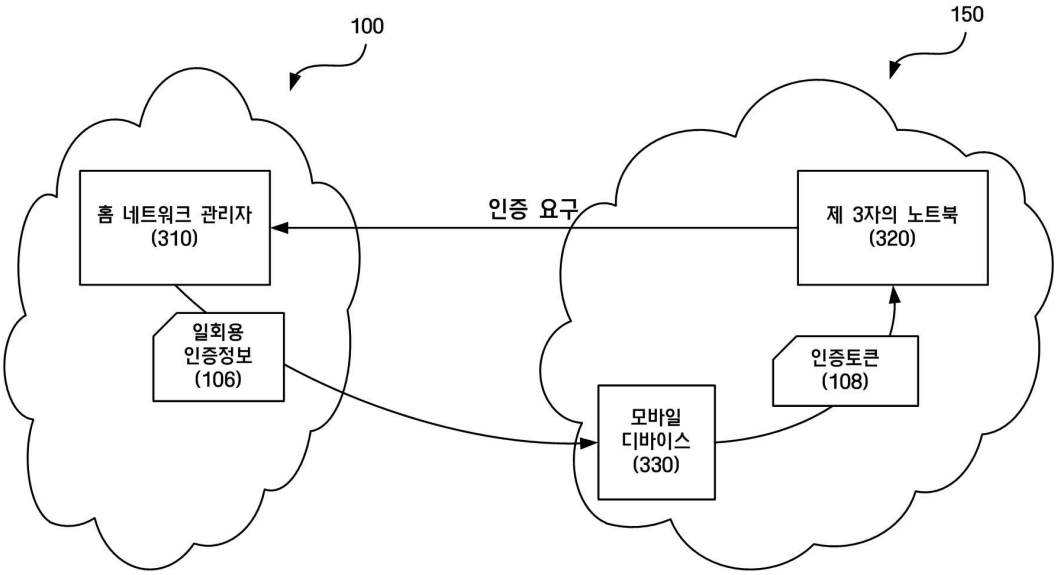
도면1



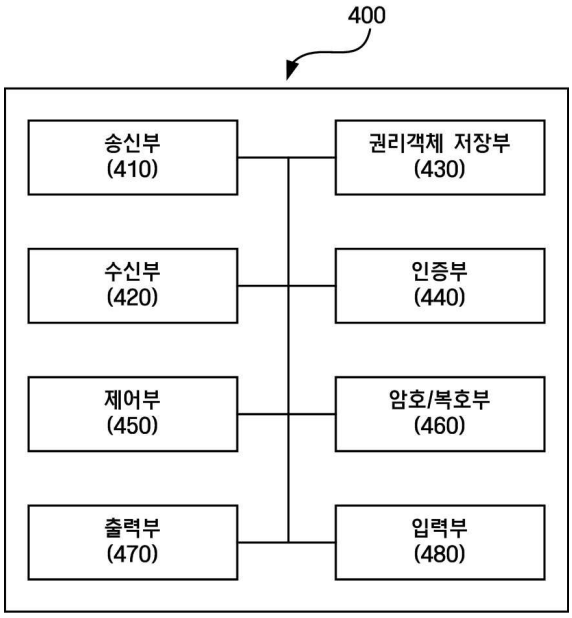
도면2



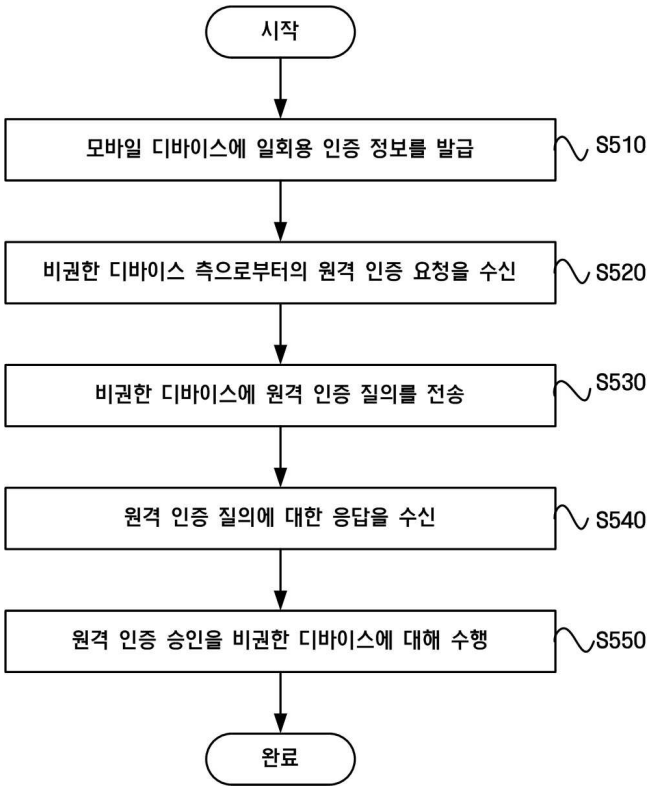
도면3


100
150
홈 네트워크 관리자
(310)
인증 요구
제 3자의 노트북
(320)
일회용
인증정보
(106)
인증토큰
(108)
모바일
디바이스
(330)

