(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년02월08일
(11) 등록번호 10-2497208
(24) 등록일자 2023년02월02일

(51) 국제특허분류(Int. Cl.)
H04N 21/266 (2011.01) *H04N 21/418* (2011.01)
H04N 21/4623 (2011.01) *H04N 21/6334* (2016.01)
H04N 7/167 (2011.01)
(52) CPC특허분류
H04N 21/26606 (2013.01)
H04N 21/4181 (2013.01)
(21) 출원번호 10-2019-7035828
(22) 출원일자(국제) 2018년05월03일
심사청구일자 2021년03월12일
(85) 번역문제출일자 2019년12월03일
(65) 공개번호 10-2020-0004353
(43) 공개일자 2020년01월13일
(86) 국제출원번호 PCT/EP2018/061332
(87) 국제공개번호 WO 2018/202768
국제공개일자 2018년11월08일
(30) 우선권주장
17169830.1 2017년05월05일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
US06424717 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
나그라비젼 에스에이알엘
스위스 체하-1033 세조-쉬르-로잔느 루뜨 드 쥬네브 22-24
(72) 발명자
후나첵 디디에르
스위스1033 세조-쉬르-로잔느 루뜨 드 쥬네브 22-24 나그라비젼 에스에이 씨/오
피셔 진-버나드
스위스1033 세조-쉬르-로잔느 루뜨 드 쥬네브 22-24 나그라비젼 에스에이 씨/오
(74) 대리인
박장원

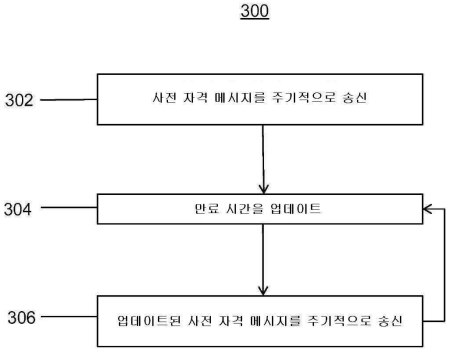
전체 청구항 수 : 총 8 항 심사관 : 김건우

(54) 발명의 명칭 **사전 자격 수행**

(57) 요 약

액세스 제어 시스템에서 자격 메시지들을 콘텐츠 소비 디바이스들로 전송하는 방법으로서, 상기 방법은, 액세스 제어 시스템에서 자격 메시지들을 콘텐츠 소비 디바이스에 주기적으로 전송하는 단계 및 상기 자격 메시지들에 포함된 만료 시간을 주기적으로 연장하는 단계를 포함한다. 상기 자격 메시지들은 지시자 데이터를 포함하고, 상기 지시자 데이터는, 제1 자격 메시지가 콘텐츠 소비 디바이스에 로딩된 후에 콘텐츠 소비 디바이스에 로딩된 후속 자격 메시지가 콘텐츠 소비 디바이스에 의해 보호된 미디어 콘텐츠에 액세스하는데 사용되지 않아야 함을 나타낸다.

대 표 도 - 도3



(52) CPC특허분류
H04N 21/4623 (2019.01)
H04N 21/63345 (2013.01)
H04N 7/1675 (2013.01)

명 세 서

청구범위

청구항 1

액세스 제어 모듈로서,

상기 액세스 제어 모듈은 회로를 포함하고, 상기 회로는:

주기적으로 전송되는 보안 메시지인 제1 자격 메시지를 수신하고, 상기 제1 자격 메시지는, 만료 시간을 포함하는 자격 데이터, 만료 시간까지 보호된 미디어 콘텐츠에 액세스를 가능하게 하는 액세스 데이터, 및 지시자 데이터를 포함하며,

자격 데이터가 이미 저장되어 있는지를 확인하여, 자격 메시지가 제1 수신된 자격 메시지인지를 결정하고,

상기 제1 수신된 자격 메시지의 자격 데이터를 메모리에 저장하고,

현재 시간 및 디스크램블링 키를 포함하는 액세스 정보를 수신하고,

상기 현재 시간을 상기 만료 시간과 비교하고, 상기 디스크램블링 키를 상기 액세스 데이터의 암호 해독 키로 암호 해독하고, 그리고 긍정적인 비교에 응답하여 상기 보호된 미디어 콘텐츠에 대한 액세스 권한을 부여하고,

후속 자격 메시지를 수신하며,

상기 후속 자격 메시지가 상기 제1 자격 메시지에 포함된 지시자 데이터에 포함된 만료 시간 식별자와 일치하는 만료 시간 식별자를 포함하는 경우, 상기 후속 자격 메시지에 포함되는 만료 시간에 기초하여 상기 만료 시간을 업데이트하고, 상기 만료 시간 식별자는 카운트 값이며, 그리고

상기 제1 수신된 자격 메시지의 자격 데이터가 상기 메모리에 저장된 경우 그리고 상기 후속 자격 메시지가 상기 제1 자격 메시지의 지시자 데이터에 포함된 만료 시간 식별자와 일치하는 만료 시간 식별자를 포함하지 않는 경우, 상기 후속 자격 메시지를 거절하도록 구성되는 것을 특징으로 하는

액세스 제어 모듈.

청구항 2

제1항에 있어서,

상기 자격 데이터는 상기 만료 시간에 고유한 식별자를 포함하는 것을 특징으로 하는

액세스 제어 모듈.

청구항 3

제2항에 있어서,

상기 회로는:

1회 프로그래밍 가능한 메모리에 식별자의 검증을 가능하게 하는 검증 데이터를 저장하고;

자격 데이터를 사용하여 미디어 콘텐츠에 액세스하기 전에, 상기 자격 데이터의 식별자가 상기 검증 데이터와 일치하는지를 결정하고; 그리고

상기 자격 데이터의 식별자가 상기 검증 데이터와 일치하지 않는 경우, 상기 자격 데이터를 사용하여 미디어 콘텐츠에 액세스하는 것을 방지하도록 더 구성되는 것을 특징으로 하는

액세스 제어 모듈.

청구항 4

제1항에 있어서,

상기 회로는, 상기 자격 데이터를 휘발성 메모리에 저장하도록 더 구성되는 것을 특징으로 하는

액세스 제어 모듈.

청구항 5

제1항에 있어서,

상기 회로는:

상기 자격 데이터를 1회 프로그래밍 가능한 메모리에 저장하고, 그리고

상기 1회 프로그래밍 가능한 메모리에 저장되지 않은 지시자 데이터를 포함하는 자격 데이터의 사용을 방지하도록 더 구성된 것을 특징으로 하는

액세스 제어 모듈.

청구항 6

제3항에 있어서,

상기 회로는:

상기 1회 프로그래밍 가능한 메모리에 데이터를 저장할 때 상기 1회 프로그래밍 가능한 메모리를 비가역적으로 물리적으로 변경하도록 더 구성된 것을 특징으로 하는

액세스 제어 모듈.

청구항 7

제1항에 있어서,

상기 회로는:

상기 자격 데이터를 수신할 때, 지시자 데이터를 포함하는 이전의 자격 데이터가 상기 액세스 제어 모듈에 저장된 후에 상기 자격 데이터가 수신되었는지를 결정하고, 그리고

상기 결정이 긍정인 경우 상기 결정에 응답하여 상기 자격 데이터의 저장을 방지하거나 또는 상기 자격 데이터를 삭제하도록 더 구성되는 것을 특징으로 하는

액세스 제어 모듈.

청구항 8

콘텐츠 소비 디바이스로서,

제3항에 따른 상기 액세스 제어 모듈과;

보호된 콘텐츠 및 자격 메시지들을 수신하는 수신기와;

상기 액세스 데이터로부터 도출된 제어 데이터를 사용하여 상기 보호된 콘텐츠를 디스크램블링하는 디스크램블러(descrambler)와; 그리고

상기 디스크램블링된 콘텐츠로부터 비디오 신호를 생성하는 비디오 프로세서를 포함하는 것을 특징으로 하는

콘텐츠 소비 디바이스.

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은, 방송 미디어 콘텐츠에 대한 액세스를 허가하는 것에 관한 것으로, 특히, 콘텐츠 소비 디바이스의 최초 활성화시 컨텐츠 소비 디바이스에 설치된 자격들을 사용하는 것에 관한 것이다.

배 경 기 술

[0002] 조건부 액세스 시스템(CAS)을 통해 방송 서비스 제공자들, 특히, 디지털 방송 서비스 제공자들은 구독 채널들, 서비스들 또는 방송 이벤트들 또는 프로그램들과 같은 콘텐츠를 서비스 제공 업체의 가입자로 제한할 수 있다. 콘텐츠는, 수신기 (예를 들어, 셋톱 박스(STB))가 콘텐츠를 디스크램블링하여 볼 수 있게 하는 암호화된 제어 워드(CW)와 함께 스크램블링된 형태로 방송된다. CW는 일반적으로 콘텐츠 스트림에 암호화된 CW, 날짜 및/또는 시간 및 콘텐츠를 보는 데 필요한 자격의 표시(예를 들어, 가입 레벨)를 포함하는 자격 제어 메시지(ECM)의 콘텐츠 스트림에 배포된다. 또한, CAS는 일반적으로 자격 관리 메시지(EMM)를 전송하고, 그리고 상기 자격 관리 메시지는, CW를 해독하고 그리고 콘텐츠 액세스를 제어하는 STB에서 자격 조건들(예를 들어, 해당 구독 수준/패키지, 만료 날짜 등)을 설정하기 위한 암호 해독 키를 포함한다. 대안적으로, EMM은 권리들을 포함하고, 그리고 해독키는, 예를 들어, 제조 시간 또는 스마트카드 또는 펌웨어 업데이트를 통해 STB에 개별적으로 저장된다. CW는 짧은 간격으로(예를 들어, 2초마다) CAS에 의해 변경되므로, 필요한 자격이 없거나 만료된 경우 CW를 올바르게 해독하지 못하면 디스크램블링이 실패한다. 이러한 방식으로, 콘텐츠는 필요한 자격이 STB에서 유효한 경우에만 실질적으로 액세스 가능하다. CAS는 일반적으로 STB에 삽입할 수 있는 스마트 카드를 사용하며 그리고 명확한 형식으로 CW에 액세스할 수 있고 디스크램블링을 가능하게하는 가입자 세부 사항들을 포함한다. 보다 최근에는, 일부 STB들이 스마트 카드없이 CAS를 구현하며 그리고 원격으로 구성할 수 있는 소프트웨어 환경에서 콘텐츠 소비 권한이 처리된다. 지리적 위치에 따라 상이한 표준(예를 들어, 유럽에서 주로 적용되는 DVB 표준)을 사용하는 여러 가지 CAS 구현들이 존재한다.

[0003] 사용자가 새 스마트 카드를 구매할 때, 스마트 카드에는 종종 설치된 후 하나 이상의 기본 자격을 설정하는 루틴이 제공된다. 자격은 특정 서비스 오퍼링에 대한 액세스(예를 들어, 스마트 카드가 처음 설치된 시점부터 제한된 기간 동안 서비스 제공 업체가 제공한 모든 채널에 대한 액세스)를 제공한다. 이를 통해 신규 고객은 계정을 설정하는 동안 오퍼링을 샘플링하고 액세스할 수 있다. 이를 위해, 스마트 카드는, 활성화될 때 자격을, 활성화 날짜 이후 사전 정의된 기간의 만료 날짜와 함께 설정하도록 구성된다. 이 메커니즘은 스마트 카드에서 잠복 상태를 유지하므로, 공격자가 사전 권한의 만료 날짜를 갱신하기 위해 정기적으로 설정된 사전 권한을 다시 실행하는 것을 통해 공격 경로의 관점에서 보안 취약점을 나타낸다. 이러한 위험은 강력한 보안을 제공할 수 있는 스마트 카드와 관련하여 수용 가능할 수 있지만, 스마트 카드없이 STB에 의존하는 CAS와 관련하여 훨씬 더 중요하다. 이러한 디바이스는 소프트웨어에서 사전 자격 설정 루틴을 실행하므로 이러한 유형의 공격에 훨씬 더 취약하다.

도면의 간단한 설명

[0004] 도 1a는 조건부 액세스 시스템의 개략도를 도시한다.

도 1b는 사전 자격 메시지의 개략도를 보여준다.

도 2는 일 실시예에 따른 콘텐츠 소비 디바이스의 블록도를 도시한다.

도 3은 일 실시예에 따른 자격 메시지들을 콘텐츠 소비 디바이스로 전송하는 방법을 도시한다.

도 4는 수신된 자격 정보를 저장하는 제1 방법을 도시한다.

도 5는 수신된 자격 정보를 저장하는 제2 방법을 도시한다.

도 6은 저장된 자격을 사용하여 보호된 미디어 콘텐츠에 액세스하는 방법을 도시한다.

도 7은 일 실시예에 따른 조정된 자격 메시지들을 콘텐츠 소비 디바이스들로 전송하는 방법을 도시한다.

도 8은 일 실시예에 따른 조정된 자격 메시지들을 콘텐츠 소비 디바이스들로 전송하는 다른 방법을 도시한다.

도 9는 컴퓨팅 디바이스의 일 구현의 블록도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0005] 개요에서, 액세스 제어 시스템(ACS)이 전술한 라인들을 따라 사전 자격 기능을 제공할 수 있게 하는 자격 메시지 및 액세스 제어 모듈(ACM)을 전송하는 방법들이 개시된다. 이 방법들은 ACM(또는 새로운 ACM)을 통합한 새로운 콘텐츠 소비 디바이스가 제한된 기간 동안 처음 사용하는 콘텐츠에 액세스할 수 있는 기본 자격을 사용자에게 제공할 수 있게 하고, 이는 고정된 만료 시간으로 전송되는 자격 메시지들에 기초하여 개선된 보안성을 갖고, 그리고 예를 들어, 주기적으로 만료 시간을 업데이트하여 각각의 전송된 메시지에 대한 전송 날짜에 대해 정의된 유효 기간을 제공한다. 용어 ACS 및 ACM은 본 명세서에서 미디어 콘텐츠에 대한 액세스를 제어하는 시스템들 및 모듈들을 지칭하는 것으로 사용됨이 이해될 것이다. 조건부 액세스 시스템(CAS) 또는 조건부 액세스 모듈(CAM)과 같은 미디어 콘텐츠 액세스 제어 분야에서 확립된 의미를 가질 수 있는 특정 용어들이 본 발명에서 사용되는 경우, 이들 용어들은 당업자가 이해한 확립된 의미를 갖는한 예시들로서 사용됨을 이해할 것이다. 일부 구현들에서, ACM은 CAM일 수 있고 그리고/또는 ACS는 당업계에 일반적으로 이해되는 바와 같이 CAS일 수 있다.

