(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0118752
(43) 공개일자 2020년10월16일

(51) 국제특허분류(Int. Cl.)
H04N 21/266 (2011.01) *H04N 21/235* (2011.01)
H04N 21/254 (2011.01) *H04N 21/6334* (2016.01)
(52) CPC특허분류
H04N 21/26606 (2013.01)
H04N 21/2351 (2013.01)
(21) 출원번호 10-2020-0015374
(22) 출원일자 2020년02월10일
심사청구일자 2020년02월10일
(30) 우선권주장
1020190041001 2019년04월08일 대한민국(KR)

(71) 출원인
박화영
경기도 성남시 분당구 산운로 55, 308동 104호 (운중동, 산운마을)
(72) 발명자
박화영
경기도 성남시 분당구 산운로 55, 308동 104호 (운중동, 산운마을)
(74) 대리인
오종환

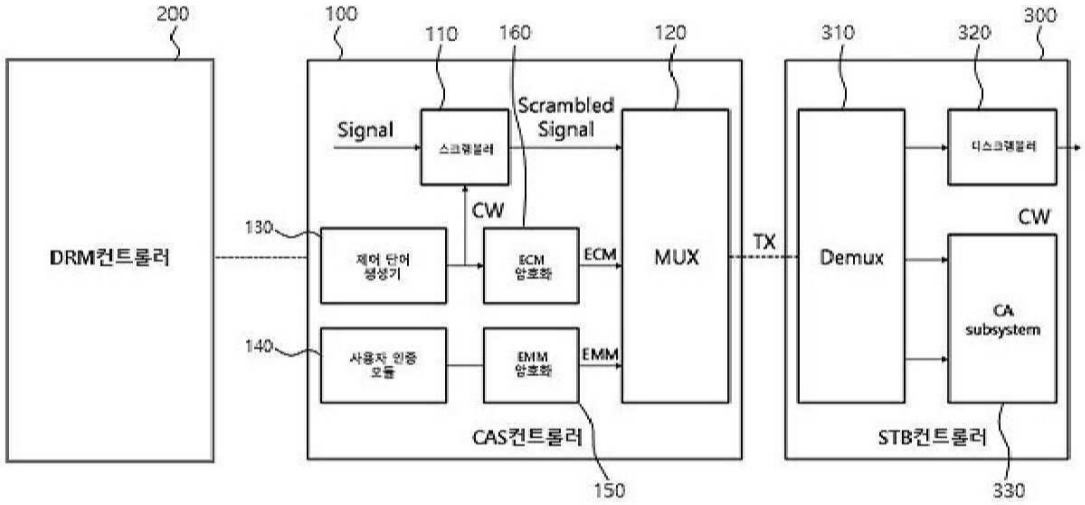
전체 청구항 수 : 총 3 항

(54) 발명의 명칭 **UHD 방송 콘텐츠 보안 시스템**

(57) 요 약

본 발명은 방송 콘텐츠 보안 시스템에 관한 것으로서, 방송 콘텐츠 보안을 위해 방송 콘텐츠를 스크램블링(scrambling)하여 생성된 자격제어메세지(ECM, Entitlement Control Message)를 포함하는 시큐리티 정보를 전달하는 시큐리티 정보 전송 모듈; 및 방송 콘텐츠 각각에 대해 자격관리메세지(EMM, Entitlement Management Message)를 생성하여 방송 콘텐츠 수신 자격 정보를 전달하는 자격 관리 모듈을 포함하는 CAS시스템; 및 CAS시스템과 연동하여 CAS시스템에 대한 권한 제어를 수행하는 DRM시스템을 포함하고, DRM시스템은 방송 콘텐츠를 암호화하는 DRM암호화 모듈; 및 암호화된 방송 콘텐츠에 대해 복호화가 가능하도록 사용자권한정보 및 복호화 키를 포함하는 라이센스를 생성하고 관리하는 위조 방지 모듈을 포함하며, 수신 자격 정보는 DRM암호화 모듈에 의해 방송 콘텐츠 암호화에 필요한 채널키로 변환한다.

대 표 도 - 도1



(52) CPC특허분류
H04N 21/2541 (2013.01)
H04N 21/26613 (2013.01)
H04N 21/63345 (2013.01)

명 세 서

청구범위

청구항 1

방송 콘텐츠 보안을 위해 방송 콘텐츠를 스크램블링(scrambling)하여 생성된 자격제어메세지(ECM,Entitlement Control Message)를 포함하는 시큐리티 정보를 전달하는 시큐리티 정보 전송 모듈; 및 상기 방송 콘텐츠 각각에 대해 자격관리메세지(EMM, Entitlement Management Message)를 생성하여 방송 콘텐츠 수신 자격 정보를 전달하는 자격 관리 모듈을 포함하는 CAS시스템; 및 상기 방송 콘텐츠를 암호화하는 DRM암호화 모듈; 상기 암호화된 방송 콘텐츠에 대해 복호화가 가능하도록 사용자권한정보 및 복호화 키를 포함하는 라이센스를 생성하고 관리하는 위조 방지 모듈; 방송 콘텐츠 사용자를 인증하기 위해 사용자 정보를 기초로 인증키를 생성하는 사용자 인증 모듈; 및 상기 생성된 인증키와 상기 채널키를 비교하여 일치 여부에 따라 상기 복호화 키를 생성하여 상기 암호화된 방송 콘텐츠에 대한 복호화를 수행하는 복호화 모듈을 포함하고, 상기 CAS시스템과 연동하여 상기 CAS시스템에 대한 권한 제어를 수행하는 DRM시스템; 및 상기 CAS시스템과 연동된 STB시스템을 포함하는 디스플레이 기기;

휴대기기;

및 콘텐츠 관리서버를 포함하며,

상기 수신 자격 정보는 상기 DRM암호화 모듈에 의해 상기 방송 콘텐츠 암호화에 필요한 채널키로 변환되며, 상기 위조 방지 모듈은 상기 복호화 모듈에 의해 복호화된 상기 채널키에 대한 사용이 중복된다고 판단하는 경우, 상기 라이센스 인증을 차단하며, 상기 채널키는 상기 방송 콘텐츠에 대한 수신 자격 정보를 포함하고, 상기 인증키는 상기 방송 콘텐츠 사용자에 대한 사용자ID 및 비밀번호를 포함하고, 상기 인증키는 상기 방송 콘텐츠 사용자에게 인증 부분키의 형태로 전달되며,

상기 복호화 키는 상기 휴대기기, 상기 콘텐츠 관리서버 및 상기 디스플레이 기기에서 일대일로 발생시켜 공유한 난수, 오프셋 및 반복회수에 기초하여 생성된 일회성 인증값에 의하여 상기 콘텐츠 관리서버에서 상기 디스플레이 기기가 인증되는 경우에 상기 콘텐츠 관리 서버로부터 상기 디스플레이 기기에 전달되는,

방송 콘텐츠 보안 시스템.