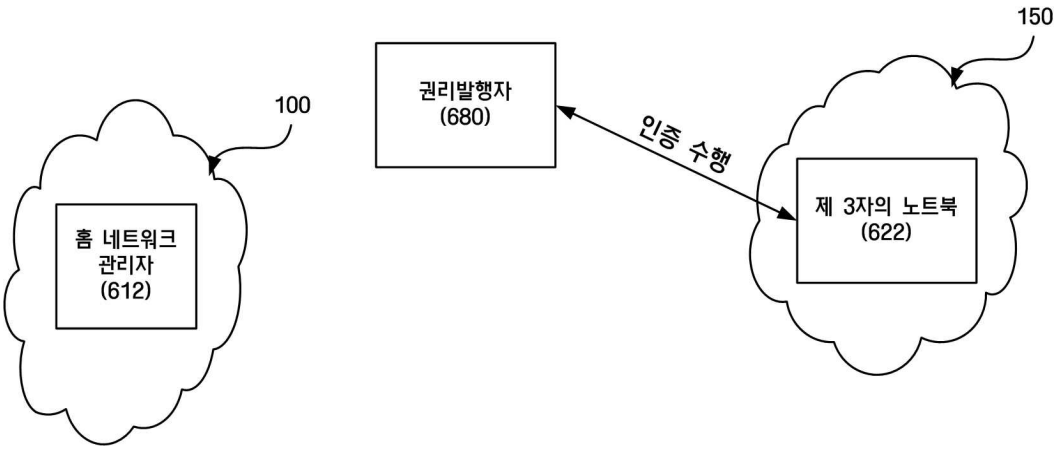
도면4


400
송신부
(410)
권리객체 저장부
(430)
수신부
(420)
인증부
(440)
제어부
(450)
암호/복호부
(460)
출력부
(470)
입력부
(480)

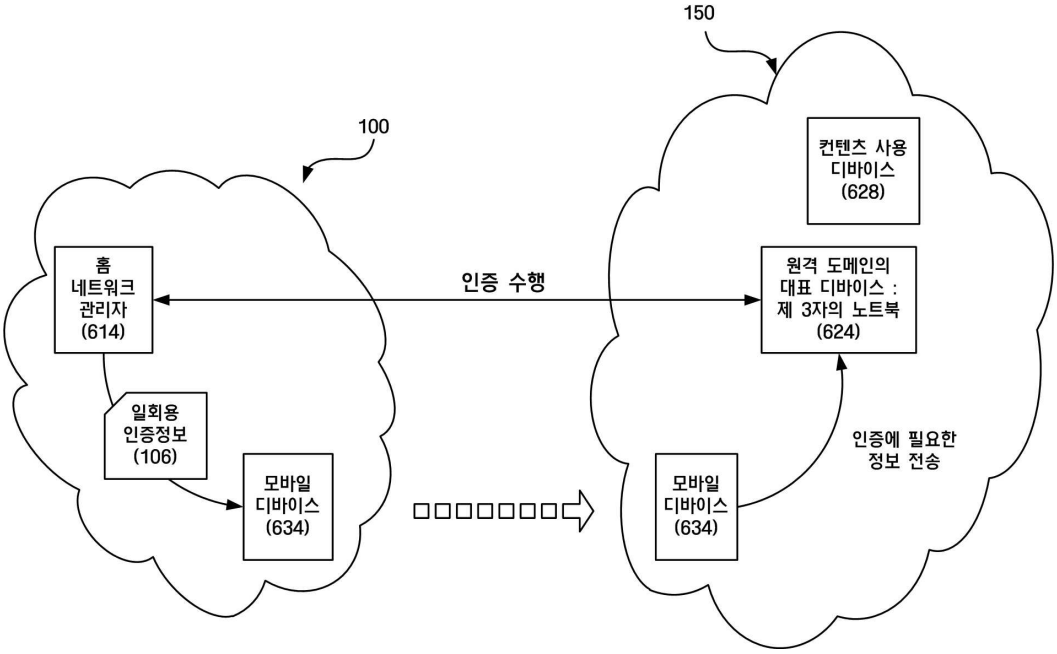
도면5


시작
모바일 디바이스에 일회용 인증 정보를 발급
S510
비권한 디바이스 측으로부터의 원격 인증 요청을 수신
S520
비권한 디바이스에 원격 인증 질의를 전송
S530
원격 인증 질의에 대한 응답을 수신
S540
원격 인증 승인을 비권한 디바이스에 대해 수행
S550
완료

도면6a


100
홈 네트워크
관리자
(612)
권리발행자
(680)
인증 수행
150
제 3자의 노트북
(622)

도면6b


150
100
컨텐츠 사용
디바이스
(628)
홈
네트워크
관리자
(614)
인증 수행
원격 도메인의
대표 디바이스 :
제 3자의 노트북
(624)
일회용
인증정보
(106)
모바일
디바이스
(634)
모바일
디바이스
(634)
인증에 필요한
정보 전송