[0006] 제1 양상에서, ACS에서 자격 메시지를 전송하는 방법이 개시된다. 자격 메시지는, 만료 시간 및 만료 시간까지 보호된 미디어 콘텐츠에 액세스할 수 있는 액세스 데이터, 예를 들어, 암호화된 CW들 및/또는 다른 데이터를 해독하여 액세스할 수 있는 키, 예를 들어, ACM이 콘텐츠 아이템에 대한 액세스 권한을 부여할 수 있는지 여부를 결정할 수 있는 구독 레벨 또는 카테고리의 표시를 포함한다. 자격 메시지는, 또한, 예를 들어, 제1 자격 메시지의 만료 시간이 무단으로 연장되는 것을 방지하기 위해 로딩 또는 설치를 방지해야 하므로, 제1 자격 메시지가 수신 ACM에 의해 처리된 후, 수신 ACM에 의해 수신된 후속 자격 메시지들을 사용하는 것을 수신 콘텐츠 소비 디바이스에 표시하는 지시자 데이터를 포함한다. 이러한 만료 시간, 액세스 및 지시자 데이터를 포함하는 자격 메시지들은 간략화 및 설명의 명확성을 위해 다음의 사전 자격 메시지들로 지칭될 것이다. 마찬가지로, 이러한 만료 시간, 액세스 및 지시자 데이터를 포함하는 사전 자격 메시지들의 데이터는 이하에서 사전 자격 데이터로 지칭될 것이다.

[0007] 이 방법은 사전 자격 메시지를 주기적으로 전송하는 단계, 보호된 콘텐츠에 대한 액세스가 활성화되는 유효 기간을 유지하기 위해 사전 자격 메시지의 만료 시간 업데이트하는 단계, 및 업데이트된 만료 시간과 함께 사전 자격 메시지를 주기적으로 전송하는 단계를 포함한다. ACS는, 예를 들어, 보호된 콘텐츠를 방송하는 방송 시스템 일 수 있고, 그리고 사전 자격 메시지들은, 예를 들어, 적합한 프로토콜(예를 들어, 직교 진폭 변조(QAM), 코딩된 직교 주파수 도메인 멀티 플렉스(COFDM), 직교 위상 편이 변조(QPSK), 디지털 비디오 방송-위성-2세대 DVB-S2, 비동기식 직렬 인터페이스(ASI), 인터넷 프로토콜 텔레비전(IP-TV 등)을 사용하여 케이블 및 위성을 통해 또는 공중으로 방송될 수 있다. 사전 자격 메시지들은, 예를 들어 데이터 캐러셀에서 또는 브로드 캐스트 스트림의 일부로서, 예를 들어, ACS를 운영하는 서비스 제공자의 하나 이상의 브로드 캐스트 채널에서 수초마다, 예를 들어, 10초마다 전송될 수 있다. ACS가 여러 서비스 제공자들 또는 최근 ACM들 또는 가입자들에게 서비스를 제공하는 경우, ACM 일련 번호들 또는 가입자 식별자들의 범위에 따라 결정될 수 있듯이, 사전 자격 메시지는 복수의 ACM들, 예를 들어, ACM들의 그룹, 예를 들어, 특정 서비스 제공자와 관련된 것들에 어드레스될 수 있다. 대안적으로, 사전 자격 메시지는 ACS 내의 임의의 및 모든 ACM들 또는 지정된 콘텐츠 소비 디바이스 또는 ACM들의 세트로 어드레스될 수 있다. 물론, 사전 자격 메시지는 새로운 만료 시간으로 반복적으로

업데이트되고, 사전 자격 메시지들에 대한 유효한 이동 윈도우를 생성하기 위해 업데이트들 사이에 주기적으로 전송될 수 있음을 이해할 것이다.

[0008] 일부 실시예들에서, 사전 자격 메시지는 메시지의 만료 시간에 특정한 식별자를 포함한다. 이는, 후술하는 바와 같이 사전 자격 메시지들을 보다 유연하게 사용할 수 있게 하며, 특히, 이전에 전송된 사전 자격 메시지의 초기 만료 시간 또는 이전에 전송된 사전 자격 메시지의 다른 업데이트를 연장할 수 있게 한다. 특히, 이것은 이전에 전송된 자격 메시지의 초기 만료 시간보다 늦게 연장된 만료 시간으로 업데이트된 자격 메시지를 전송함으로써 (또는 서비스 추가와 같은 상이한 서비스들의 세트에 대한 업데이트된 자격으로)달성될 수 있지만, 아래에서 더 설명되는 것처럼 이전에 전송된 메시지의 식별자는 갖는다. 식별자는 지시자 데이터의 일부일 수 있거나, 또는 지시자 데이터는, 예를 들어, 지시를 제공하는 정의된 데이터 필드에 0이 아닌 식별자 값의 존재와 함께 식별자로 구성될 수 있음도 또한 이해될 것이다. 대안적으로, 식별자는 별도의 데이터 아이템일 수 있다. 어떤 경우에도, 식별자는, 예를 들어, 사전 자격 메시지의 만료 시간, (초기) 만료 시간 자체 또는 (초기) 만료 시간 자체에 특정한 다른 식별자가 업데이트될 때마다 증가하는 일련번호일 수 있고, 따라서, (초기) 만료 시간을 갖는 사전 자격 메시지를 상이한 (초기) 만료 시간을 갖는 다른 사전 자격 메시지들과 구별할 수 있다.

[0009] 일부 실시예들에서, 식별자는 만료 시간이 아닌 메시지 전체에 고유하므로 동일한 메시지들의 리로딩(re-loading)만 가능하다. 어느 경우이든, 아직 만료되지 않은 모든 사전 자격 메시지들은 주기적으로 재전송되어 수신기에서 수신된 제1 로딩된 사전 자격 메시지의 리프레시, 복원 또는 수정을 가능하게 한다. 일부 실시예들에서, 사전 자격 메시지 또는 사전 자격 데이터는 디지털 방식으로 서명되어 수신기에서 인증을 가능하게 하고 그리고 사전 자격 메시지 또는 전송 중인 데이터 또는 수신자에 대한 무단 변조 위험을 감소시킨다.

[0010] 제2 양상에서, 사전 자격 데이터가 ACM에 의해 처리(예를 들어, 로딩, 설치 또는 사용)된 후 ACM이 사전 자격 데이터를 수신한 경우, ACM은 사전 자격 데이터를 포함하는 사전 자격 메시지를 수신하고 그리고 ACM에 의한 사전 자격 데이터의 사용을 방지하도록 구성된다. 사용을 방지하기 위한 조건은, 예를 들어, 이전의 사전 자격 메시지가 어떤 방식으로든 처리되었다고 판단하는 경우, 여러 가지 방식으로 평가될 수 있다. 일부 실시예들에서, 이 평가는 사전 자격 데이터의 일부인 식별자에 기초할 수 있으며, 엔티티가 사전 자격 메시지/데이터를 생성함으로써 루프홀(loophole) 허용하여 후술하는 바와 같이 만료 시간을 연장할 수 있게 한다. 실제로, 제1 수신 요구 사항에 대한 명시적인 평가가 없을 수 있다. 예를 들어, ACM은 수신한 제1 사전 자격 메시지를 제1 사전 자격 메시지를 단순하게 저장할 수 있어, 나중에 사전 자격 메시지들은 사전 자격 메시지 사용을 위해 ACM에 의해 요구되는 방식으로 저장될 수 없다. 제1 수신 요건은 메시지를 수신할 때 (예를 들어, 메시지를 폐기함으로써 사용을 방지함) 또는 만료 시간 평가와 함께 사용시에 평가될 수 있다.

[0011] 유리하게는, 나중에 사전 자격 메시지를 사용할 수 없다는 규칙을 시행함으로써, ACM에서 사전 자격 기간의 무단 연장을 방지할 수 있다. 이 규칙은 셋톱 박스에서 만료 시간 설정을 포함하여 사전 자격을 생성하는 알려진 프로세스의 조작을 방지하는 것보다 적용하기가 더 쉽다. 예를 들어, 사전 자격 메시지 및/또는 데이터는, 예를 들어, 헤드 엔드에서 전송 전에 완전히 생성되기 때문에, 만료 시간의 무결성을 포함한 무결성은, 메시지 및/또는 데이터의 디지털 서명의 검증에 기초한 알려진 인증 메커니즘들에 의해 검증될 수 있다. 이 프로세스는 ACM에서 로컬로 자격들을 작성하는 것과 비교하여 쉽게 보호되고, 따라서, 프리뷰 자격들의 생성 및 사용에 대한 성공적인 공격 가능성을 줄이고 이 메커니즘을 스마트 카드가 없는 ACM들 및 STB들로 확장하여 이전에는 충분한 보안으로 실현할 수 없다.

[0012] 예를 들어, 만료 시간이 경과한 경우, 다른 점검들이 자연스럽게 수행될 수 있음을 이해된다.

[0013] 일부 실시예들에서, ACM은 사전 자격 메시지 및/또는 데이터를 인증하도록 구성된다. 즉, ACM은 메시지 및/또는 데이터가 서비스 제공 업체 또는 헤드 엔드와 같이 인증된 소스에서 전송된 후 메시지 및/또는 데이터가 조작되지 않았는지 확인하도록 구성된다. 메시지 및/또는 데이터는 전송 전에 디지털 서명될 수 있고, 그리고 메시지 및/또는 데이터를 인증하는 것은, 예를 들어, 메시지의 소스와 연관된 것으로 신뢰되는 디지털 인증서 사용하여 디지털 서명을 검증하는 것을 포함할 수 있다. 신뢰할 수 있는 인증서들의 사용, 비대칭 키 쌍들의 공개 키 등을 포함하여 수많은 디지털 서명 확인 방법이 잘 알려져 있으며, 필요에 따라 개시된 방법들 및 ACM들과 함께 통상의 기술자에 의해 용이하게 통합될 것이다. 이들 실시예들에서, 메시지 및/또는 데이터의 사용을 방지하는 것은 인증이 실패하는 경우 사용을 방지하는 것을 포함할 수 있다.

[0014] 일부 실시예들에서, 이전의 사전 자격 데이터가 조건부 액세스 모듈에 로딩된 후 수신된 사전 자격 데이터가 수신된 경우, ACM은 수신된 사전 자격 데이터를 사용하여 보호된 콘텐츠에 액세스하려고 시도할 때를 결정하도록 구성된다. ACM은, 또한, 결정이 긍정적인 경우 결정에 응답하여 사전 자격 데이터의 사용을 방지하도록 구성된

다. 일부 실시예들에서, ACM이 문제의 자격의 만료 시간이 동시에 지나지 않았음을 확인하고 그리고 일부 실시예들에서, 메시지 및/또는 데이터를 인증하는 것으로 이해된다. 이러한 조건 중 하나라도 충족되지 않으면(즉, 사전 자격이 첫 번째 조건이 아니거나, 만료 시간이 지났거나 또는 메시지 및/또는 데이터가 인증을 통과하지 못했거나 그리고/또는 디지털 서명을 확인하지 못한 경우), 액세스는 금지된다. 사용시에 이들 결정을 유리하게 하면, 메시지 및/또는 데이터가 일반적인 메모리, 예를 들어, ACM의 휘발성 RAM 또는 관련 콘텐츠 소비 디바이스에 저장될 수 있고, 보안 환경(예를 들어, TEE(Trusted Execution Environment) 또는 SE(Secure Element))에서 결정들을 수행하여 자격의 보안이 유지된다. 일부 실시예들에서, 메시지 및/또는 데이터는 비휘발성 메모리(예를 들어, 플래시)에 저장될 수 있고, 메시지의 처리 동안 비휘발성 메모리로부터 RAM으로 전송될 수 있다. 후자는 스마트카드 또는 칩셋 또는 다른 하드웨어 컴포넌트의 격리되고 보호된 부분에 의해 제공될 수 있다. ACM의 서술된 기능들 중 일부 또는 전부, 특히, 액세스를 가능하게 하는 액세스 데이터의 사용, 메시지들 및/또는 데이터의 인증 그리고 만료 시간의 검증과 같은 액세스를 가능하게 하는 조건들의 검증에 관련된 기능들은, 보안 하드웨어 또는 소프트웨어, 예를 들어, TEE, SE, 전용 칩 또는 칩셋 등으로 구현될 수 있다.

[0015] 일부 실시예들에서, 대안적으로 또는 부가적으로, 메시지 및/또는 데이터가 처음 수신된 것인지의 여부의 결정은 메시지를 수신할 때 수행되며, 예를 들어, 예를 들어 사전 자격 메시지 또는 데이터가 이미 저장되어 있는지를 확인한다. 이러한 경우에, 사전 자격 메시지 및/또는 데이터의 저장이 방지될 수 있다.