청구항 2

제1항에 있어서,

상기 복호화 키의 전달이 상기 반복회수만큼 반복되면 상기 콘텐츠 관리 서버는 상기 휴대기기에 난수, 오프셋 및 반복회수의 공유를 상기 휴대기기에 요청하는,

방송 콘텐츠 보안 시스템.

청구항 3

제1항에 있어서,

상기 디스플레이 기기는 상기 난수에 해쉬 함수를 상기 오프셋 및 상기 복호화 키의 전달 회수의 합만큼 중첩 적용하여 상기 일회성 인증값을 생성하는,

방송 콘텐츠 보안 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 방송 콘텐츠 보안 시스템에 관한 것으로서, 보다 상세하게는 하나의 통합 플랫폼에서 CAS기술과 DRM 기술을 결합하여 동작시킴으로써 IPTV의 보안 신뢰성을 향상시킨 방송 콘텐츠 보안 시스템에 관한 것이다.

배 경 기 술

[0002] IPTV(Internet Protocol Television)는 초고속 인터넷 망을 통해 정보나 방송 등을 TV로 제공하는 통신과 방송이 융합된 서비스로 디지털 정보 서비스, 동영상 콘텐츠, 다양한 개인 맞춤형 서비스 등을 제공하고 있다.

[0003] IPTV에 의해 제공되는 콘텐츠들은 전송되기 위해서 모두 디지털화되어야 하는데 디지털화 콘텐츠들은 누구나 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있으며, 복사된 콘텐츠는 원본과 동일한 품질로 제공되고 확산 속도가 빠르다는 특징이 있다. 이에 따라 디지털 콘텐츠에 대한 보안과 저작권보호가 중요한 문제로 대두되고 있다.

[0004] 현재, 콘텐츠에 대한 불법 복제 및 배포를 방지하기 위한 기술들에 대하여 연구가 활발하게 진행되고 있으며, 대표적인 보안 기술로 CAS(Conditional Access System)와 DRM(Digital Rights Management)이 있다.

[0005] 기존의 방송 시스템에서 시청자의 접근 제어를 목적으로 사용되던 CAS가 하나의 대안으로 활용될 수 있지만, IPTV가 제공하고자 하는 다양한 부가 서비스에 대해서는 여러 가지 문제가 있다. 예컨대, PVR(Private Video Recording)과 같이 하드 디스크 저장이 필요한 서비스에 대한 콘텐츠 보호 문제는 CAS만으로는 대응이 어려운 문제이다. 이에, CAS의 부족한 기능을 대체할 수 있는 시스템으로 IP및 PC 환경에서 발전되어 온 DRM 기술이 있다.

[0006] DRM 기술은 디지털로 유통되는 모든 콘텐츠 종류에 대한 불법 사용 및 불법 복제에 대응하기 위한 기술로서, CAS보다는 더 넓은 범위에서 콘텐츠 보안 문제를 해결할 수 있다. 다만, DRM기술이 PVR같은 서비스에 적용이 용이한 기술이긴 하지만, 현재의 방송 시스템에 그대로 적용하기에는 부족한 점이 존재한다.

[0007] 한편, 최근 통신기술과 스마트폰 기술의 발달로 개인들은 여러가지 휴대기기를 소지한다. 예컨대, 개인들은 스마트워치, 태블릿 PC, 휴대폰 등 다양한 휴대 기기를 동시에 소지할 수 있다. 이 경우, 개인들은 IPTV를 통하여 유통되는 콘텐츠들을 여러 화면에서 보고 싶어 하는 니즈가 있다. 단, 개인이 소지한 여러 화면에서 해당 콘텐츠를 볼 수 있도록 모두 인증을 하는 경우에는 개인이 소유한 기기의 분실 시, 해당 인증에 필요한 키가 노출될 수가 있어서 보안에 문제가 발생할 수 있다.

[0008] 따라서, 본 발명은 DRM을 CAS와 결합하여 DRM/CAS 기술이 하나의 플랫폼에서 동작하도록 함으로써 악의적인 사용자로부터 콘텐츠를 보호할 수 있는 방송 콘텐츠 보안 시스템을 개발하고자 한다. 또한, 본 발명은 여러가지 휴대기기를 소유한 개인에게 방송 콘텐츠의 보안을 크게 향상시킨 방송 서비스를 제공하면서도 다양한 화면에서 할 수 있도록 하는 보안 시스템을 제공하고자 한다.

발명의 내용

해결하려는 과제

[0009] 본 발명이 해결하고자 하는 과제는 하드웨어 방식과 소프트웨어 방식을 결합함으로써 비용 절감과 동시에 악의적인 사용자로부터 콘텐츠를 효과적으로 보호할 수 있는 방송 콘텐츠 보안 시스템을 제공하는 것이다.

[0010] 본 발명이 해결하고자 하는 또 다른 과제는 하나의 플랫폼에서 CAS기술과 DRM기술을 동작함으로써 IPTV의 보안 신뢰성을 향상시킨 방송 콘텐츠 보안 시스템을 제공하는 것이다.

[0011] 본 발명의 과제들은 이상에서 언급한 과제들로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 전술한 바와 같은 과제를 해결하기 위하여 본 발명의 일 실시예에 따른 방송 콘텐츠 보안 시스템은 방송 콘텐츠 보안을 위해 방송 콘텐츠를 스크램블링(scrambling)하여 생성된 자격제어메세지(ECM,Entitlement Control Message)를 포함하는 시큐리티 정보를 전달하는 시큐리티 정보 전송 모듈; 및 상기 방송 콘텐츠 각각에 대해 자격관리메세지(EMM, Entitlement Management Message)를 생성하여 방송 콘텐츠 수신 자격 정보를 전달하는 자격관리 모듈을 포함하는 CAS시스템; 및 상기 방송 콘텐츠를 암호화하는 DRM암호화 모듈; 상기 암호화된 방송 콘텐츠에 대해 복호화가 가능하도록 사용자권한정보 및 복호화 키를 포함하는 라이센스를 생성하고 관리하는 위조방지 모듈; 방송 콘텐츠 사용자를 인증하기 위해 사용자 정보를 기초로 인증키를 생성하는 사용자 인증 모듈; 및 상기 생성된 인증키와 상기 채널키를 비교하여 일치 여부에 따라 상기 복호화 키를 생성하여 상기 암호화된 방송 콘텐츠에 대한 복호화를 수행하는 복호화 모듈을 포함하고, 상기 CAS시스템과 연동하여 상기 CAS시스템에

