(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년01월14일
(11) 등록번호 10-0936885
(24) 등록일자 2010년01월06일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2007-0127380
(22) 출원일자 2007년12월10일
심사청구일자 2007년12월10일
(65) 공개번호 10-2009-0060528
(43) 공개일자 2009년06월15일
(56) 선행기술조사문헌
JP2005245010 A
KR1020070057318 A
KR1020080041369 A
KR1020010090167A
전체 청구항 수 : 총 20 항

(73) 특허권자
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
권은정
대전시 서구 만년동 상아아파트 102동 603호
구한승
대전시 서구 삼천동 가람아파트 10동 1302호
(뒷면에 계속)
(74) 대리인
특허법인무한

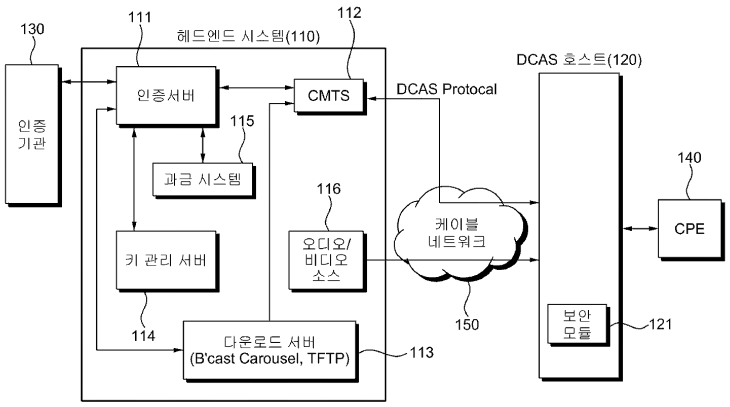
심사관 : 강윤석

(54) 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및그 장치

(57) 요 약

본 발명은 헤드엔드 시스템 및 DCAS(Downloadable Conditional Access System) 호스트를 포함하는 제한수신시스템에서의 상호 간을 인증하기 위한 방법 및 그 장치에 관한 것으로, 더욱 상세하게는 헤드엔드 시스템의 인증서버와 DCAS 호스트의 보안모듈 간 상호 인증 후에 CAS 소프트웨어를 보안모듈(121)로 다운로드하는 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및 그 장치에 관한 것이다. 본 발명에 의하면 케이블 네트워크에서 헤드엔드의 인증서버와 DCAS 호스트의 보안모듈 간의 상호 인증 프로토콜을 제공하여, 스마트 카드 또는 케이블 카드와 같은 하드웨어 기반의 실체 인증이 필요 없는 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및 그 장치를 제공할 수 있다.

대 표 도



(72) 발명자

김순철

대전시 유성구 반석동 622 양지마을5단지아파트 503동 1101호

정영호

대전시 유성구 관평동 대우푸르지오 210동 304호

권오형

대전시 유성구 어은동 한빛아파트 107동 1103호

이수인

대전시 서구 둔산동 크로바아파트 106동 606호

김희정

대전시 유성구 노은동 열매마을아파트 802동 1101호

이 발명을 지원한 국가연구개발사업

과제고유번호	2007-S-007-01
부처명	정보통신부 및 정보통신연구진흥원
연구사업명	IT성장동력기술개발
연구과제명	Downloadable 제한수신 시스템 개발
주관기관	한국전자통신연구원
연구기간	2007년 03월 01일 ~ 2008년 02월 29일

특허청구의 범위

청구항 1

보안모듈에서의, 다운로드가능한 제한수신시스템의 상호 간을 인증하기 위한 방법에 있어서,

인증서버로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하는 단계;

상기 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증 메시지를 상기 인증서버로 전송하는 단계;

상기 인증서버로부터 상기 서명검증 메시지로부터 생성된 제2 공유세션키에 대한 서명검증확인 메시지를 수신하는 단계; 및

상기 서명검증확인 메시지로부터 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상호인증결과 정보를 생성하고, 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 2

제1항에 있어서,

인증서버로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하는 상기 단계는,

상기 인증서버로부터 인증표시 메시지를 수신하고, 상기 인증표시 메시지로부터 상기 인증서버의 공개키를 획득하여 상기 인증표시 메시지를 검증하는 단계; 및

상기 인증서버로부터 다운로드 메시지를 수신하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 3

제2항에 있어서,

상기 인증서버로부터 다운로드 메시지를 수신하는 상기 단계는,

상기 다운로드 메시지에 대한 서명 검증을 수행하는 단계; 및

상기 인증서버로 세션키요청 메시지를 전송하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 4

제2항에 있어서,

상기 인증표시 메시지는 상기 인증서버의 인증서 정보, 또는 상기 CAS 소프트웨어의 버전 정보를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 5

제2항에 있어서,

상기 다운로드 메시지는 상기 CAS 소프트웨어의 업데이트를 위한 스케줄 정보, 세션 키 요청 정보, 또는 구매내역기록 요청 정보를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 6

제3항에 있어서,

상기 세션키요청 메시지는 보안모듈의 인증서 정보 또는 세션키생성유도 정보를 포함하는 것을 특징으로 하는

상호 인증 방법.