[0016] 전술한 바와 같이, 사전 자격 데이터는 만료 시간에 특정한 식별자를 포함할 수 있다. 따라서, 일부 실시예들에서, ACM은 1회 프로그램가능한 메모리에 식별자의 검증을 가능하게 하는 검증 데이터를 저장하고, 그리고 미디어 콘텐츠에 액세스하기 위해 사전 자격 데이터를 사용하기 전에, 문제의 메시지 및/또는 데이터가 처음 수신된 것인지 또는 후속 데이터인지를 결정하기 위해 사전 자격 데이터의 식별자가 검증 데이터와 일치하는지를 결정하도록 구성된다. 사전 자격 데이터의 식별자가 검증 데이터와 일치하지 않는 경우, ACM은 사전 자격 데이터를 사용하여 미디어 콘텐츠에 액세스하는 것을 방지하도록 구성된다. 검증 데이터를 일회성 프로그램 가능 메모리에 저장함으로써, 검증 데이터의 추후 덮어 쓰기 또는 변경이 방지되어, 제1 수신 메시지 및/또는 데이터가 식별된다. 검증 데이터는 단순히 식별자 자체일 수 있거나, 또는 식별자의 기능 또는 변환을 사용하여 생성될 수 있다. 기능 또는 변환은 ACM이 나중에 검증 데이터가 식별자에 해당하는지를 결정할 수 있도록 한다.

[0017] 식별자의 검증은 ACM이 만료 시간이 더 늦은 최신 메시지 및/또는 데이터의 사용을 거부하거나 방지하여 만료 시간의 무단 연장을 방지할 수 있게 한다. 그러나, 헤드 엔드(또는 다른 ACS 소스)가 ACM에 의해 처음 수신된 사전 자격 메시지의 만료 시간에 대응하는 식별자를 갖지만 이후 만료 시간을 갖는 사전 자격 메시지를 전송하는 경우, 이 메시지의 사용은 식별자 확인 실패에 기초하여 방지되지 않는다. 이는 만료 시간의 승인된 연장을 위해 메시지의 소스에 의해 이용될 수 있는 루프홀 제공함으로써 만료 시간의 허가된 연장을 가능하게 한다. 검증은, 예를 들어, 메시지 및/또는 데이터의 사용, 저장 또는 양자 모두를 방지하기 위해, 서술된 다른 점검들과 함께 또는 저장할 때와 함께, 전술한 바와 같이 사용시에 수행될 수 있다.

[0018] 일부 실시예들에서, 사용시 또는 그렇지 않으면, 식별자를 검증하는 대신 또는 검증하는 것 외에, ACM은 사전 자격 부여 데이터 자체를 일회성 프로그램 가능 메모리에 저장하고 일회성 프로그래밍 가능 메모리에 저장되지 않은 사전 자격 부여 데이터의 사용을 방지하도록 구성될 수 있다. 일회성 프로그래밍 가능 메모리는 한 번만 쓸 수 있으므로, 이것은 처음 수신된 사전 자격 데이터만 사용하도록 강제하므로 조건을 명시적으로 평가하지 않고 나중에 수신된 사전 자격 데이터를 사용하지 못하게 하는 예이다. 일부 실시예들에서, 사전 자격 데이터를 1회 프로그램 가능 메모리에 저장하는 대신, 사전 자격 데이터 또는 그것의 일부의 다이제스트, 예를 들어, 암호적으로 안전한 해시와 같은 해시가 1회 프로그램 가능 메모리에 저장된다. 저장된 다이제스트는 수신된 사전 자격 데이터의 다이제스트와 비교하여 수신된 사전 자격 데이터의 사용을 방지할지 여부를 결정하는데 사용될 수 있다. 일부 실시예들에서, 다이제스트는 사전 자격 데이터의 실제 만료 시간을 포함하는 적어도 일부로부터 생성되어, 그 결과 만료 시간의 승인된 연장을 위한 루프홀 폐쇄한다.

[0019] 일부 실시예들에서, ACM은 일회성 프로그램 가능 메모리에 데이터를 저장할 때 일회성 프로그램 가능 메모리를 비가역적으로 그리고 물리적으로 변경하도록 구성된다. 예를 들어, 일회성 프로그램 가능 메모리는 PROM(Programmable Read Only Memory) 또는 이퓨즈(eFuse) 메모리일 수 있다. 다른 실시예들에서, 일회성 프로그래밍 가능 메모리는 물리적으로 다시 프로그래밍 가능한 비휘발성 메모리, 예를 들어, EEPROM(Electrically Erasable Programmable Read Only Memory), 플래시 메모리 또는 다른 솔리드 스테이트 메모리이지만, 그러나 ACM에서의 물리적 연결이나 메모리에 대한 기입 액세스를 위한 소프트웨어 권한으로 인해 한 번만 프로그래밍 가능하도록 구성된다.

[0020] 서술된 실시예들은 제1 메시지 및/또는 데이터 이후에 수신된 사전 자격 메시지 및/또는 데이터의 사용을 방지하는 관점에서 정의되었다. 문제의 금지 조건이 충족되지 않아 사용이 방지되지 않는 경우, 활성화되고 사전 자격 데이터는, 보호 된 미디어 콘텐츠에 액세스하는데 사용된다(다른 허용 조건도 충족됨). 당연히, 통상의 기술자는, 충족되는 금지 조건이 충족되지 않은 허용 조건과 동등한 것과 그리고 그 반대도 이해할 것이며, 본 발명은 그에 따라 이해될 것이다. 또한, 서술된 실시예들은 만료 시간의 관점에서 서술되었다. 많은 실시예들에서, 만료 시간은 만료 날짜에 의해 정의되지만, 본 발명은 그와 같이 제한되지는 않는다. 결과적으로, 만료 시간을 설정함으로써 달성되는 유효 기간은, 많은 실시예들에서, 일, 주, 달 등의 기간, 또는 이들의 조합이다. 만료 시간 및 유효 기간의 보다 세밀한 정의는 일부 실시예들에서, 예를 들어, 시간 또는 다른 시간 단위로 사용된다. 유효 기간 또는 지속 기간은 만료 시간의 각 업데이트에 대해 미리 결정되고 고정될 수 있거나 또는 편의 및 특정 애플리케이션에 의해 지시된 바와 같이 업데이트에 따라 달라질 수 있다.

[0021] 일부 실시예들에서, 콘텐츠 소비 디바이스는, 상기에서 서술된 콘텐츠 소비 디바이스, 보호된 콘텐츠 및 자격 메시지들을 수신하는 수신기, 액세스 데이터로부터 도출된 제어 데이터, 예를 들어, CW 및 디스크램블링된 콘텐츠로부터 비디오 신호를 생성하는 비디오 프로세서를 사용하여 보호된 콘텐츠를 디스크램블링하는 디 스크램블러를 포함한다. 예를 들어, 콘텐츠 소비 디바이스는 STB 또는 스마트 텔레비전 세트일 수 있다. ACM은 콘텐츠 소비 디바이스의 필수 컴포넌트일 수 있거나 또는 콘텐츠 소비 디바이스에 연결될 수 있다. 예를 들어, ACM은 콘텐츠 소비 디바이스의 연결 포트, 예를 들어, USB(Universal Serial Bus) 포트, HDMI(High-Definition Multimedia Interface) 포트 등과 같은 직렬 포트에 연결될 수 있는 동글 또는 다른 연결 가능(예를 들어, 메모리 스틱 폼 팩터를 갖는) 컴포넌트로서 제공될 수 있다.

[0022] 다른 양태들은 상기 정의된 바와 같은 사전 자격 메시지, 상기에서 서술된 하나 이상의 방법들을 구현하는 수단을 포함하는 시스템, 컴퓨터 프로그램 제품, 예를 들어, 컴퓨터 프로세서상에서 실행될 때 상기에서 서술된 것처럼 하나 이상의 방법들을 구현하는 코딩된 명령어들을 포함하는 하나 이상의 유형의 비일시적인 컴퓨터 판독가능한 매체에 관한 것이다. 또 다른 양태들은 상기에서 서술된 ACM에 의해 구현되는 하나 이상의 방법들, 및 컴퓨터 프로그램 제품, 예를 들어, 컴퓨터 프로세서상에서 실행될 때 하나 이상의 그와 같은 방법들을 구현하는 코딩된 명령어들을 포함하는 하나 이상의 유형의 비일시적인 컴퓨터 판독가능한 매체에 관한 것이다.

[0023] 일부 특정 실시예들은 이제 유사한 참조 번호들이 유사한 특징들을 나타내는 첨부 도면들을 참조하여 예시적으로 서술된다.

[0024] 도 1a를 참조하면, 액세스 제어 미디어 콘텐츠 전달 시스템(100)은 처리 환경 및 통신 인터페이스를 갖는 송신기(102)를 포함한다. 송신기(102)는 전송 매체 (104), 예를 들어, 케이블, 위성, 공중 방송 또는 인터넷 또는 다른 패킷화된 데이터 연결을 통해 다수의 콘텐츠 소비 디바이스들(106)에 미디어 콘텐츠를 브로드캐스팅한다. 콘텐츠 소비 디바이스(106)는, 예를 들어, 디스플레이가 없는 셋톱 박스, 통합 수신기 디코더, 통합 텔레비전, 액세스 제어 동글, 개인용 컴퓨터, 또는 스마트 폰 또는 태블릿과 같은 모바일 디바이스일 수 있다. 송신기(102)는, 예를 들어, 액세스 제어된 미디어 콘텐츠 전달 시스템(100)의 헤드 엔드에 의해 제공될 수 있다. 콘텐츠 소비 디바이스(106)는 액세스 제어 기능을 구현한다. 콘텐츠의 전송은 대신에, 일부 실시예들에서, 멀티캐스트, 포인트캐스트 또는 주문형일 수 있으며, 그리고 전송 매체는 양방향 데이터 통신 네트워크일 수 있고, 그리고 콘텐츠는 데이터 통신 네트워크의 상위 OTT를 통해 제공될 수있다. 이하의 방송 및 방송에 대한 언급은 그러한 실시 예에서 적절하게 이해될 것이다.

[0025] 송신기(102)는 액세스 제어 시스템(100)에서 미디어 콘텐츠 및 자격 메시지들을 콘텐츠 소비 디바이스(106)에 전송한다. 자격 메시지들은, 예를 들어, 데이터 캐러셀(data carousel)에서 미디어 콘텐츠와 함께 또는 별도로 알려진 방식으로 전송된다. 자격 메시지들은 시스템(100)의 임의의 콘텐츠 소비 디바이스(106)로 전달될 수 있거나 또는 잘 알려진 바와 같이 디바이스(106)들의 그룹(예를 들어, 디바이스 또는 가입자 식별자들의 범위에 의해 식별됨) 또는 개별 콘텐츠 소비 디바이스(106)들로 어드레스될 수 있다.

[0026] 송신기(102)에 의해 제공되는 서비스들, 예를 들어, 유료 채널들, 프로그램들 또는 미디어 이벤트들의 가입자는, 콘텐츠 소비 디바이스(106)들을 사용하여 가입한 서비스들에 액세스한다. 특정 자격 메시지들은 가입자의 컨텐츠 소비 디바이스(106)로 어드레스된 송신기(102)에 의해 브로드캐스트되고, 그리고 일반적으로 스크램블링된 형태로 제공된 유료 컨텐츠를 디스크램블링함으로써 콘텐츠 소비 디바이스가 콘텐츠에 액세스할 수 있게 한다. 그러나, 예를 들어, 새로운 가입자가 처음으로 콘텐츠 소비 디바이스(106)를 사용하는 경우, 가입자의 가입이 처리되는 동안 액세스를 가능하게 하고 그리고 가입자가 더 넓은 오퍼링에 가입하도록 유도하기 위해 가입자에게 디폴트의, 가능한 넓은 서비스 오퍼링에 대한 즉각적인 액세스를 제공하는 것이 바람직할 수 있다. 이

를 위해, 시스템(100) 내의 임의의 콘텐츠 소비 디바이스(106)로 어드레스되고 그리고 상기 콘텐츠 소비 디바이스(106)에 의해 액세스될 수 있는 특정 자격 메시지들, 예를 들어, 콘텐츠 소비 디바이스(106)들의 범위 또는 리스트 또는 상기 디바이스(106)의 지리적 영역 또는 연식 또는 가입에 대응하는 가입자 식별자들에 의해 정의될 수 있는 특정 서브세트일 수 있다. 이러한 자격 메시지는 본 발명에서 사전 자격 메시지들로 지칭될 것이다.

[0027] 도 1b를 참조하면, 사전 자격 메시지(150)는, 콘텐츠 소비 디바이스(106)에 의해 로딩되거나 설치될 수 있는 시스템(100)의 하나 이상의 서비스에 액세스하기 위해 특정 자격에 관한 정보를 포함한다. 정보는 자격 테이블에 기록된다. 각각의 사전 자격 메시지(150)는 헤더(152)를 포함하고, 이 헤더(152)는, 예를 들어, 메시지가 디바이스 또는 가입자 식별자로 어드레스되는지를 각 콘텐츠 소비 디바이스(106)가 설정할 수 있게 하는 정보를 갖는다. 어드레스의 부재가 모든 디바이스(106)들에 액세스 가능한 글로벌 메시지를 나타내는 실시예들에서, 어드레스 정보는 필요하지 않다. 헤더는 지시자를 더 포함하고, 이 지시자는 메시지(150)가 사전 자격 메시지이고, 그리고 후술되는 바와 같이, 가입자들에게 구체적으로 발행된 자격 메시지들과는 디바이스(106)들에 의해 다르게 취급될 것을 나타낸다. 구체적으로, 지시자는 사전 자격 메시지(150)가 각 디바이스(106)에 의해 한번만 설치 및/또는 사용되어야 한다는 것을 디바이스(106)들에 지시한다. 즉, 최초의 사전 자격 메시지가 수신된 후 수신된 사전 자격 메시지는 설치 및/또는 사용되지 않아야 한다. 또한, 각각의 사전 자격 메시지(150)는 자격이 유효할 때까지, 즉, 자격에 의해 허가된 서비스에 액세스할 수 있을 때까지 만료 시간(154)을 포함한다. 후술하는 바와 같이, 사전 자격 메시지(150)들은 롤링 만료 시간과 함께 송신기(102)에 의해 전송되고, 제1 사전 자격 메시지(150)의 사용에 대한 제한은 만료 시간의 무단 연장을 방지한다.