대한 권한 제어를 수행하는 DRM시스템; 및 상기 CAS시스템과 연동된 STB시스템을 포함하는 디스플레이 기기; 휴대기기; 및 콘텐츠 관리서버를 포함하며, 상기 수신 자격 정보는 상기 DRM암호화 모듈에 의해 상기 방송 콘텐츠 암호화에 필요한 채널키로 변환되며, 상기 위조 방지 모듈은 상기 복호화 모듈에 의해 복호화된 상기 채널키에 대한 사용이 중복된다고 판단하는 경우, 상기 라이센스 인증을 차단하며, 상기 채널키는 상기 방송 콘텐츠에 대한 수신 자격 정보를 포함하고, 상기 인증키는 상기 방송 콘텐츠 사용자에 대한 사용자ID 및 비밀번호를 포함하고, 상기 인증키는 상기 방송 콘텐츠 사용자에게 인증 부분키의 형태로 전달되며, 상기 복호화 키는 상기 휴대기기, 상기 콘텐츠 관리서버 및 상기 디스플레이 기기에서 일대일로 발생시켜 공유한 난수, 오프셋 및 반복회수에 기초하여 생성된 일회성 인증값에 의하여 상기 콘텐츠 관리서버에서 상기 디스플레이 기기가 인증되는 경우에 상기 콘텐츠 관리 서버로부터 상기 디스플레이 기기에 전달될 수 있다.

[0013] 이 경우, 상기 복호화 키의 전달이 상기 반복회수만큼 반복되면 상기 콘텐츠 관리 서버는 상기 휴대기기에 난수, 오프셋 및 반복회수의 공유를 상기 휴대기기에 요청할 수 있다.

[0014] 또한, 상기 디스플레이 기기는 상기 난수에 해쉬 함수를 상기 오프셋 및 상기 복호화 키의 전달 회수의 합만큼 중첩 적용하여 상기 일회성 인증값을 생성할 수 있다.

발명의 효과

[0015] 본 발명은 하드웨어 방식과 소프트웨어 방식을 결합함으로써 비용 절감과 동시에 악의적인 사용자로부터 콘텐츠를 효과적으로 보호할 수 있다.

[0016] 또한, 본 발명은 하나의 플랫폼에서 CAS기술과 DRM기술을 동작함으로써 IPTV의 보안 신뢰성을 향상시킬 수 있다.

[0017] 본 발명에 따른 효과는 이상에서 예시된 내용에 의해 제한되지 않으며, 더욱 다양한 효과들이 본 명세서 내에 포함되어 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 방송 콘텐츠 보안 시스템의 구성도이다.

도 2는 CAS시스템 및 DRM시스템을 나타낸 블록도이다.

도 3은 본 발명의 일 실시예에 따른 수신 자격 정보 생성 과정을 설명하기 위한 예시도이다.

도 4는 본 발명의 일 실시예에 따른 CAS시스템을 설명하기 위한 예시도이다.

도 5는 본 발명의 일 실시예에 따른 CAS시스템의 하드웨어방식을 설명하기 위한 예시도이다.

도 6은 본 발명의 일 실시예에 따른 CAS시스템의 소프트웨어방식을 설명하기 위한 예시도이다.

도 7은 본 발명의 또 다른 실시예에 따른 콘텐츠 관리서버, 휴대기기 및 디스플레이 기기를 도시한 도면이다.

도 8은 본 발명의 또 다른 실시예에 따른 콘텐츠 관리서버, 휴대기기 및 디스플레이 기기의 그룹키(복호화 키) 생성 및 확인 프로세스를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하의 내용은 단지 발명의 원리를 예시한다. 그러므로 당업자는 비록 본 명세서에 명확히 설명되거나 도시되지 않았지만 발명의 원리를 구현하고 발명의 개념과 범위에 포함된 다양한 장치를 발명할 수 있는 것이다. 또한, 본 명세서에 열거된 모든 조건부 용어 및 실시예들은 원칙적으로, 발명의 개념이 이해되도록 하기 위한 목적으로만 명백히 의도되고, 이와 같이 특별히 열거된 실시예들 및 상태들에 제한적이지 않는 것으로 이해되어야 한다.

[0020] 또한, 이하의 설명에서 제1, 제2 등과 같은 서수식 표현은 서로 동등하고 독립된 객체를 설명하기 위한 것이며, 그 순서에 주(main)/부(sub) 또는 주(master)/종(slave)의 의미는 없는 것으로 이해되어야 한다.

[0021] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해질 것이며, 그에 따라 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다.

[0022] 본 발명의 여러 실시예들의 각각 특징들이 부분적으로 또는 전체적으로 서로 결합 또는 조합 가능하며, 당업자가 충분히 이해할 수 있듯이 기술적으로 다양한 연동 및 구동이 가능하며, 각 실시예들이 서로에 대하여 독립적으로 실시 가능할 수도 있고 연관 관계로 함께 실시 가능할 수도 있다.

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

[0024] 도 1은 방송 콘텐츠 보안 시스템의 구성도이다. 도 2는 CAS시스템 및 DRM 시스템을 나타낸 블록도이다. 도 3은 본 발명의 일 실시예에 따른 수신 자격 정보 생성 과정을 설명하기 위한 예시도이다. 도 4는 본 발명의 일 실시예에 따른 CAS시스템을 설명하기 위한 예시도이다. 도 5는 본 발명의 일 실시예에 따른 CAS시스템의 하드웨어방식을 설명하기 위한 예시도이다. 도 6은 본 발명의 일 실시예에 따른 CAS시스템의 소프트웨어방식을 설명하기 위한 예시도이다.

[0025] 도 1을 참조하면, 방송 콘텐츠 보안 시스템은 CAS시스템(100), DRM시스템(200) 및 STB시스템(300)을 포함한다. 도 2를 참조하면, CAS시스템(100)은 시큐리티 정보 전송 모듈 및 자격 관리 모듈을 포함하고, DRM시스템(200)은 DRM암호화 모듈 및 위조 방지 모듈을 포함한다.

[0026] CAS시스템(100)은 방송 콘텐츠 보안 시스템에 가입한 사용자만이 특정 프로그램을 수신할 수 있도록 하는 시스템으로서, 유료 방송 사업자의 비즈니스 수익을 보호할 수 있다. 예컨대, CAS시스템(100)은 스크램블링/디스크램블링(scrambling/descrambling), 자격제어(Entitlement Control), 자격관리(Entitlement Management) 기능을 수행할 수 있다. 본 발명에서, CAS시스템(100)은 동일한 알고리즘으로 상기 방송 콘텐츠를 기 설정된 암호 레벨에 따라 스크램블링하고 하드웨어 및/또는 소프트웨어를 기반으로 동작하는 것으로 이해되는 것이 바람직하다.