청구항 7

제1항에 있어서,

상기 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증 메시지를 상기 인증서버로 전송하는 상기 단계는

상기 인증서버로부터, 인증기관에서 생성된 제1 랜덤 값, 및 상기 인증기관에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값을 포함하는 세션키응답 메시지를 수신하는 단계; 및

DCAS 호스트의 고유 정보, 상기 시드 값, 보안모듈에서 생성된 제2 랜덤 값, 또는 상기 보안모듈의 하드웨어/소프트웨어에 대한 버전 정보로부터 상기 제1 공유세션키를 생성하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 8

제7항에 있어서,

DCAS 호스트의 고유 정보, 상기 시드 값, 보안 모듈에서 생성된 제2 랜덤 값, 또는 상기 보안모듈의 하드웨어/소프트웨어에 대한 버전 정보로부터 상기 제1 공유세션키를 생성하는 상기 단계는,

상기 고유 정보, 상기 제2 랜덤 값, 상기 하드웨어/소프트웨어의 상기 버전 정보, 또는 상기 시드 값을 입력 값으로 하는 해쉬 함수를 수행하는 단계;

상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수를 수행하는 단계; 및

상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 제1 공유세션키로 선택하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 9

제8항에 있어서,

상기 서명검증 메시지는 상기 DCAS 호스트의 상기 고유 정보, 상기 제2 랜덤 값, 또는 상기 하드웨어/소프트웨어의 상기 버전 정보를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 10

제1항에 있어서,

상기 서명검증확인 메시지로부터 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상호인증결과 정보를 생성하고, 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하는 상기 단계는,

초기 벡터 값 및 상기 제1 공유세션키로 암호화된 상기 서명검증확인 메시지를 대칭키 암호 알고리즘을 통하여 복호화하여 상호인증결과 정보를 생성하며, 상기 상호인증결과 정보를 상기 인증서버로 전송하는 단계; 및

상기 인증서버로부터 상기 CAS 소프트웨어의 다운로드를 위한 다운로드 정보 메시지를 수신하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 11

제10항에 있어서,

상기 다운로드 정보 메시지는

상기 CAS 소프트웨어가 저장된 서버의 IP 어드레스, 소프트웨어 식별정보, 프로토콜 정보, 또는 구매내역기록 요청 정보를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 12

제10항에 있어서,

상기 서명검증확인 메시지로부터 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상호인증결과 정보를 생성하고, 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하는 상기 단계는,

상기 다운로드 정보로부터 상기 CAS 소프트웨어를 다운로드 서버로부터 다운로드하고, 상기 CAS 소프트웨어에 대한 다운로드상태 정보를 포함하는 다운로드확인 메시지를 상기 인증서버로 전송하는 단계

를 더 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 13

제12항에 있어서,

상기 다운로드 정보로부터 상기 CAS 소프트웨어를 다운로드 서버로부터 다운로드하고, 상기 CAS 소프트웨어에 대한 다운로드상태 정보를 포함하는 다운로드확인 메시지를 상기 인증서버로 전송하는 상기 단계는,

구매내역기록 정보를 포함하는 구매내역 메시지를 상기 인증서버로 전송하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 14

인증서버에서의, 다운로드가능한 제한수신시스템의 상호 간을 인증하기 위한 방법에 있어서,

인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, 보안모듈로 상기 세션키 생성 정보를 전송하는 단계;

상기 보안모듈로부터 상기 세션키 생성 정보로부터 생성된 제1 공유세션키에 대한 서명검증 메시지를 수신하는 단계; 및

상기 서명검증 메시지로부터 제2 공유세션키를 생성하고, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 15

제14항에 있어서,

인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, 보안모듈로 상기 세션키 생성 정보를 전송하는 상기 단계는,

상기 인증기관에서 생성된 제1 랜덤 값, 또는 상기 인증기관에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값을 포함하는 세션키응답 메시지를 수신하는 단계; 및

상기 세션키응답 메시지를 상기 보안모듈로 전송하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 16

제15항에 있어서,

상기 시드 값은 상기 보안모듈 및 상기 인증기관이 사전에 공유하고 있는 사전공유키를 입력 값으로 하여 상기 키 생성 알고리즘을 통하여 생성된 것임을 특징으로 하는 상호 인증 방법.