[0028] 일부 실시예들에서, 사전 자격 메시지(150)는 만료 시간(154)에 특정한 식별자(156)를 포함하며, 이는 나중에 사전 자격 메시지의 사용에 대한 금지가 방지될 수 있게 한다. 또한, 식별자(156)는 송신기(102)에 의해 조작될 수 있기 때문에, 이는 후술하는 바와 같이 송신기(102)가 이전에 전송된 사전 자격 메시지의 만료 시간(154)을 업데이트할 수 있게 한다. 식별자(156)는 헤더(152)의 표시자를 대체 할 수 있으며, 즉 일부 실시예들에서, 사전 자격 메시지(150)를 인식하기 위해 클라이언트 디바이스(106)에 의해 사용될 수 있다.

[0029] 사전 자격 메시지(150)는, 일부 실시예들에서, 송신기(102)로부터 이용 가능한 모든 컨텐츠, 또는 그것의 서브셋, 예를 들어, 특정 가입 레벨을 요구하거나 또는 특정 카테고리에 속하는 특정 채널들 또는 콘텐츠에 액세스를 제공할 수 있다. 시스템(100)이 여러 서비스 제공자들에 의해 공유되는 경우, 액세스는 특정 서비스 제공자로 제한될 수 있다. 액세스 세부 사항들은 자격을 지정하는 액세스 데이터 (158)에 의해, 예를 들어, 가입 레벨, 콘텐츠 카테고리, 하나 이상의 특정 채널들, 프로그램들 또는 미디어 이벤트들, 또는 이들 중 둘 이상의 조합의 관점에서 사전 자격 메시지(150)에 정의된다. 액세스 데이터(158)는, 문제의 콘텐츠에 대한 액세스를 가능하게하는 추가 데이터, 예를 들어, 제어 워드들을 해독하고 콘텐츠의 디 스크램블링 및 이에 따른 액세스를 가능하게 하기 위해 문제의 콘텐츠와 함께 전송 된 제어 워드들을 해독하는데 사용될 수 있는 해독 키를 포함할 수 있다.

[0030] 사전 자격 메시지(150)는, 일부 실시예들에서, 디지털 서명(160)과 같은 데이터를 포함할 수 있으며, 이는 사전 자격 메시지(150)를 인증하기 위해 콘텐츠 소비 디바이스(106)에서 사용될 수 있다. 인증은, 예를 들어, 신뢰된 디지털 인증서 또는 서명 엔티티와 관련된 공개 키, 예를 들어, 송신기(102)를 동작하는 엔티티 또는 보다 일반적으로 서비스 제공자를 사용하여 디지털 서명(160)의 검증에 의해 컨텐츠 소비 디바이스(106)에서 진행될 수 있다.

[0031] 사전 자격 메시지(150)의 인증은, 메시지의 내용(구체적으로, 사전 자격 데이터)이 콘텐츠 소비 디바이스(160)에서 탐지되지 않은 상태로 변조될 수 없도록 보장하여, 사전 자격 메시지들은 콘텐츠 소비 디바이스(106)에서 특별한 보안 수단들 없이 범용 메모리에 저장될 수 있다. 또한, 사전 자격 메시지(150)의 일부, 특히, 액세스 데이터(158)는 암호화될 수 있다. 일부 실시예들에서, 전체 사전 자격 메시지(150)는 암호화된다.

[0032] 도 2를 참조하면, 콘텐츠 소비 디바이스(106)와 관련된 ACM(200)은 통신 인터페이스(202), 통상적으로, 브로드캐스트 콘텍스트에서의 브로드캐스트 수신기, 리치 실행 환경(REE)(204), 신뢰할 수 있는 실행 환경(TEE)(206) 및 보안 영구 메모리(208)를 포함한다. 일부 실시예들에서, ACM은, 콘텐트 소비 디바이스(106)에 통합될 수 있으며, 그리고 통신 인터페이스(202)는 ACM(200)과 콘텐트 소비 디바이스(106) 사이에서 공유된다. 콘텐츠 소비 디바이스(106)는 스크램블링된 콘텐츠를 디스크램블링하기위한 디스크램블러, 비디오 생성기 및 디스플레이 제어기와 같은 콘텐츠의 재생에 필요한 많은 다른 콤포넌트들을 포함하는 것으로 이해될 것이다. 이들은 소프트웨어와 전용 하드웨어의 조합으로 구현될 수 있다. 일부 실시예들에서, ACM(200)은 연결 포트를 통해 콘텐츠 소비 디바이스(106)에 외부적으로 연결 가능한 별도의 유닛으로서 제공되고, 그리고 이들 실시예들에서의 통신 인터

페이스는 포트 드라이버, 예를 들어, 콘텐츠 소비 디바이스(106)와 ACM(200) 사이의 통신을 위한 직렬 포트 드라이버를 제공할 수 있다.

[0033] 통신 인터페이스(202)는, 통합 실시예들에서 방송 신호의 관점에서 또는 콘텐츠 소비 디바이스(106)에서 수신기에 의해 수신된 후 연결 포트를 통해, 상기에서 서술된 사전 자격 메시지(150)와 같은 사전 자격 메시지를 수신하고 그리고 사전 자격 메시지를 REE(204)로 전달하도록 구성된다. REE(204)는 디바이스 정상 운영 체제, 네트워크 통신 어댑터, 사용자 인터페이스 기능, 그래픽 및 비디오 기능, 및 일부 실시예들에 따르면, TEE(206)에서 구현된 콘텐츠 액세스 기능과 관련하여, 복호화된 콘텐츠를 처리하고 추가 처리를 위해 사용자 또는 비디오/디스플레이 프로세서로 출력하기 위한 콘텐츠 처리 및 디스크램블링 모듈의 일부를 포함한다.

[0034] TEE(206)는 REE(204)와 격리되어 실행되는 실행 환경을 제공한다. TEE(206)는 일반적인 소프트웨어 공격들로부터 콘텐츠를 보호하도록 구성되며 프로그램이 TEE(206) 외부에서 액세스할 수 있는 데이터 및 기능들에 대한 보호 수단들을 정의한다. TEE는 신뢰할 수 있는 환경에서 데이터를 처리하고 안전한 저장소에 저장하여 중요한 데이터를 보호하는 안전한 영역이다. 일부 실시예들에서, TEE(206)는 자신의 전용 보안 스토리지(예를 들어, 일회성 프로그램가능 메모리(OTP), RAM 또는 판독 전용 메모리(ROM))를 갖는다. '신뢰할 수 있는 애플리케이션들'로 알려진 인증된 보안 소프트웨어의 안전한 실행을 제공하는 TEE의 기능을 통해, 보호, 기밀성, 무결성 및 데이터 액세스 권한들을 강화하여 엔드 투 엔드 보안을 제공할 수 있다.

[0035] 일부 실시예들에서, TEE(206)는 보안 요소(SE)(210)를 더 포함하며, 이는 보안성이 가장 높은 기능을 구현한다. SE(210)은 소프트웨어 및 변조 방지 하드웨어를 사용하여 보안을 강화한다. 높은 수준의 보안이 가능하며 TEE(206)와 함께 작동할 수 있다. SE(210)는 애플리케이션이 설치, 개인화 및 관리될 수 있는 플랫폼을 포함할 수 있다. 액세스 권한 평가와 같은 인증서들의 안전한 저장 및 애플리케이션들의 실행을 가능하게 하는 하드웨어, 소프트웨어, 인터페이스들 및 프로토콜들로 구성된다. SE(210)는 범용 집적 회로 카드(UICC) 또는 근거리 통신(NFC)에 의해 링크된 디바이스와 같은 상이한 형태들로 구현될 수 있다. SE(210)는 디바이스(106)의 슬롯에 삽입될 수 있는 별도의 칩 또는 보안 디바이스로서 제공될 수 있다. SE(210)는 또한 디바이스(106)에 내장되어 제공될 수 있다. SE(210)는 하나 이상의 보안 도메인을 포함할 수 있으며, 이들 각각은 공통 엔티티를 신뢰하는 (즉, 공통 또는 글로벌 암호화 키 또는 토큰을 사용하여 인증 또는 관리되는) 데이터의 컬렉션을 포함한다.

[0036] 이들 실시예들 중 일부 또는 전부에서, 이들 기능 중 일부 또는 전부는 전용 하드웨어에서 구현되어 액세스 제어 시스템에 대한 성공적인 공격의 위험을 추가로 감소시킨다. 또한, 일부 실시예들에서, 서술된 기능의 일부는 TEE(206)에서, 일부 실시예들에서, 전용 하드웨어로 구현될 수 있다. 디지털 서명 확인 또는 액세스 조건 평가와 같은 보안이 중요한 작업, 및 영구 암호 해독 및/또는 암호화 키들과 같은 비밀 정보 처리와 관련된 모든 동작들은, 바람직하게는 SE(210)에 의해, 존재한다면, 더 바람직하게는 보안 칩셋의 전용 하드웨어에 의해 처리된다. SE(210) 또는 전용 보안 칩셋이 없는 경우, 이러한 기능들은 TEE(206)에서 처리된다.

[0037] 보안 영구 메모리(208)는 1회 프로그램 가능 메모리(OTP)로서 구성된다. 이는 보안 플래시 메모리에 대한 쓰기 권한을 제어하거나 또는 물리적으로 OTP인 메모리를 사용하여 구현할 수 있다. 즉, 메모리에 처음 기록할 때 메모리가 물리적으로 비가역적으로 변경되어 저장된 데이터를 변경할 수 없게 된다. 이러한 물리적 OTP의 예는 PROM이다. 일부 실시예들에서, OTP는, 아래에서 서술되는 바와 같이, 그러한 첫번째 메시지가 수신된 후 후속 사전 자격 메시지들의 사용에 대한 금지를 시행하는데 사용된다.

[0038] 도 3은 액세스 제어 시스템(100)에서 송신기(102)로부터 콘텐츠 소비 디바이스(106)로 사전 자격 메시지들을 전송하는 방법(300)을 도시한다. 방법(300)은 액세스 제어 시스템(100)의 헤드 엔드에서 구현될 수 있다.

[0039] 단계 302에서, 사전 자격 메시지(150)와 같은 사전 자격 메시지는, 예를 들어, 데이터 캐러셀에서 주기적으로 전송된다. 사전 자격 메시지는, 예를 들어, 도 1b와 관련하여 위에서 서술한 것 같은 임의의 적합한 형식으로 또는 위에서 서술한 데이터를 포함하고 시스템(100)에 의해 사용되는 조건부 액세스 시스템들에 대한 관련 표준을 준수하도록 구성된 EMM 포맷으로 전송될 수 있다. 전송 간격은, 몇 초, 예를 들어, 10초 또는 2초에 같이 짧을 수 있거나, 또는, 예를 들어, 1분 또는 1시간 이상과 같이 길 수 있다. 새로운 가입자들에게 짧은 대기 시간으로 사전 자격 콘텐츠에 액세스할 수 있도록 전송 간격이 짧을수록 좋다.

[0040] 단계 304에서, 사전 자격 메시지(150)는 만료 시간(154)을 업데이트함으로써 업데이트되고, 그리고 식별자(156)가 존재하는 실시예들에서, 식별자(156)는 또한 업데이트된 만료 시간(154)을 반영하도록 업데이트된다. 예를 들어, 식별자(156)는 사전 자격 메시지가 업데이트될 때마다 설정 값만큼 증가되는 카운터일 수 있고, 사전 자격 메시지(150)의 만료 시간(154)에 특정한 식별자(156)를 제공한다.

[0041] 업데이트된 사전 자격 메시지(150)는, 전술한 바와 같이 단계 306에서 다시 주기적으로 전송된다. 단계 304 및 단계 306는 주기적으로 반복되며, 바람직하게는 각각의 반복에서 만료 시간(154)을 연속하는 단계들(304) 사이의 간격에 대응하는 양만큼 연장하며, 이를 통해, 고정된 기간인 사전 자격 메시지(150)에 대한 유효 슬라이딩 윈도우를 유지한다. 만료 시간(154)은, 예를 들어, 매일, 매주 또는 매달 단위로 해당하는 양만큼 변경될 수 있다. 예를 들어, 만료 시간(154)은 매일 마다, 매주 마다 연장될 수 있다. 다른 실시예들에서, 만료 시간(154)은 사전 자격 메시지들이 변경되는 것과 상이한 기간만큼 연장된다. 물론, 유효 기간은 일부 실시예들에서 반복에 따라 변경될 수 있으며, 원하는 대로 지속 시간을 연장, 축소 또는 무작위로 변화시킬 수 있음을 이해할 것이다.

[0042] 전송된 사전 자격 메시지(150)들은 이제 서술될 바와 같이 콘텐츠 소비 디바이스(106)에서 수신 및 처리된다.

[0043] 도 4를 참조하면, 수신된 사전 자격 정보를 처리하는 방법(400)은 임의의 후속 사전 자격 메시지가 수신되기 전에 사전 자격 메시지(150)와 같은 제1 사전 자격 부여 메시지가 컨텐츠 소비 디바이스(106)에 의해 수신되는 단계(402)를 포함한다. 단계 404에서, 제1 사전 자격 메시지는, 컨텐츠 소비 디바이스(106)와 관련된 ACM(200)에 의해 로딩되거나 설치된다. 제1 사전 자격 메시지는, 사전 자격 메시지의 데이터를, 예를 들어, 보호된 미디어 컨텐츠에 액세스하기 위해 컨텐츠 소비 디바이스(106)에 대한 자격들을 정의하는 자격 데이터를 포함하는 테이블 또는 데이터베이스에 저장함으로써 로딩되거나 설치된다. 사전 자격 메시지는, 예를 들어, 헤더(152) 또는 식별자(156)의 지시자를 사용하여 사전 자격 메시지로서 ACM(200)에 의해 인식되고 그에 따라 처리된다. 예를 들어, REE(204)는 통신 인터페이스 (202)를 통해 사전 자격 메시지를 수신하고 그리고 처리를 위해 수신된 사전 자격 메시지를 TEE(206) 및/또는 SE(210)에 전송한다. 일부 실시예들에서, REE(204)는 수신된 사전 자격 메시지를 임의의 암호 해독을 수행하지 않고 TEE(206) 및/또는 SE(210)에 전송하고, 다른 자격 메시지와 마찬가지로 사전 자격 메시지를 TEE(206) 및/또는 SE(210)에 단지 전달한다. 일부 실시예들에서, 예를 들어, 비휘발성 메모리에 저장된 자격 데이터베이스에 사전 자격 데이터를 기록하는 대신에, 사전 자격 부여 데이터가 보안 영구 메모리(208)에 기입될 수 있다.