[0027] 또한, 본 발명에서 방송 콘텐츠는 다운로드 되는 이미지에 대한 정보를 포함하는 이미지 헤더(image header); 및 이미지의 내용인 이미지데이터(image data)를 포함할 수 있다. 또한, 다운로드 되는 콘텐츠 이미지파일은 검증요구시 필요한 Signature data를 더 포함할 수 있다. 구체적으로, 다운로드되는 콘텐츠 이미지는 기본적으로 하나의 SM Client 이미지(CAS or DRM or ASD)를 포함하고 있지만, 최초의 SM Client 다운로드의 경우에는 CAS, DRM, ASD 중 2개 이상의 이미지를 하나의 다운로드 이미지로 생성하여 전송할 수 있다. 그렇기 때문에 다운로드 이미지 헤더에 이미지에 대한 정보를 포함할 수 있다. 예컨대, packed_image_num는 다운로드 이미지에 포함되어 있는 SM Client 이미지의 수이며, total_image_length는 SM Client 이미지의 전체 크기를 나타내고, Reserved는 추가정보를 의미할 수 있다. 이에 따라, 상술한 정보는 이미지 헤더에 포함될 수 있다.

[0028] 이때, CAS시스템(100)이 하드웨어를 기반으로 동작하는 경우, 시큐리티 정보, 자격제어메세지 및 자격관리메세지에 대한 보안 처리를 CAS시스템(100)과 연동된 STB(Set-Top Box)시스템(300)의 스마트카드(Smart Card)에서 수행할 수 있다. 구체적으로, 도 5에 도시된 바와 같이, 하드웨어 방식의 CAS시스템(100)은 서비스 가입 정보(Entitlement, PIN Code 등) 및 키 등의 저장, ECM/EMM 보안 처리 등을 물리적인 보안을 제공하는 스마트카드에서 담당을 한다. 이때, 외부에서는 CAS코드와 데이터에 접근할 수 없도록 설정한다.

[0029] 또한, CAS시스템(100)이 소프트웨어를 기반으로 동작하는 경우, 시큐리티 정보, 자격제어메세지 및 자격관리메세지에 대한 보안 처리를 방송 콘텐츠 보안 장치의 메인 메모리에서 수행할 수 있다. 구체적으로, 도 6에 도시된 바와 같이, 서비스 가입 정보(Entitlement, PIN Code 등) 및 키 등의 저장, ECM/EMM 보안 처리 등을 단말기에 있는 Main CPU에서 처리할 수 있다.

[0030] 구체적으로, 스크램블링(scrambling) 기능은 스크램블러(110)에 의해 비 인가된 수신자는 방송 콘텐츠를 시청할 수 없도록 원래의 TV신호를 변형시키는 기능으로서, TV프로그램 형태(예컨대, 오디오, 비디오, 데이터)와 신호 형태(예컨대, 아날로그, 디지털)에 따라 방식이 상이할 수 있다. 디스크램블링(Descrambling) 기능은 디스크램블러(320)가 가진 디스크램블링 키인 CW(Control Word)를 이용하여 수신된 방송 콘텐츠를 디스크램블링하는 기능이다. 이때, 스크램블링 방식은 고도의 암호 메커니즘으로 구성될 수 있다. 여기서, CW는 주기적으로 생성되며 암호화되어 전송된다.

[0031] 도 1 및 도 2를 참조하면, 자격 제어(Entitlement Control) 기능은 시큐리티 정보 전송 모듈이 방송 콘텐츠 보안을 위해 방송 콘텐츠를 스크램블링(scrambling)하여 생성된 자격제어메세지(ECM, Entitlement Control Message)를 포함하는 시큐리티 정보를 전달하는 것을 의미한다. 여기서, 자격제어메세지(ECM)에는 제어변수가 포함될 수 있고, 모든 수신기는 전송된 제어변수와 수신기의 인증변수와 비교하여 올바른 사용자일 경우 도 5와 같이, 스마트카드(Smart Card) 내의 비밀키로 CW(CW1, CW2, CW3)를 복호화하고 수신된 방송 콘텐츠를 디스크램블링 할 수 있다.

[0032] 도 1 및 도 2를 참조하면, 자격 관리(Entitlement Management) 기능은 자격 관리 모듈이 방송 콘텐츠 각각에 대해 자격관리메세지(EMM, Entitlement Management Message)를 생성하여 방송 콘텐츠 수신 자격을 관리하는 것을 의미한다. 자격 관리 모듈은 분배키를 이용하여 인증키를 암호화하여 자격관리메세지를 생성하고 수신 측에 전송한다. 이때, 전송된 자격관리메세지는 수신 측에 있는 스마트카드(Smart Card)에 자격을 부여하는 기능을 수행할 수도 있다. 단, 보안성을 증가시키기 위하여, 사용자의 개인 단말기와의 직접 통신을 통하여 스마트카드의 대용으로 활용 가능하다. 개인 단말기를 사용하여 보안성을 높이는 것에 대해서는 도 7 및 도 8을 설명하면서 후술한다.

[0033] 도 1을 참조하면, 방송 콘텐츠 보안 시스템은 CAS시스템(100)과 연동하여 CAS시스템(100)에 대한 권한 제어를 수행하는 DRM시스템(200)을 포함한다. 이때, 도 2에 도시된 바와 같이, DRM시스템(200)은 방송 콘텐츠를 암호화하는 DRM암호화 모듈 및 암호화된 방송 콘텐츠에 대해 복호화가 가능하도록 사용자권한정보 및 복호화 키를 포함하는 라이센스를 생성하고 관리하는 위조 방지 모듈을 포함한다.

[0034] 구체적으로, DRM(Digital Right Management)시스템(200)은 방송 콘텐츠의 데이터를 암호화하여 유통하고, 사용자 인증 및 단말기에 대해 라이센스를 발급함으로써 방송 콘텐츠의 불법 복제를 방지할 수 있다. 도면에 도시하지는 않았지만, DRM시스템은 방송 콘텐츠를 암호화하는 DRM패키저와 라이센스를 이용하는 DRM클라이어트를 더 포함할 수 있다. 이때, 라이센스는 콘텐츠에 대한 사용권한과 복호화 키를 포함하며, 사용 권한에 대한 제한 조건과 비교함으로써 조건에 맞는 경우에만 복호화 기능을 수행한다.

[0035] 따라서, DRM시스템(200)의 위조 방지 모듈은 위조 방지(Tamper Resistance)기술을 통해 보호함으로써 악의적인 사용자에 의한 방송 콘텐츠 불법 유출을 차단할 수 있다. 위조 방지 모듈은 복호화 모듈에 의해 복호화된 채널키에 대한 사용이 중복된다고 판단하는 경우, 라이센스 인증을 차단할 수도 있다. 한편, DRM시스템은 VOD콘텐츠용 DRM과 멀티캐스트 콘텐츠용 DRM으로 구분될 수 있다.

[0036] 또한, DRM시스템(200)은 방송 콘텐츠 사용자를 인증하기 위해 사용자 정보를 기초로 인증키를 생성하는 사용자 인증 모듈; 및 생성된 인증키와 상기 채널키를 비교하여 일치 여부에 따라 복호화 키를 생성하여 암호화된 방송 콘텐츠에 대한 복호화를 수행하는 복호화 모듈을 더 포함할 수 있다. 여기서, 채널키는 방송 콘텐츠에 대한 수신 자격 정보를 포함하고, 인증키는 방송 콘텐츠 사용자에 대한 사용자ID 및 비밀번호를 포함한다. 한편, 인증키는 방송 콘텐츠 사용자에게 인증 부분키의 형태로 전달될 수도 있다.

[0037] 도 1을 참조하면, 방송 콘텐츠 보안 시스템은 CAS시스템(100) 및 DRM시스템(200)과 연동하여 동작하는 STB시스템(300)을 포함한다. STB시스템(300)은 상기 DRM시스템(200)으로부터 채널기를 수신하고 암호화된 방송 콘텐츠를 복호화 함으로서 안전하게 방송을 시청할 수 있다.

[0038] 도 3을 참조하면, 미디어 복호화 모듈이 DRM 멀티캐스터에서 보낸 암호화와 멀티캐스팅 된 콘텐츠를 받으면 미디어 복호화 모듈에서는 콘텐츠에 삽입된 $E_{Groupkey}(Channelkey)$ 를 키 복호화 모듈로 보낸다. 키 복호화 모듈에서는 가지고 있던 그룹키나 키 관리 서버(KMS)에서 보내온 그룹키(복호화 키)를 이용하여 암호화된 채널키를 복호화하여 채널키를 다시 미디어 복호화 모듈로 보낸다. 채널키를 받은 미디어 복호화 모듈에서 암호화된 콘텐츠를 채널키로 복호화 하면서 인증모듈에 채널키 사용함을 알리면 인증모듈은 수신 자격 정보를 생성한다.

[0039] 인증을 위한 수신 자격 정보는 도 3에 도시된 바와 같이, 사용자 ID(User_ID), 특정사용자의 셋톱박스를 한정시키기 위한 정보(Div_info), 채널키(channelkey)를 사용하는 채널 번호(Channel_num)로 구성되어 있다. User_ID는 처음 IPTV 서비스에 가입하였을 때 발급받는 사용자ID로서 각 방송 콘텐츠 사용자를 식별할 수 있는 정보이어야 하므로 중복이 없어야 한다. Div_info는 사용자의 특정 장치 ID로 사용자와 셋톱박스를 바인딩하기 위해 생성된 값을 의미한다. 본 명세서에서, 셋톱박스는 스크램블링 및 DRM이 동시에 적용된 콘텐츠를 시청할 수 있는 기능을 탑재한 모든 기기를 의미하며, 전통적인 셋톱박스 이외에도 기술의 발전에 따라 스마트폰, 스마트 TV 등 다양한 기기들이 될 수 있다.

[0040] Div_info는 User_ID와 셋톱박스 MAC 어드레스의 해쉬값으로 이루어진다. Channel_num은 현재 채널키를 사용하여 복호화하고 있는 채널의 번호로서 사용자가 채널에 대한 사용가능 여부를 판단할 수 있다.

[0041] 수신 자격 정보를 수신 자격 정보서버(REIS)로 보낼 때는 User_ID는 평문으로, Div_info와 Channel_num은 사용자의 개인키로 암호화하여 보낸다.

[0042] 이하에서는, 도 7 및 도 8을 참조하여, CAS 시스템과 DRM 시스템을 모두 포함하며, 특정 사용자가 휴대한 휴대기기를 인증기기로 하여, 사용자가 있는 다양한 화면에서 보안 콘텐츠를 시청할 수 있는 시스템에 대하여 상세

하게 설명한다.

[0043] 도 7을 참조하면, 콘텐츠 관리서버(500)는 키 관리, 인증 및 콘텐츠 제공의 기능을 수행하는 서버 또는 서버군을 의미한다. 이 경우, 콘텐츠 관리서버(500)는 휴대기기(400), 공유기(600) 및 셋탑박스 기능을 포함하는 디스플레이 기기(310)와 연동될 수 있다.

[0044] 휴대기기(400)은 디스플레이 기기(310)과 직접 또는 공유기(600)에 의하여 생성된 로컬 네트워크를 통하여 연결될 수 있으며, 콘텐츠 관리서버(500)과도 연결될 수 있다.

[0045] 도 8을 참조하면, 최초에 휴대기기(400)는 콘텐츠 관리서버(500)과 연결될 때에 인증요청을 하여 인증을 받게 된다. 이 때, 휴대기기(400)과 직접 또는 공유기(600)에 의하여 생성된 로컬 네트워크를 통하여 연결될 수 있는 디스플레이 기기(310)이 존재하는 경우, 휴대기기(400)는 디스플레이 기기(310)의 기능, 종류 또는 제품번호(제품 고유번호, UUID)를 문의하는 쿼리를 송신한다. 이 때, 디스플레이 기기는 쿼리에 대한 응답으로 기능, 제품번호, 또는 제품 종류에 대하여 응답을 전송하게 된다.

[0046] 이 때, 기능 또는 제품 종류가 디스플레이 기기 또는 오디오 기기 등 콘텐츠를 플레이할 수 있는 기기인 경우에는 휴대기기(400)는 기기의 응답을 저장한다.

[0047] 한편, 콘텐츠 관리서버(500)의 콘텐츠를 플레이하고자 하는 경우에는 디스플레이 기기(310)를 통하여, 그룹키를 휴대기기(400)에 요청한다. 그 경우, 휴대기기(400), 콘텐츠 관리서버(500) 및 디스플레이 기기(310)는 서로 간에 난수, 오프셋, 및 반복회수를 공유하게 된다. 이 경우, 난수, 오프셋, 및 반복회수의 공유 절차는 모든 연결이 확립되어 있는 휴대기기(310)에 의하여 개시된다.

[0048] 이 경우, 각 연결 중 어느 하나의 연결이 해킹되어 난수, 오프셋, 및 반복회수가 모두 유출되는 것을 방지하기 위하여, 난수, 오프셋, 및 반복회수를 휴대기기(400), 콘텐츠 관리서버(500) 및 디스플레이 기기(310)에서 일대일로 대응되도록 발생시키는 것이 바람직하다. 예를 들어, 난수는 콘텐츠 관리서버(500)에서, 오프셋은 휴대기기(400)에서, 반복회수는 디스플레이 기기(310)에서 각각 설정할 수도 있다.