[0044] 단계 406에서, 추가 자격 메시지가 수신된다. 추가 자격 메시지는, 단계 402 직후에 수신되는 경우, 단계 402에서 수신된 자격 메시지와 콘텐츠가 실질적으로 동일할 수 있거나, 또는 이후의 업데이트된 만료 시간(154)을 가질 수 있다. 단계 408에서, 추가 자격 메시지의 사용이 방지된다. 이는 각각의 개시된 실시예들에 따라 다수의 방식으로 달성될 수 있다.

[0045] 제1 그룹의 실시예들에서, ACM(200)은 사전 자격 메시지가 보안 영구 메모리 (208)에 기록되고 액세스될 것을 요구하도록 구성된다. 단계 404에서, 제1 사전 자격 메시지가 보안 영구 메모리(208)에 기입되고, 사전 자격 메시지가 후속적으로 수신되는 것을 나타내는 특정 금지 조건의 평가가 필요없이 후속 사전 자격 메시지들의 추가 로딩 및 사용을 방지하는 단계를 포함한다. 원래 만료 시간을 시행하기 위해 모든 후속 사전 자격 메시지의 사용을 막을 필요는 없지만, 이후의 만료 시간을 갖는 것들만 후자의 조건이 이들 실시예들에서 충족되며, 이는 이후의 만료 시간을 갖는 것들을 포함한 임의의 후속 자격 메시지들의 사용을 방지한다.

[0046] 제2 그룹의 실시예들에서, ACM(200)은 제1 사전 자격 메시지 또는 그 데이터를 식별하는 검증 데이터, 또는 종종 지문이라고하는 데이터를 저장하도록 구성된다. 다른 실시예들에서, 지문은, 제1 사전 자격 메시지 또는 데이터, 예를 들어, ACM(200)에서 생성된 제1 사전 자격 메시지의 암호화 해시의 다이제스트일 수 있다. 일부 실시예들에서, 지문은, 존재하는 경우 식별자(156)일 수 있고, 사전 자격 메시지의 다른 데이터, 예를 들어, 만료 시간(154)과 무관하게 송신기(102)에서 지문의 조작을 가능하게 한다. 아래에 서술된 바와 같이, 이것은 추가적인 유연성을 송신기에 제공한다. 제2 그룹의 실시예들 중 이들 실시 예들의 임의의 것에서, 사전 자격 메시지 자체는 범용 랜덤 액세스 메모리, 예를 들어, 콘텐츠 소비 디바이스(106)의 RAM 또는 ACM(200)에 저장될 수 있고, 이는, 특히 PROM 또는 이퓨즈(eFuse) 메모리와 같은 물리적 OTP가 사용되는 경우, 보안 영구 메모리(208)에서의 저장보다 비용 효과적이다. 일부 실시예들에서, 사전 자격 메시지는 비휘발성 메모리(플래시)에 저장되고, 그리고 소비 디바이스(106)의 부팅시에, RAM으로 전송되거나 비휘발성 메모리로부터 단순하게 사용된다. 한편, 이하 설명되는 바와 같이, 이들 실시예들에서 추가 검증 조건이 평가되어야 한다.

[0047] 도 5를 참조하면, 수신된 사전 자격 메시지를 저장하는 방법(500)은, 제1 사전 자격 메시지가 수신되는 단계 502를 포함한다. 이 방법은, 컨텐츠 소비 디바이스(106) 및/또는 ACM(200)에서 구현될 수 있다. 일부 실시예들에서, 사전 자격은 특정 디바이스에 의해 한 번만 수신되고, 그리고 디바이스는 사전 자격을 비휘발성 메모리에 저장한다. 단계 504에서, 수신된 자격 메시지는 전술한 바와 같이 로딩되며, 예를 들어, 자격 데이터는 자격 데이터베이스에 기입되며, 이 자격 데이터베이스는 콘텐츠 소비 디바이스(106) 또는 ACM(200)의 범용 RAM 또는 비

휘발성 메모리에 저장될 수 있다.

[0048] 단계 506에서, 검증 데이터는 보안 영구 메모리(208)에 기입된다. 해당 실시예들에서, 검증 데이터는 다음 형식 중 하나 이상이다.

[0049] • 디바이스에 의해 사전 자격 메시지가 로딩되었음을 나타내는 플래그;

[0050] • 콘텐츠 소비 디바이스(106) 또는 ACM(200)에서 생성되거나 수신된 사전 자격 메시지의 요약, 예를 들어, 사전 자격 메시지 또는 데이터의 암호화 해시, 또는 사전 자격 메시지 또는 상기 메시지와 함께 수신되고, 상기 사전 자격 메시지와 함께 수신된 사전 자격 데이터의 수신된 디지털 서명(160); 및

[0051] • 식별자(156).

[0052] 후자의 두 경우에, 검증 데이터는 요약, 식별자(156) 또는 디지털 서명(160) 자체, 또는 검증 기능에 의해 그로부터 도출된 데이터일 수 있음이 이해된다.

[0053] 단계 508에서, 후속 자격 메시지가 수신된다. 전송된 자격 메시지들의 업데이트 전에, 특히, 만료 시간(154)이 발생하기 전에 후속 자격 메시지가 전송되는 경우, 후속 자격 메시지는 단계 502에서 수신된 자격 메시지와 콘텐츠가 동일할 수 있다. 제1 사전 자격 메시지를 수신한 이후 업데이트가 발생한 경우, 후속 메시지의 만료 시간(154)이 달라질 것이다. 일부 실시예들에서, 업데이트는 대안적으로 또는 부가적으로 자격과 관련된 서비스들을 업데이트할 수 있다(예를 들어, 새로운 채널이 추가되는 경우).

[0054] 단계 510에서, 검증 데이터가 검사된다. 일부 실시예들에서, 이것은 검증 데이터의 존재 및 그에 따른 사전 자격 메시지의 사전 수신을 검사하는 것을 포함할 수 있다. 결과적으로, 이들 실시예들에서, 후속 수신된 사전 자격 메시지는 로딩되지 않을 것이다. 다른 실시예들에서, 검증 데이터는, 후속으로 수신된 사전 자격 메시지를 검증하는데 사용되고, 그리고, 검증이 통과되면, 후속으로 수신된 사전 자격 메시지가 로딩된다. 구체적으로, 검증 데이터는 후속 사전 자격 메시지로부터 도출되거나 후속 사전 자격 메시지와 함께 수신된 대응하는 데이터, 즉 다음 중 하나 이상과 비교된다:

[0055] • 콘텐츠 소비 디바이스(106) 또는 ACM(200)에서 생성되거나 수신된 사전 자격 메시지의 요약, 예를 들어, 사전 자격 메시지 또는 데이터의 암호화 해시, 또는 사전 자격 메시지 또는 상기 사전 자격 메시지와 함께 수신된 사전 자격 데이터의 수신된 디지털 서명(160); 및

[0056] • 식별자(156).

[0057] 검증 데이터와의 일치를 검사하기 위해, 다이제스트, 식별자(156) 또는 디지털 서명(160)은 검증 데이터와 직접 비교되거나 검증 데이터와 비교하기 위해 검증 기능을 통해 전달된다. 검사가 통과되면(두 세트의 검증 데이터가 일치하면), 후속 자격 데이터는 단계 512에서 컨텐츠 소비 디바이스(106) 또는 ACM(200)에 의해 로딩되고, 그리고 예를 들어, 휘발성 메모리에 저장된 경우 부팅시에 사전에 로딩된 사전 자격 메시지 또는 데이터를 덮어쓰거나 사전 자격 데이터를 복원할 수 있다.

[0058] 검증 데이터가 (다이제스트 또는 디지털 서명(160)의 경우) 모든 사전 자격 메시지 및/또는 데이터에 특정한지 또는 (식별자(156)의 경우) 만료 시간(154)에 특정한지 여부에 따라, 사전에 로딩된 사전 자격 메시지와 일치하는 후속 사전 자격 메시지들을 로딩하는 기능은 이전에 수신된 사전 자격 메시지들을 리로딩할 수 있게 한다. 이것은, 예를 들어, 콘텐츠 소비 디바이스(106) 또는 ACM(200)의 자격 데이터베이스가 휘발성 메모리에 저장되는 경우, 부팅시에 사전 자격을 복원되도록 할 수 있거나 또는 상기 데이터베이스를 리프레시할 수 있도록 한다. 이를 위해, 일부 실시예들에서, 송신기(102)는, 예를 들어, 각각의 만료 시간까지 모든 자격 메시지들을 주기적으로 재전송한다.

[0059] 다이제스트 또는 디지털 서명(160)에 대응하는 검증 데이터의 경우, 후속 사전 자격 메시지의 검증은 사전에 로딩되고 후속으로 수신된 자격 메시지들이 다이제스트 및/또는 디지털 서명(160)에 사용된 데이터에서 동일한지 검증하는 것에 상당한다. 식별자(156)에 대응하는 검증 데이터의 경우, 송신기에 의해 사전에 전송되고 로딩된 사전 자격 메시지의 수정이 가능하지만, 특히, 사전 자격 메시지가 예를 들어 전술한 바와 같이 디지털 서명(160)을 사용하여 ACM(200)에 의해 인증되는 실시예들에서, 만료 시간(154)의 무단 연장의 위험을 방지하거나 감소시킨다. 구체적으로, 송신기(102)가, 예를 들어, 만료 시간(154)을 연장하거나 또는 액세스될 수 있는 서비스들, 예를 들어, 추가 채널들, 프로그램들 또는 다른 미디어 이벤트들을 추가하기 위해 사전에 전송된 사전 자

격 메시지를 수정하기 원하는 경우, 송신기는, 그에 따라 수정되지만, 예를 들어, 연장된 만료 시간 또는 추가된 서비스들로 대체될 사전에 전송된 사전 자격 메시지의 식별자(156)를 갖는 사전 자격 부여 메시지를 전송한다. 그와 같은 업데이트된 사전 자격 메시지가 수신되면, 이전에 수신된 사전 자격의 저장된 검증 데이터에 대한 검증을 통과하고, 상기 업데이트된 사전 자격 메시지는 처음 수신된 사전 자격 부여 메시지로서 로딩될 것이다.

[0060] 도 6을 참조하면, 보호된 미디어 콘텐츠에 액세스하기 위해 로딩된 자격을 사용하는 방법(600)은, 보호된 미디어 콘텐츠가, 예를 들어, 콘텐츠 소비 디바이스(106) 및/또는 ACM(200)에서 수신되는 단계 602를 포함한다. 보호된 미디어 콘텐츠는, 스크램블링된 미디어 스트림으로서 송신기(102)로부터 송신(예를 들어, 브로드캐스트 스케줄에 따라 브로드캐스트)될 수 있다. 다른 실시예들에서, 보호된 미디어 콘텐츠는 요청에 따라 수신된다. 보호된 미디어 콘텐츠는, ECM과 함께 또는 스크램블링된 콘텐츠, 예를 들어, 종종 제어 워드로 지칭되는 디스크램블링 키에 액세스(디스크램블)하는데 필요한 액세스 정보를 포함하는 다른 데이터 구조들과 함께 전송될 수 있다. 일부 실시예들에서, 액세스 정보는 (콘텐츠 소비 디바이스(106) 또는 ACM(200)에서 디바이스 클록에 의존하는 것을 피하기 위해) 현재 시간을 더 포함한다. 일부 실시예들에서, 정보는 보호된 콘텐츠, 예를 들어, 하나 이상의 필요한 가입 레벨, 채널 ID 또는 콘텐츠의 클래스 또는 카테고리에 대한 액세스를 제공하는 자격(들)을 포함하지만, 자격을 결정하기 위한 정보는, 예를 들어, 수신된 콘텐츠와 관련된 프로그램 ID, 채널 식별자, 채널 주파수 등의 형태로 다른 형태로 수신될 수 있다.

[0061] 단계 604에서, 수신된 보호된 미디어 콘텐츠가 액세스될 수 있는지에 대한 결정이 이루어진다. 결정은 다음 검사들로 구성된다.

[0062] • 예를 들어, 범용 RAM에 저장된 디바이스 및/또는 모듈의 자격 데이터베이스에서 보호된 콘텐츠에 대한 액세스를 인증하는 자격이 콘텐츠 소비 디바이스(106) 및/또는 ACM(200)에 로딩되어 있나?

[0063] • 선택적으로 적용 가능한 자격들 중 하나라도 여전히 유효한가? 예를 들어, 자격의 만료 시간은 액세스 정보(또는 일부 실시예들에서 디바이스 클록)에서의 현재 시간과 비교될 수 있다. 예를 들어, 만료 시간의 경우, 단계 604는 만료 시간이 현재 시간인지 또는 이전인지를 검사할 수 있다. 대안적으로, 컨텐츠 소비 디바이스(106) 및/또는 ACM(200)은 만료시 모든 만료된 자격들을 삭제함으로써 자격들을 관리할 수 있다.

[0064] • 사용되는 자격이 사전 자격인 경우, 그것은 콘텐츠 소비 디바이스(106) 및/또는 ACM(200)에 로딩된 최초의 사전 자격인가? 이 검사는 자격 데이터의 일부 또는 전부를 보안 영구 메모리(208)의 검증 데이터와 비교하고 상기에서 서술한 바와 같이 일치를 검사하는 것을 포함할 수 있다.

[0065] • 선택적으로, 예를 들어, 상기에서 서술한 바와 같이 디지털 서명(160)을 사용하여 사용될 자격을 인증한다.

[0066] 단계 604에서 수행되는 그러한 검사들은 보호된 콘텐츠에 대한 액세스가 허용되어야 하는지를 집합적으로 결정하고, 내부 점검에 따라 이러한 검사들이 수행되는 순서는 그다지 중요하지 않으며 실시예마다 다를 수 있음을 이해한다. 예를 들어, 자격에 대한 나머지 검사들을 수행하기 전에 먼저 적용 가능한 자격을 결정하는 것이 더 효율적이지만, 검사는 모든 단계에서 또는 모든 검사들에 대한 종합적인 평가 후에 고려되는 모든 로딩된 자격들 및 남아있는 자격들에 대해 순서대로 수행될 수 있다. 마찬가지로, 검사들의 구현은 본 발명의 중심이 아니고 그리고 많은 가능한 솔루션들, 예를 들어, 액세스 기준(예를 들어, 구독 레벨 및/또는 카테고리 및 만료 시간)에 대한 데이터베이스 질의를 사용하여 로딩된 자격 데이터베이스에 액세스하는 것 및 데이터베이스에서 리턴된 기록들의 나머지 조건들을 평가하는 것이 통상의 기술자에게 가능할 것이다.

[0067] 단계 510(사전 자격 메시지의 저장에서 검증 데이터를 검사함) 및 단계 604(저장된 사전 자격 메시지를 사용하여 검증 데이터를 검사함) 모두가 구현되는 실시예들에서, 사기 시도가 없는 경우에는 단계 604가 중복될 것이고, 이는 (상기에서 서술된 제한된 리로딩의 가능성에 따라) 첫번째 수신된 사전 자격 메시지만이 소비 디바이스(106) 또는 ACM(200)에 로딩될 것이기 때문이다. 그러나, 예를 들어, 단계 604를 우회하여 자격 데이터베이스의 내용을 조작하고 데이터베이스에 추후 사전 자격 메시지(인증된 사전 자격 메시지일 수 있고, 따라서, 인증 검사를 통과함)를 부정적으로 기입함으로써 사기를 시도한 경우, 단계 510는 사전 자격을 사용할 때 이러한 사기 시도를 포착할 것이고, 그리고 액세스 차단, 디바이스 차단, 법 의학적 데이터 저장 및 경보 전송(리턴 연결이 이용가능한 경우) 중 하나 이상과 같은 적절한 조치를 취할 수 있다. 따라서, 후속적으로 수신된 사전 자격 메시지의 로딩을 방지하는 단계(예를 들어, 단계 510)와 사용시에 후속적으로 수신된 사전 자격 메시지의 사용을 방지하는 단계(예를 들어, 단계 604)의 조합은 실시예들에 강화된 보안을 제공한다. 하지만, 일부 실시예들

은, 후속적으로 수신된 사전 자격 메시지의 로딩을 방지하는 것(예를 들어, 단계 510) 또는 후속적으로 수신된 사전 자격 메시지의 사용을 방지하는 것(예를 들어, 단계 604)을 위한 검사들을 수행한다.

[0068] 수신된 보호된 미디어 콘텐츠에 액세스할 수 있다고 결정된 경우(예를 들어, 액세스 권한을 부여받은 사전 자격이 발견되었고, 인증되었으며, 첫 번째 수신된 사전 자격이며(이것의 식별자는 영구 메모리에 저장되 것과 동일), 그리고 만료되지 않았음), 방법은 단계 606으로 진행하여 보호된 콘텐츠에 대한 액세스를 제공한다. 수신된 보호된 미디어 컨텐츠에 액세스할 수 없다고 결정되면, 방법은 액세스를 가능하지 않고 정지한다. 또한, 법의학 데이터가 생성되거나 장치가 영구적으로 비활성화되거나 경보가 발생할 수 있다.

[0069] 단계 606에서, 액세스를 가능하게 하는 것은 일부 실시예들에서 암호화된 CW 또는 다른 디스크램블링 키를 해독하는 것 및 디스크램블러가 콘텐츠를 디스크램블링할 수 있도록 콘텐츠 소비 디바이스의 디스크램블러에 복호화된 CW를 제공하는 것을 포함한다. 액세스를 제어하기 위해 암호화된 CW를 사용하는 것은 CAS 분야에서 잘 알려져 있으며, 그리고 개시된 실시예들에서 통상의 기술자에 의해 용이하게 구현될 것이다. 보호된 콘텐츠를 스크램블링 및/또는 디스크램블링하는 것에 기초한 실시예들에서, 해독된 CW 또는 다른 디스크램블링 키는 보호된 미디어 콘텐츠를 디스크램블링하기위한 디스크램블러에 제공되고 그리고 스크램블링된 미디어 콘텐츠는 단계 608에서 디스크램블링된다. 단계 610에서, 디스크램블링된 미디어 콘텐츠는, 예를 들어, 비디오 프로세서가 비디오 스트림을 디코딩하고 그리고 디스플레이 제어기가 디스플레이로 하여금 콘텐츠를 디스플레이하도록 하거나 또는 별도의 디스플레이 디바이스 상에 디스플레이하기 위해 미디어 출력을 통해 콘텐츠를 출력하여 추가 처리 이후 출력된다.

[0070] 사전 자격 메시지들의 전송 및 업데이트로 돌아가, 도 7은 컨텐츠 소비 디바이스(106)들에서 이전에 전송된 사전 자격 메시지를 업데이트하기 위해 액세스 제어 시스템(100)의 송신기(102)로부터 콘텐츠 소비 디바이스(106)들로 사전 자격 메시지를 송신하는 방법(700)을 도시한다. 방법(700)은, 예를 들어, 액세스 제어 시스템(100)의 헤드 엔드에서 구현될 수 있다.

[0071] 단계 702에서, 이전에 전송된 사전 자격 메시지가 업데이트된다. 이러한 업데이트는 이전에 전송된 사전 자격 메시지의 만료 시간(154)의 연장(또는 축소), 또는, 예를 들어, 채널들, 프로그램들 또는 다른 미디어 이벤트들에 액세스될 수 있는 서비스들의 추가(또는 제거)를 포함할 수 있다. 단계 704에서, 업데이트된 사전 자격 메시지가 주기적으로 송신된다. 이러한 방식으로, 업데이트된 사전 자격 메시지를 합법적으로 수신하고 로딩하는 콘텐츠 소비 디바이스들(106)은, 상기에서 서술된 것처럼, 이전에 전송된 사전 자격 부여 메시지를 이전에 수신하고 로딩하였음에도 불구하고 가장 최신의 조건에 따라 콘텐츠에 액세스할 수 있다.

[0072] 도 8은 방법(800)의 형태로 방법(300)과 통합된 방법(700)을 도시한다. 단계 802에서, 원래 전송된 메시지 및 업데이트될 수 있는 메시지들을 포함하여, 아직 만료되지 않은 모든 사전 자격 메시지들, 즉 만료 시간이 있는 메시지들이 전송된다. 단계 804에서, 이전의 사전 자격 메시지들 중 하나 이상이 업데이트된다. 이 업데이트에는 추가 채널들, 프로그램들 또는 기타 미디어 이벤트들과 같이 액세스할 수 있는 서비스들의 추가(또는 제거)가 포함될 수 있다. 단계 806에서, 단계 304에서 전술한 바와 같이, 새로운 사전 자격 메시지가 업데이트된 만료 시간으로 생성된다. 새로운 메시지 및 이전에 전송된 만료되지 않은 사전 자격 메시지는 주기적으로 전송되며, 예를 들어, 단계 802에서 데이터 캐러셀에 추가된다.

[0073] 도 3, 도 7 및 도 8의 흐름도들을 참조하여 다수의 방법들이 위에서 설명되었지만, 다양한 방법 단계들이 재정렬될 수 있거나 또는 하나 이상의 단계들, 예를 들어 단계 804 또는 단계 806이 임의의 특정 실시예 또는 애플리케이션에 적합하도록 생략될 수 있다는 것이 이해될 것이다.

[0074] 도 9는 컴퓨팅 디바이스 하여금, 예를 들어, 도 3, 도 7 또는 도 8의 본 명세서에서 논의된 방법들 중 임의의 하나 이상을 수행하게 하는 명령어들의 세트를 갖는 컴퓨팅 디바이스(900)의 일 구현의 블록도를 도시한다. 대안적인 구현들에서, 컴퓨팅 디바이스는 근거리 통신망 LAN, 인트라넷, 엑스트라넷 또는 인터넷의 다른 머신들에 연결(예를 들어, 네트워킹)될 수 있다. 컴퓨팅 디바이스는 클라이언트-서버 네트워크 환경에서 서버 또는 클라이언트 머신의 용량으로 또는 피어 투 피어 (또는 분산) 네트워크 환경에서 피어 머신으로서 동작할 수 있다. 컴퓨팅 디바이스는, 개인용 컴퓨터(PC), 태블릿 컴퓨터, 셋톱 박스(STB), 개인용 디지털 단말기(PDA), 휴대폰, 웹 기기, 서버, 네트워크 라우터, 스위치 또는 브리지, 또는 해당 머신이 수행할 행동들을 지정하는 명령들의 세트(순차적 또는 다른 방식)를 실행할 수 있는 머신일 수 있다. 또한, 하나의 컴퓨팅 장치만이 도시되어 있지만, "컴퓨팅 디바이스"라는 용어는 또한 본 명세서에서 논의된 하나 이상의 방법론을 수행하기 위해 명령어들의 세트(또는 복수의 세트들)를 개별적으로 또는 공동으로 실행하는 임의의 머신들(예를 들어, 컴퓨터)의 집합을 포함하는 것으로 간주된다.

[0075] 예시적인 컴퓨팅 디바이스(900)는, 프로세싱 디바이스(902), 메인 메모리(904) (예를 들어, 판독 전용 메모리(ROM), 플래시 메모리, 동기식 DRAM, SDRAM 또는 램버스 DRAM(RDRAM) 등과 같은 동적 랜덤 액세스 메모리(DRAM), 정적 메모리(906) (예를 들어, 플래시 메모리, 정적 랜덤 액세스 메모리(SRAM) 등) 및 버스(930)를 통해 서로 통신하는 제2 메모리(예를 들어, 데이저 저장 디바이스(918))를 포함한다.

[0076] 프로세싱 디바이스(902)는 마이크로프로세서, 중앙 처리 장치 등과 같은 하나 이상의 범용 프로세서를 나타낸다. 보다 구체적으로, 프로세싱 디바이스(902)는, CISC(complex instruction set computing) 마이크로프로세서, RICS(reduced instruction set computing) 마이크로프로세서, VLIW(very long instruction word) 마이크로프로세서, 다른 명령어 세트들을 구현하는 프로세서 또는 명령어 세트들의 조합을 구현하는 프로세서들일 수 있다. 프로세싱 디바이스(902)는 또한 ASCI(application specific integrated circuit), FPGA(field programmable gate array), DSP(digital signal processor), 네트워크 프로세서 등과 같은 하나 이상의 특수 목적용 프로세싱 디바이스들일 수 있다. 프로세싱 디바이스(902)는 본 명세서에서 논의된 동작들 및 단계들을 수행하기 위한 프로세싱 로직(명령어들(922))을 실행하도록 구성된다.

[0077] 컴퓨팅 디바이스(900)는 네트워크 인터페이스 디바이스(908)를 더 포함할 수 있다. 컴퓨팅 디바이스(900)는 또한 비디오 디스플레이 유닛(910)(예를 들어, 액정 디스플레이(LCD) 또는 음극선관(CRT)), 영숫자 입력 디바이스(912)(예를 들어, 키보드 또는 터치 스크린), 커서 제어 디바이스(914)(예를 들어, 마우스 또는 터치 스크린) 및 오디오 디바이스(916)(예를 들어, 스피커)를 포함할 수 있다.

[0078] 데이터 저장 디바이스(918)는, 본 명세서에 기술된 방법론들 또는 기능들 중 하나 이상을 구현하는 하나 이상의 명령들의 세트(922)가 저장된, 하나 이상의 기계 판독 가능 저장 매체(또는 보다 구체적으로 하나 이상의 비 일시적 컴퓨터 판독 가능 저장 매체)(928)를 포함할 수 있다. 명령어(922)는 또한 컴퓨터 시스템(900)에 의해 실행되는 동안 메인 메모리(904) 및/또는 프로세싱 디바이스(902) 내에 완전히 또는 적어도 부분적으로 상주할 수 있으며, 메인 메모리(904) 및 프로세싱 디바이스(902)는 또한 컴퓨터 판독 가능 저장 매체를 구성한다.

[0079] 상기에서 서술된 다양한 방법들은 컴퓨터 프로그램에 의해 구현될 수 있다. 컴퓨터 프로그램은 컴퓨터로 하여금 전술한 다양한 방법들 중 하나 이상의 기능을 수행하도록 지시하도록 구성된 컴퓨터 코드를 포함할 수 있다. 컴퓨터 프로그램 및/또는 이러한 방법들을 수행하기 위한 코드는 컴퓨터와 같은 장치에, 하나 이상의 컴퓨터 판독 가능 매체에, 또는 더 일반적으로는 컴퓨터 프로그램 제품에 제공될 수 있다. 컴퓨터 판독 가능 매체는 일시적이거나 비 일시적일 수 있다. 하나 이상의 컴퓨터 판독 가능 매체는, 예를 들어 전자, 자기, 광학, 전자기, 적외선 또는 반도체 시스템, 또는 데이터 전송을 위한, 예를 들어, 인터넷을 통해 코드를 다운로드하기 위한 전파 매체일 수 있다. 대안적으로, 하나 이상의 컴퓨터 판독 가능 매체는 하나 이상의 물리적 컴퓨터 판독 가능 매체, 예를 들어, 반도체 또는 솔리드 스테이트 메모리, 자기 테이프, 착탈가능한 컴퓨터 디스켓, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 강성 자기 디스크 및 CD-ROM, CD-R/W 또는 DVD와 같은 광학 디스크의 형태를 취할 수 있다.