[0049] 그 후, 디스플레이 기기(310)는 난수, 오프셋에 기초하여 일회성 인증값을 생성하여 콘텐츠 관리서버(500)에 전달할 수 있다. 예컨대, 디스플레이 기기(310)는 난수를 해쉬 함수를 오프셋 회수만큼 중첩 적용하여 일회성 인증값을 생성할 수 있다.

[0050] 콘텐츠 관리서버(500)는 일회성 인증값을 디스플레이 기기(310)과 동일한 알고리즘으로 연산한 후, 값을 비교하여 동일한 경우, 그룹키를 디스플레이 기기(310)에 전달하게 된다.

[0051] 한편, 디스플레이 기기(310)는 전달받은 그룹키를 활용하여 콘텐츠 관리서버(310)의 DRM을 해제하고 콘텐츠를 플레이하게 된다. 그룹키를 활용하는 방법은 전술한 바와 같다.

[0052] 다음으로 콘텐츠 관리서버(500)는 인증 업데이트를 디스플레이 기기(310)에 요청한다. 이렇게 인증 업데이트를 바로 디스플레이 기기(310)에 요청하는 것은 휴대기기의 통신 회수를 줄여서 휴대기기의 배터리 등의 리소스를 절약하기 위함이다.

[0053] 최초 인증 후, 콘텐츠 관리서버(500)으로부터 인증 업데이트를 요청받은 경우, 디스플레이 기기(310)는 오프셋, 이전 그룹키 전달 회수 및 동일한 난수에 기초하여 일회성 인증값을 다시 생성한다. 그리고, 일회성 인증값을 업데이트 하게 된다.

[0054] 업데이트를 반복회수만큼 반복한 후에는, 콘텐츠 관리서버(500)에서 휴대기기(400)에 난수, 오프셋, 및 반복회수 공유절차를 요청하고, 콘텐츠가 종료될 때까지 일회성 인증값 확인 프로세스를 반복한다. 여기서 일회성 인증값 확인 프로세스는 난수/오프셋/반복회수 및. 이전 그룹키 전달 회수에 기초하여 일회성 인증값을 생성하고 확인하는 절차를 의미한다. 따라서, 콘텐츠의 플레이가 종료될 때까지 계속 보안이 유지될 수 있다. 이 때, 휴대기기(400)가 디스플레이 기기(310)와 연결될 수 있는 커버리지, 예컨대, 블루투스로 직접 연결시, 블루투스 연결범위를 벗어나거나, 또는 공유기(600)를 통한 로컬 네트워크 연결시, 로컬 네트워크 커버리지를 벗어나는 경우에는, 디스플레이 기기(310)에서 인증 휴대기기가 인증범위 밖으로 벗어났음을 통지하고, 다시 커버리지에 휴대기기(400)이 들어올 때까지 콘텐츠의 플레이를 중단할 수 있다.

[0055] 따라서, 이러한 보안 연결을 통하여 콘텐츠 사용자는 이러한 보안 통신이 가능한 주변의 어떠한 디스플레이 기기(310)를 통해서도 셋톱박스 없이도 CAS 및 DRM 보안이 동시에 적용된 콘텐츠를 플레이할 수 있다.

[0056] 또한, 본 발명의 일 실시예에 따른 방송 콘텐츠 보안 하드웨어 방식과 소프트웨어 방식을 결합함으로써 비용 절

감과 동시에 악의적인 사용자로부터 콘텐츠를 효과적으로 보호할 수 있다. 또한, 본 발명은 하나의 플랫폼에서 CAS기술과 DRM기술을 동작함으로써 IPTV의 보안 신뢰성을 향상시킬 수 있다.

[0057] 이상 첨부된 도면을 참조하여 본 발명의 실시예들을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것은 아니고, 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형실시될 수 있다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