[0080] 구현에서, 본 명세서에 서술된 모듈들, 컴포넌트들 및 다른 피처들은 이산 컴포넌트들로서 구현되거나 ASIC, FPGA, DSP 또는 유사한 디바이스와 같은 하드웨어 컴포넌트들의 기능에 통합될 수 있다.

[0081] "하드웨어 컴포넌트"는 특정 동작들을 수행할 수 있는 유형의(예를 들어, 비 일시적인) 물리적 컴포넌트(예를 들어, 하나 이상의 프로세서 세트)이며, 특정 물리적 방식으로 구성 또는 배열될 수 있다. 하드웨어 컴포넌트는 특정 동작들을 수행하도록 영구적으로 구성된 전용 회로 또는 로직을 포함할 수 있다. 하드웨어 컴포넌트는 필드 프로그래밍가능 게이트 어레이(FPGA) 또는 ASIC과 같은 특수 목적용 프로세서이거나 이를 포함할 수 있다. 하드웨어 컴포넌트들 또한 특정 동작들을 수행하기 위해 소프트웨어에 의해 일시적으로 구성되는 프로그램 가능 로직 또는 회로를 포함할 수 있다.

[0082] 따라서, "하드웨어 컴포넌트"라는 문구는 물리적으로 구성되거나 영구적으로 구성(예를 들어, 하드와이어)될 수 있거나 또는 특정 방식으로 동작하거나 본 명세서에 서술된 특정 동작들을 수행하도록 일시적으로 구성된(예를 들어, 프로그래밍된) 유형의 실체를 포함하는 것으로 이해되어야 한다.

[0083] 또한, 모듈 및 컴포넌트들은 하드웨어 디바이스들 내에서 펌웨어 또는 기능 회로로서 구현될 수 있다. 또한, 모듈들 및 컴포넌트들은 하드웨어 디바이스들 및 소프트웨어 컴포넌트들의 임의의 조합으로, 또는 소프트웨어(예를 들어, 기계 판독 가능 매체 또는 전송 매체에 저장되거나 달리 구현된 코드)로만 구현될 수 있다.

[0084] 구체적으로 다르게 언급되지 않는 한, 다음 논의에서 알 수 있듯이, "수신", "결정", "비교", "사용 가능", "유지 관리", "식별", "전송", "업데이트", "방지", "로딩", "설치"과 같은 용어를 사용하는 논의는, 컴퓨터 시스

템의 레지스터들 및 메모리들 내의 물리(전자) 수량들로 표현된 데이터를 컴퓨터 시스템 메모리들 또는 레지스터들 또는 기타 그러한 정보 저장, 전송 또는 디스플레이 디바이스 내의 물리량으로 유사하게 표현되는 다른 데이터로 조작 및 변환하는, 컴퓨팅 시스템 또는 유사한 전자 컴퓨팅 디바이스의 동작들 및 프로세스들을 언급한다.

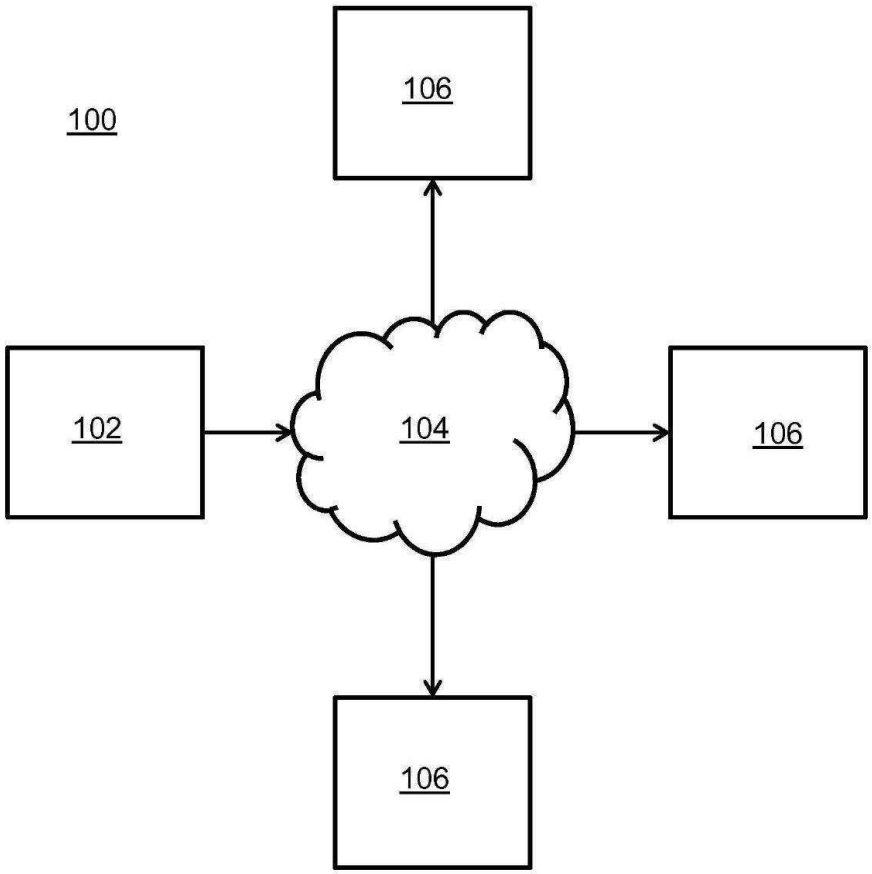
[0085] 상기 설명은 예시적인 것이며 제한적이지 않다는 것이 이해되어야 한다. 상기 서술을 읽고 이해하면 많은 다른 구현들이 통상의 기술자에게 명백할 것이다. 본 발명이 특정 예시적인 구현들을 참조하여 서술되었지만, 본 발명은 서술된 구현들로 제한되지 않으며, 첨부된 청구 범위의 사상 및 범위 내에서 수정 및 변경으로 실시될 수 있음을 인식할 것이다. 따라서, 명세서 및 도면들은 제한적인 의미보다는 예시적인 의미로 간주되어야 한다. 그러므로, 본 발명의 범위는 그러한 청구 범위가 부여되는 등가물의 전체 범위와 함께 첨부된 청구 범위를 참조하여 결정되어야 한다.

[0086] 예를 들어, 보호된 미디어 콘텐츠는 요청시 전송될 수 있다. 이러한 방식으로, 보호된 콘텐츠는 필요할 때만 전송되므로 전송 대역폭이 절약된다. 메시지들을 브로드캐스팅하는 것은 MPEG 2 스트림일 수 있다. 메시지들을 브로드캐스팅하는 것은 데이터 캐러셀에 있을 수 있다. 이를 통해 자격 메시지들을 주기적으로 전송할 수 있다. 전송 주기는 10초, 1분 또는 1시간마다 일 수 있다. 원하는 보안 수준에 따라 기간을 설정할 수 있다. 메시지는 EMM들을 포함할 수 있다. 메시지들은 액세스 제어 시스템의 모든 컨텐츠에 대한 액세스를 제공할 수 있다.

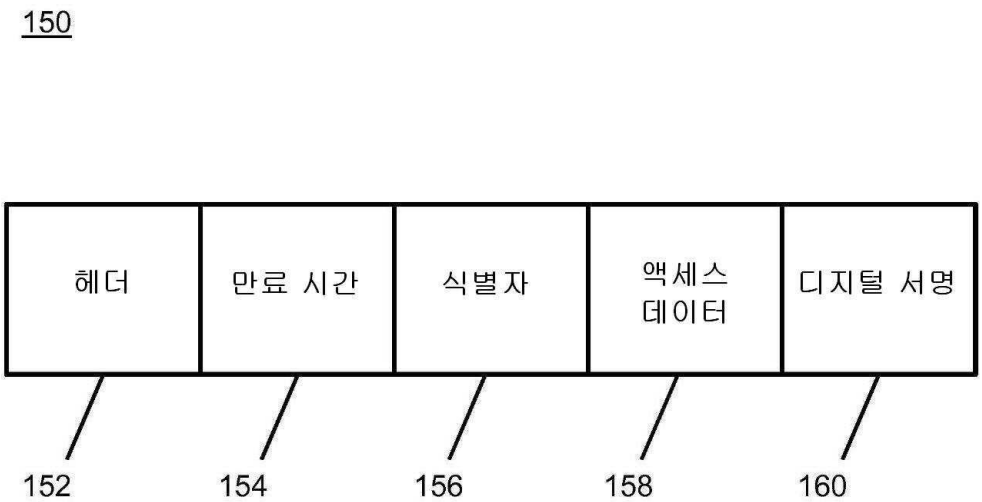
[0087] 액세스 데이터가 암호화된 경우 ACM은 이를 해독하도록 구성될 수 있다. ACM은 액세스 데이터를 사용하여 보호된 컨텐츠와 함께 수신된 제어 워드를 해독하고 그리고/또는 제어 워드의 복호화를 승인하고, 해독된 제어 워드를 디스크램블러에 제공하여 보호된 콘텐츠를 디스크램블링하도록 구성될 수 있다. 예를 들어, ACM은 키 래더 메커니즘에 기초하여 제어 워드를 해독할 수 있다. ACM은 메시지를 인증하도록 구성될 수 있다. ACM은 메시지의 디지털 서명을 확인하도록 구성될 수 있다. 이러한 각 기능은 콘텐츠 액세스의 프로세스에 추가 보안을 제공한다. OTP는 하드웨어로 구현될 수 있다. OTP는 소프트웨어로 구현될 수 있다. ACM은 메시지를 RAM에 저장하도록 구성될 수 있다.

도면

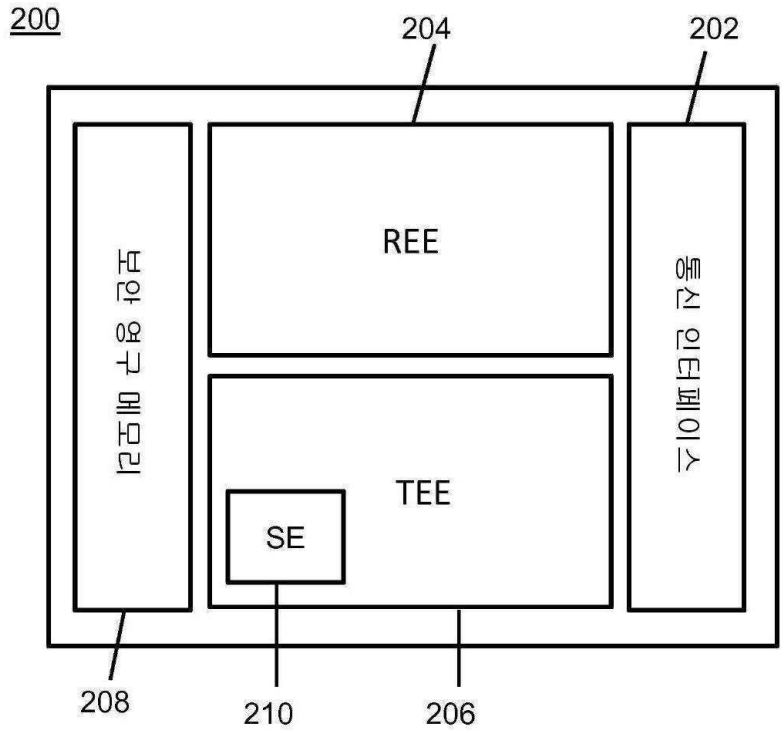
도면1a


100
106
102
104
106
106

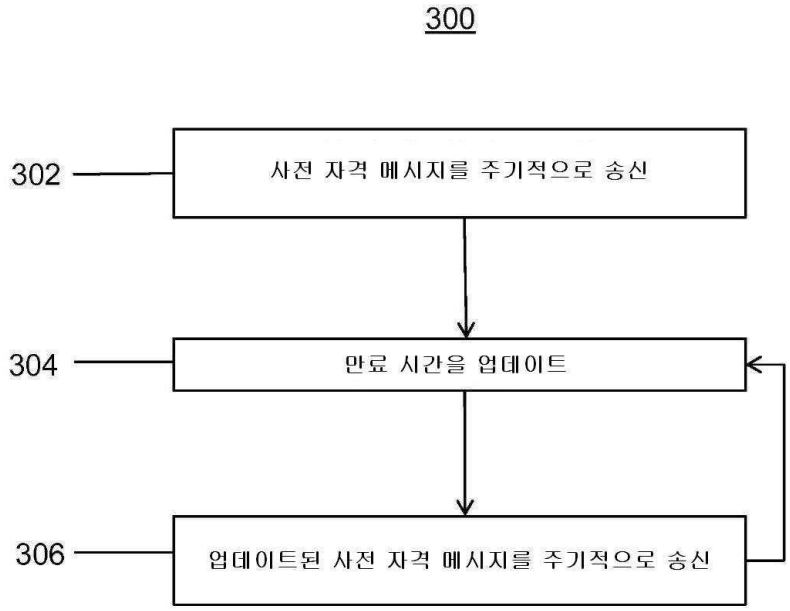
도면1b


150
헤더
만료 시간
식별자
액세스 데이터
디지털 서명
152
154
156
158
160

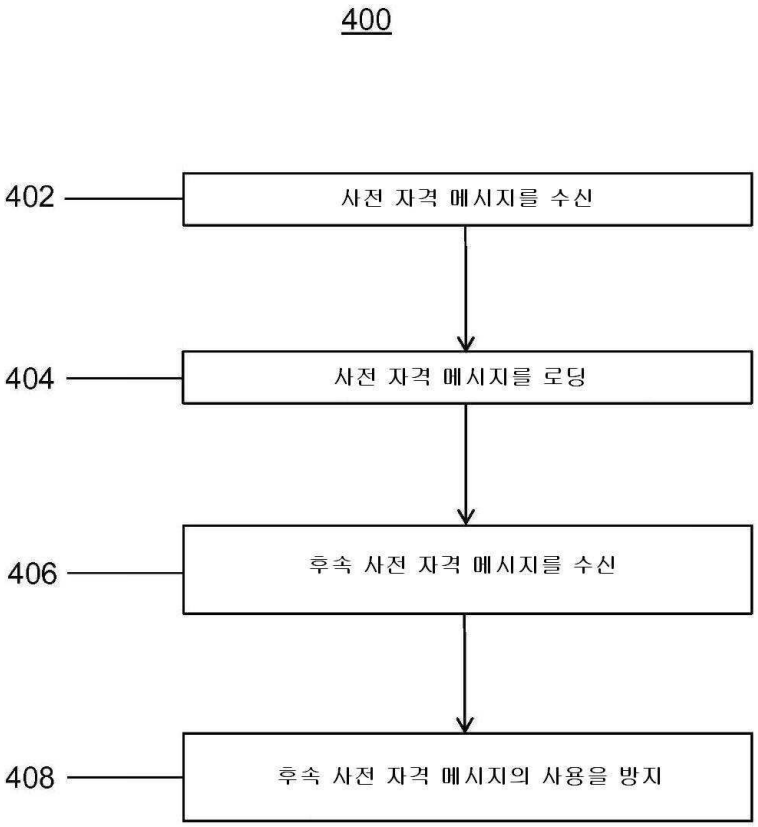
도면2


200
204
202
REE
보안 메모리 유닛
통신 인터페이스
TEE
SE
208
210
206

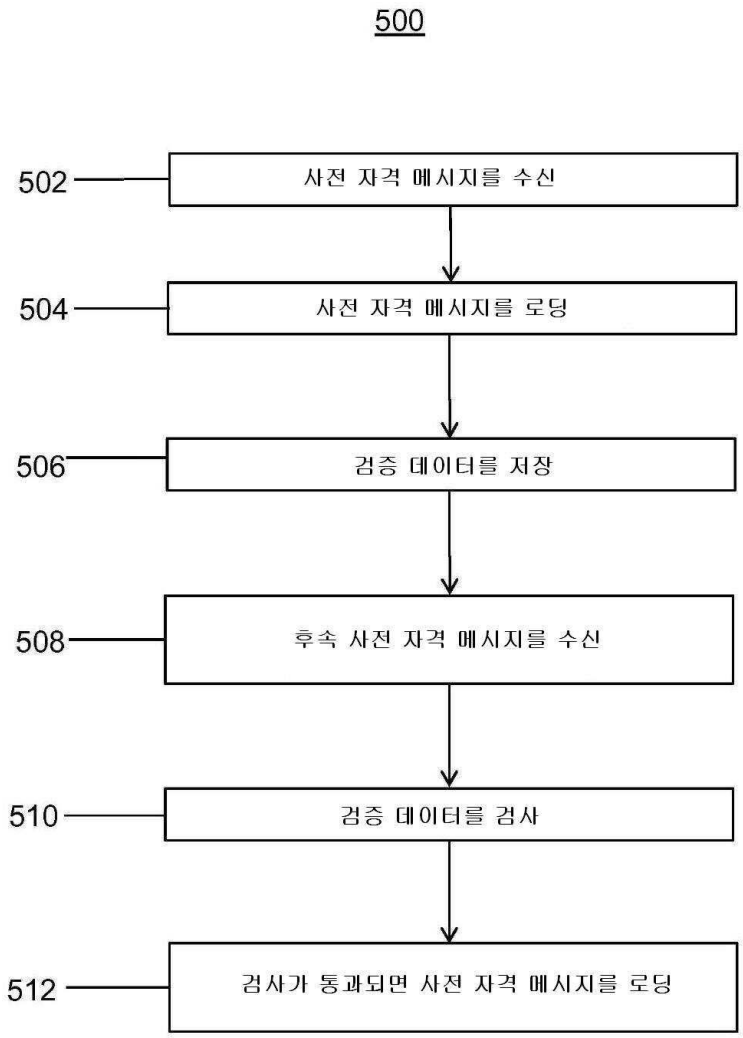
도면3


300
302
사전 자격 메시지를 주기적으로 송신
304
만료 시간을 업데이트
306
업데이트된 사전 자격 메시지를 주기적으로 송신

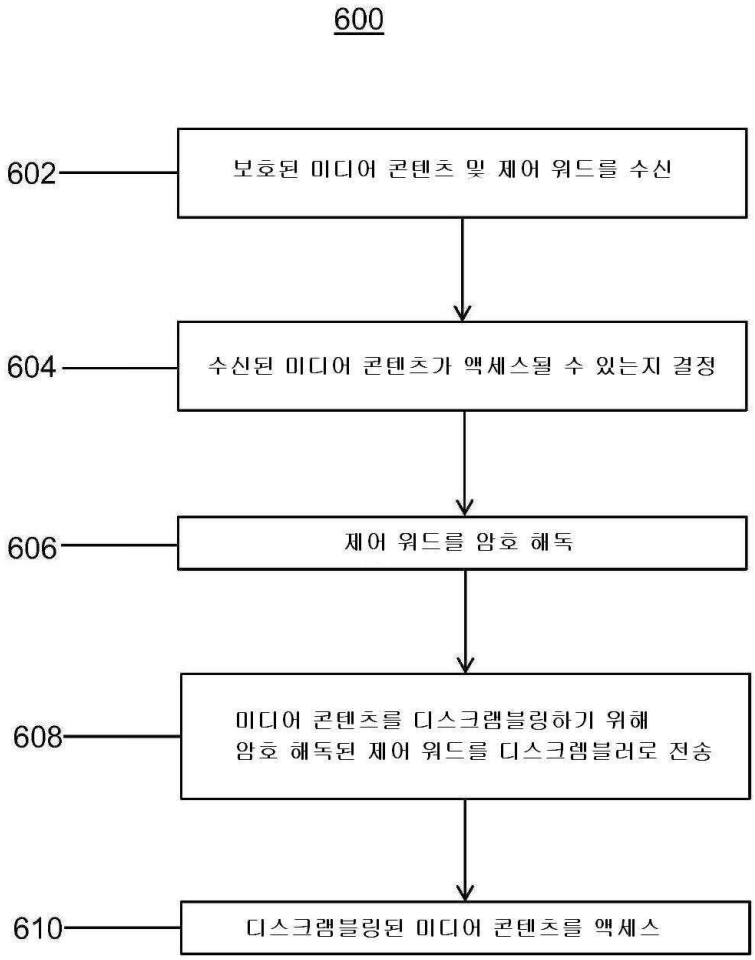
도면4


400
402
사전 자격 메시지를 수신
404
사전 자격 메시지를 로딩
406
후속 사전 자격 메시지를 수신
408
후속 사전 자격 메시지의 사용을 방지

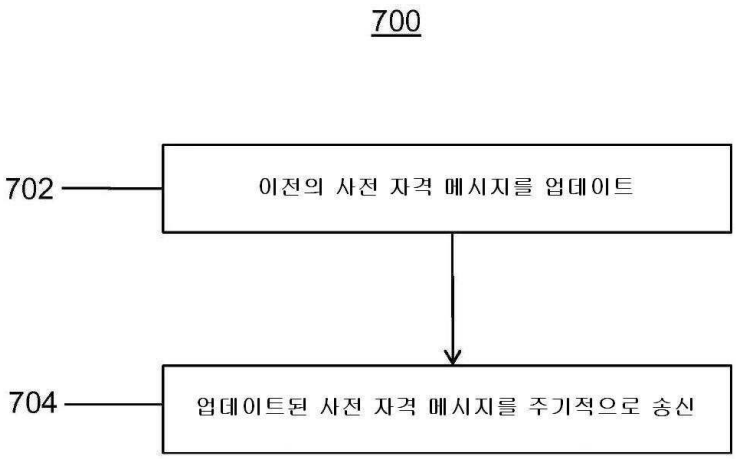
도면5


500
502
사전 자격 메시지를 수신
504
사전 자격 메시지를 로딩
506
검증 데이터를 저장
508
후속 사전 자격 메시지를 수신
510
검증 데이터를 검사
512
검사가 통과되면 사전 자격 메시지를 로딩

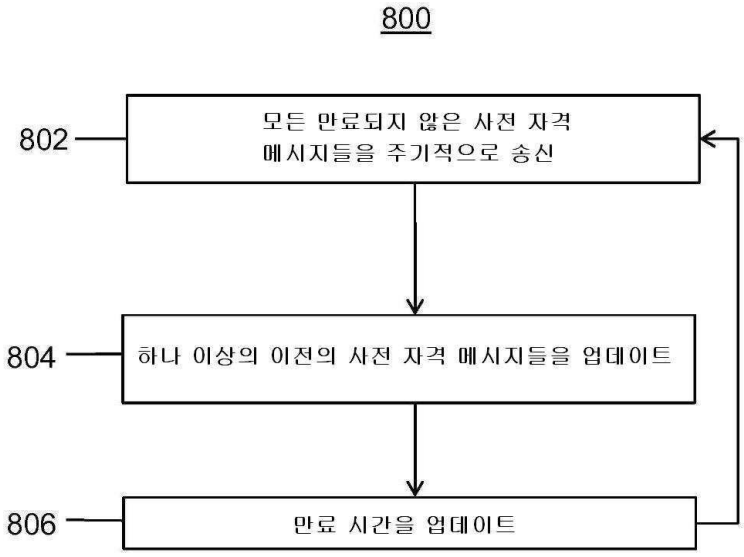
도면6


600
602
보호된 미디어 콘텐츠 및 제어 워드를 수신
604
수신된 미디어 콘텐츠가 액세스될 수 있는지 결정
606
제어 워드를 암호 해독
608
미디어 콘텐츠를 디스크램블링하기 위해
암호 해독된 제어 워드를 디스크램블러로 전송
610
디스크램블링된 미디어 콘텐츠를 액세스

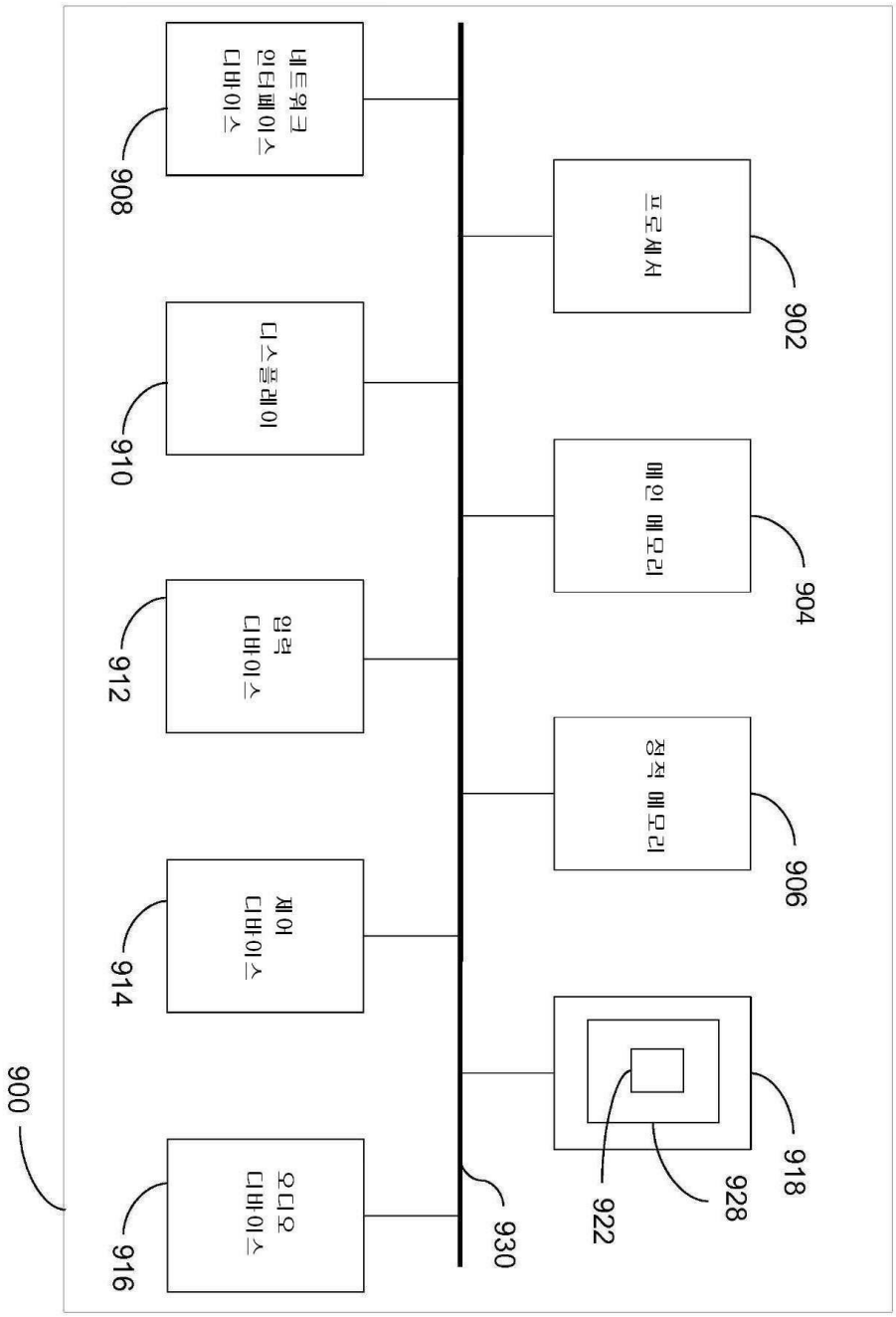
도면7


700
702
이전의 사전 자격 메시지를 업데이트
704
업데이트된 사전 자격 메시지를 주기적으로 송신

도면8


800
802
모든 만료되지 않은 사전 자격 메시지들을 주기적으로 송신
804
하나 이상의 이전의 사전 자격 메시지들을 업데이트
806
만료 시간을 업데이트

도면9


900
프로세서
902
메인 메모리
904
정적 메모리
906
918
928
922
930
네트워크 인터페이스 디바이스
908
디스플레이
910
입력 디바이스
912
제어 디바이스
914
오디오 디바이스
916