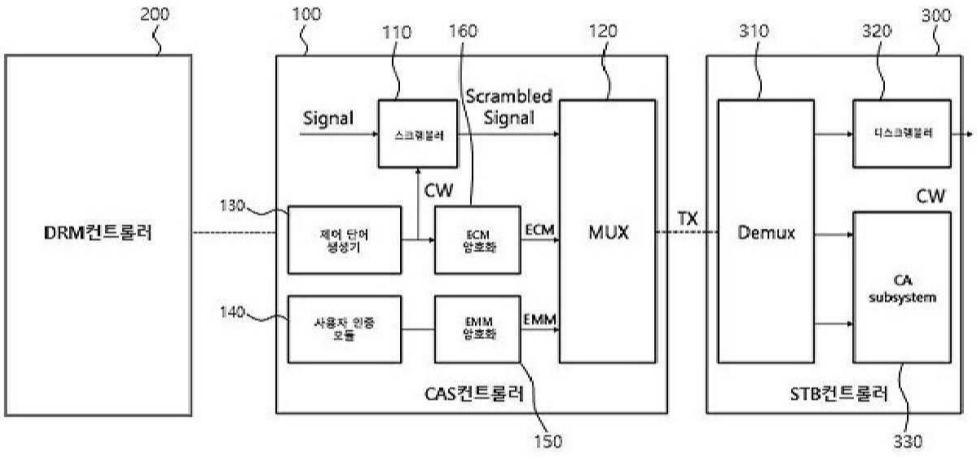
부호의 설명

[0058] 100: CAS시스템 200: DRM시스템

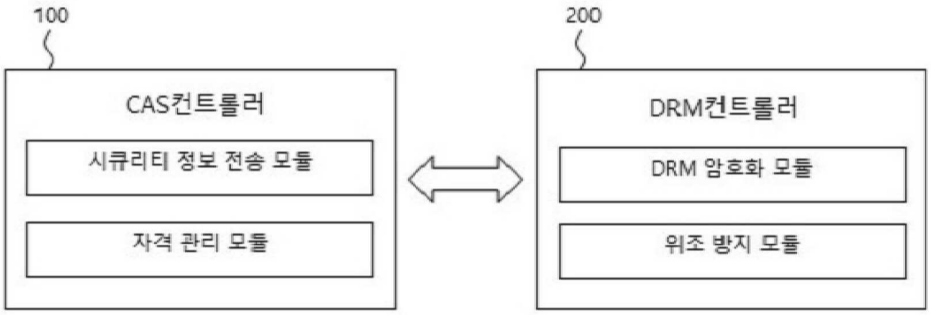
300: STB시스템

도면

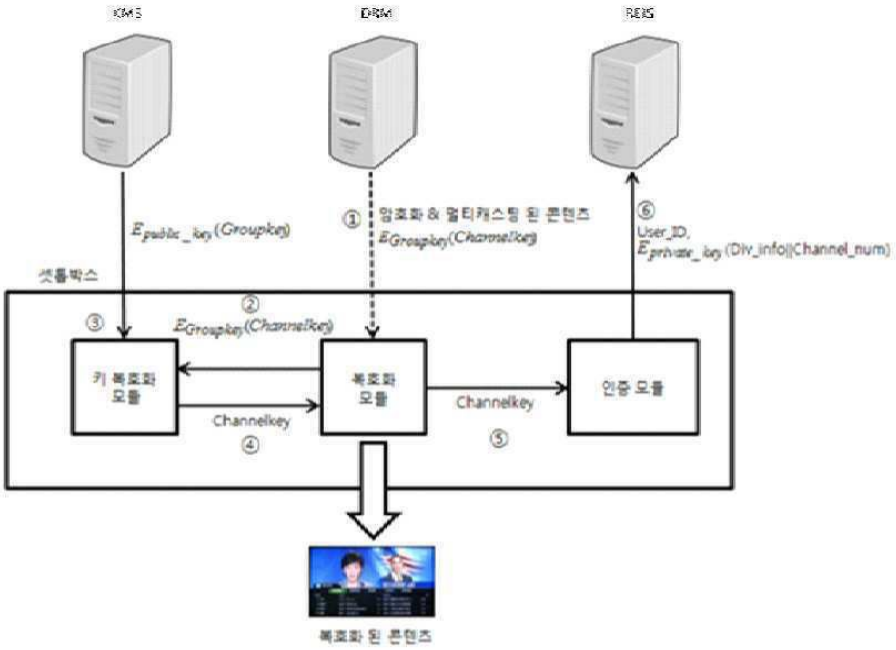
도면1



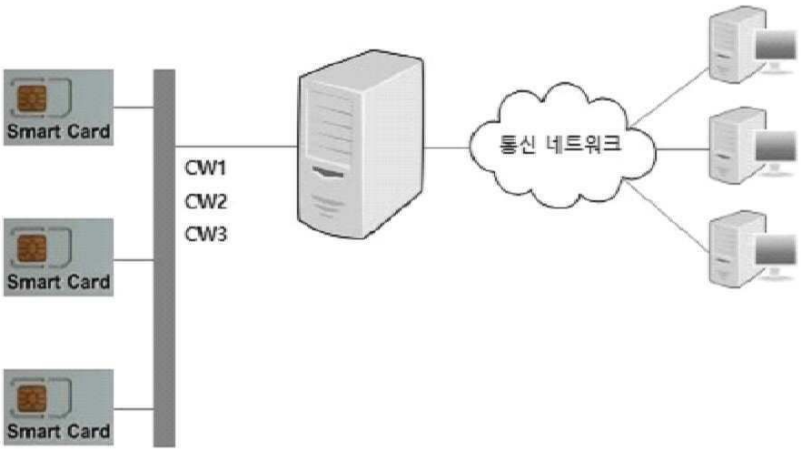
도면2



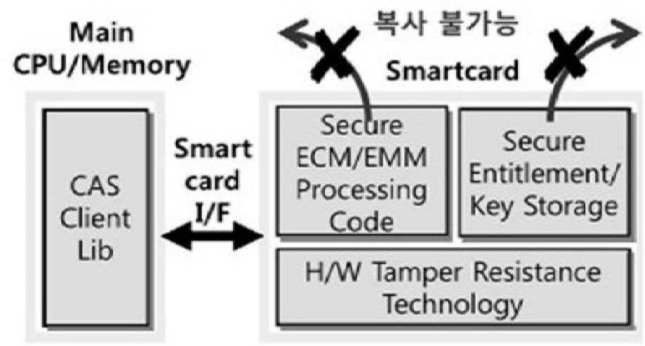
도면3


KMS
DRM
RMS
셋톱박스
① 암호화 & 멀티캐스팅 된 콘텐츠
② $E_{Groupkey}(Channelkey)$
③ $E_{public\_key}(Groupkey)$
④ Channelkey
⑤ Channelkey
⑥ User_ID, $E_{private\_key}$(Div_info||Channel_num)
키 복호화 모듈
복호화 모듈
인증 모듈
복호화 된 콘텐츠

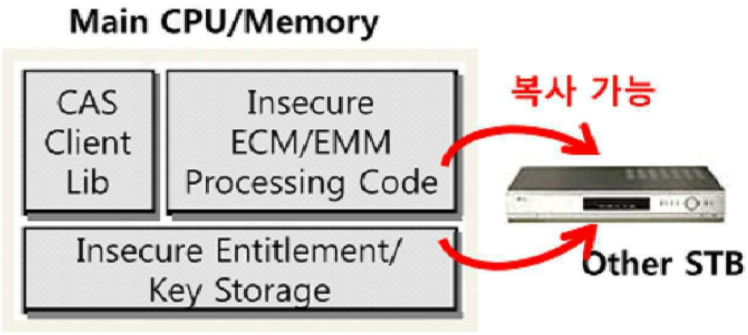
도면4


Smart Card
Smart Card
Smart Card
CW1
CW2
CW3
통신 네트워크

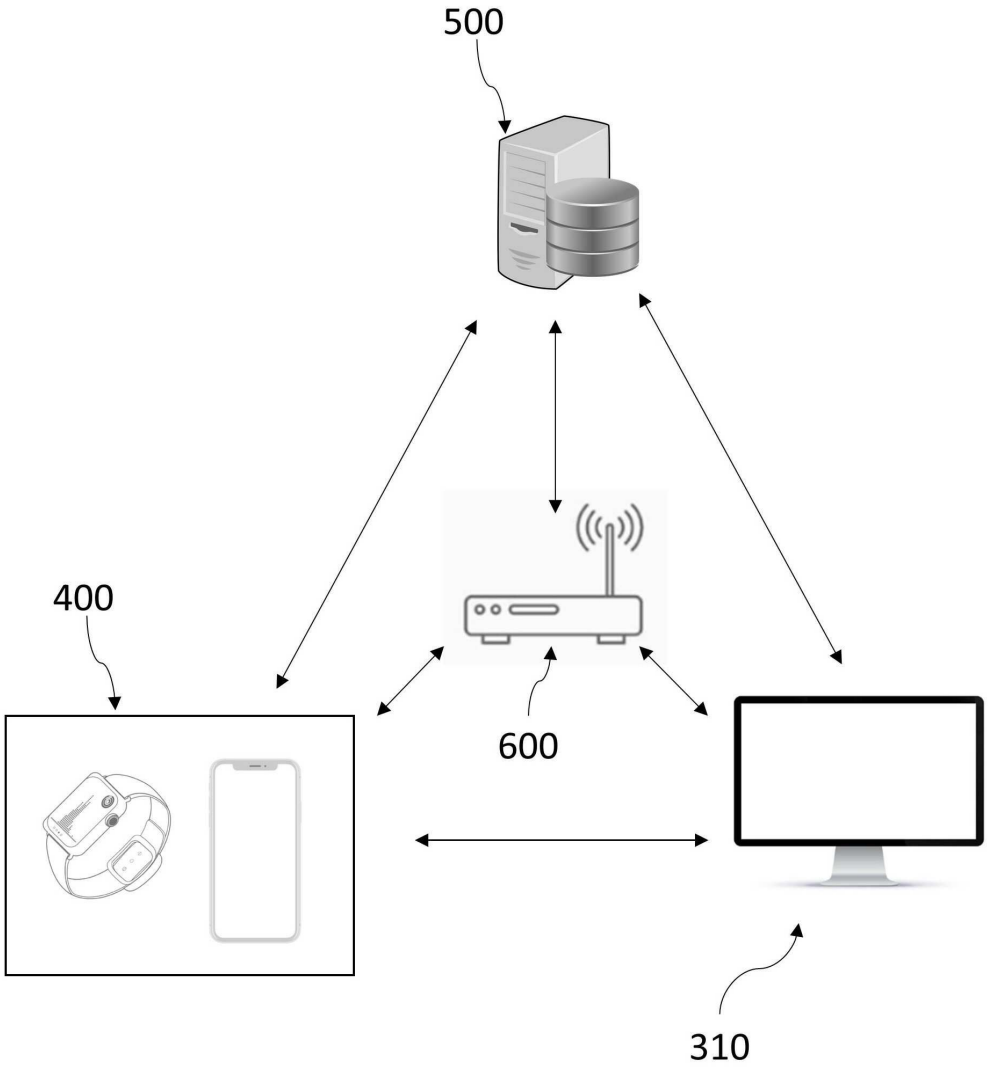
도면5


Main
CPU/Memory
복사 불가능
Smartcard
CAS
Client
Lib
Smart
card
I/F
Secure
ECM/EMM
Processing
Code
Secure
Entitlement/
Key Storage
H/W Tamper Resistance
Technology

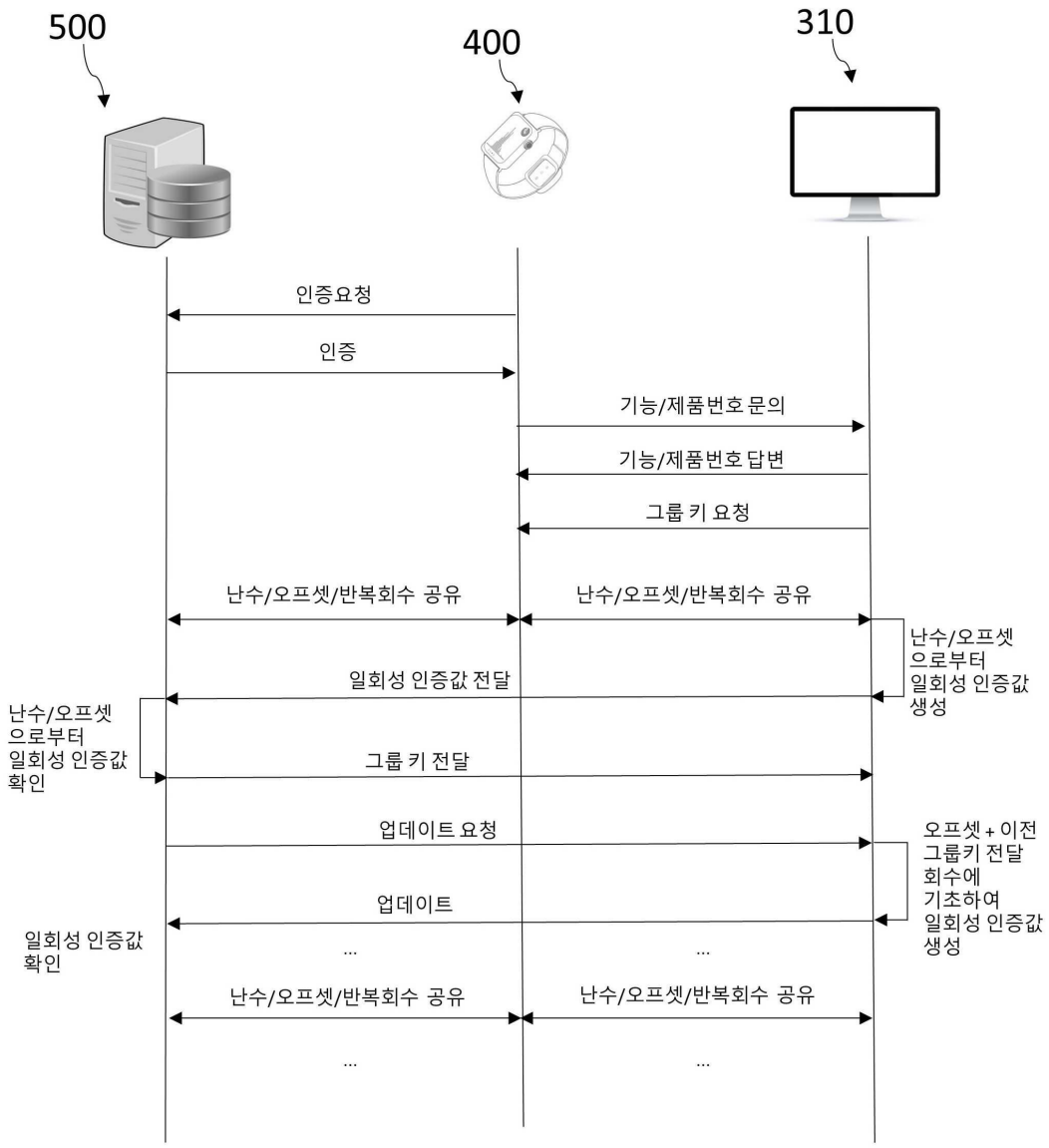
도면6


Main CPU/Memory
CAS
Client
Lib
Insecure
ECM/EMM
Processing Code
Insecure Entitlement/
Key Storage
복사 가능
Other STB

도면7



도면8


500
400
310
인증요청
인증
기능/제품번호 문의
기능/제품번호 답변
그룹 키 요청
난수/오프셋/반복회수 공유
난수/오프셋/반복회수 공유
난수/오프셋
으로부터
일회성 인증값
생성
일회성 인증값 전달
난수/오프셋
으로부터
일회성 인증값
확인
그룹 키 전달
업데이트 요청
오프셋 + 이전
그룹키 전달
회수에
기초하여
일회성 인증값
생성
업데이트
일회성 인증값
확인
...
...
난수/오프셋/반복회수 공유
난수/오프셋/반복회수 공유
...
...