청구항 17

제15항에 있어서,

상기 서명검증 메시지는 DCAS 호스트의 고유 정보, 상기 보안모듈에서 생성된 제2 랜덤 값, 또는 상기 보안모듈

의 하드웨어/소프트웨어의 버전 정보를 포함하고,

상기 서명검증 메시지로부터 제2 공유세션키를 생성하고, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송하는 상기 단계는,

상기 서명검증 메시지, 상기 시드 값, 및 상기 제1 랜덤 값으로부터 상기 제2 공유세션키를 생성하는 단계; 및

상기 제2 공유세션키 및 초기 벡터 값을 입력으로 하여 소정의 대칭키 암호 알고리즘을 통하여 상기 고유 정보, 클라이언트 정보를 암호화하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 18

제17항에 있어서,

상기 서명검증 메시지, 상기 시드 값, 및 상기 제1 랜덤 값으로부터 상기 제2 공유세션키를 생성하는 상기 단계는,

상기 DCAS 호스트의 상기 고유 정보, 상기 제2 랜덤 값, 상기 하드웨어/소프트웨어의 상기 버전 정보, 또는 상기 시드 값을 입력 값으로 하는 해쉬 함수를 수행하는 단계;

상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수를 수행하는 단계; 및

상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 제2 공유세션키로 선택하는 단계

를 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 19

제17항에 있어서,

상기 서명검증확인 메시지는 상기 DCAS 호스트의 상기 고유 정보, 상기 클라이언트 정보, 또는 상기 초기 벡터 값을 포함하는 것을 특징으로 하는 상호 인증 방법.

청구항 20

다운로드 가능한 제한수신시스템에서의 상호 간을 인증하기 위한 장치에 있어서,

인증기관으로부터 수신한 공유세션키 생성을 위한 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증 메시지를 생성하는 보안모듈; 및

상기 서명검증 메시지를 수신하고 상기 서명검증 메시지로부터 제2 공유세션키를 생성하며, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송하는 인증서버

를 포함하고,

상기 보안모듈은 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상기 판단 결과로부터 상호인증결과 정보를 생성하고, 생성된 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하는 것을 특징으로 하는 상호 인증 장치.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 헤드엔드 시스템 및 DCAS(Downloadable Conditional Access System) 호스트를 포함하는 제한수신시스템에서의 상호 간을 인증하기 위한 방법 및 그 장치에 관한 것으로, 더욱 상세하게는 헤드엔드 시스템의 인증서버와 DCAS 호스트의 보안모듈 간 상호 인증 후에 CAS 소프트웨어를 보안모듈(121)로 다운로드하는 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및 그 장치에 관한 것이다.

<2> 본 발명은 정보통신부 및 정보통신연구진흥원의 IT성장동력기술개발사업의 일환으로 수행한 연구로부터 도출된

것이다[과제관리번호: 2007-S-007-01, 과제명: Downloadable 제한수신 시스템 개발].

배 경 기 술

<3> 제한수신시스템(CAS, Conditional Access System)은 방송 프로그램에 암호를 삽입하여 시청이 허가된 가입자들에 대해서만 유료 방송 프로그램을 시청할 수 있는 권한을 부여해주는 시스템이다. 현재 디지털 케이블 방송에서는 유료 방송 서비스를 제공하기 위해서는 CA(Conditional Access) 응용의 구현 형태에 따라 대부분 스마트 카드 또는 PCMCIA 카드 형태의 케이블카드를 이용하고 있다. 그러나, 종래의 제한수신시스템에서는 CAS 소프트웨어(또는 CAS 클라이언트 이미지)를 스마트 카드 또는 PCMCIA 카드를 통해 오프라인(off-line)으로 배포함으로써, 제한수신시스템의 결함 발생 시에 카드를 재발급하는 과정에 일정 시간이 소요되어 상기 결함에 대한 신속한 대처가 어렵고, 상기 카드의 재발급으로 인한 추가 비용이 소요된다는 문제점이 있었다.

<4> 이러한 단점을 극복하고자, 최근 양방향 케이블 통신 네트워크를 기반으로 다운로드 가능한 제한수신시스템(DCAS, Downloadable Conditional Access System) 기술 개발이 이슈가 되고 있다. DCAS 기술이란 종래와 같이 CAS 사업자가 스마트 카드 또는 PCMCIA 카드에 선정된 CAS 소프트웨어를 설치하여 유료방송 서비스를 제공하는 것이 아니라, 셋탑박스(set-top box)에 상기 CAS 소프트웨어가 설치될 수 있는 보안모듈을 탑재하여 상기 양방향 케이블 통신 네트워크를 통해 상기 CAS 소프트웨어의 결함이 발생하거나 상기 CAS 소프트웨어의 버전 업데이트와 같은 상황에서 용이하게 상기 CAS 소프트웨어를 갱신할 수 있도록 하는 기술이다.

<5> 또한, DCAS 기술에서는 단일 보안모듈 칩(chip)에 복수의 CA 시스템을 처리할 수 있기 때문에, 케이블 사업자는 특정 CAS 솔루션에 종속되지 않고 CAS 업체를 선택할 수 있어, 상기 CAS 업체들 간의 경쟁 유도를 통해 다양한 형태의 서비스 개발을 촉진할 수 있다. 그러나 인증되지 않은 상태의 가입자 셋탑박스로 상기 CAS 소프트웨어를 전송할 경우, 상기 가입자는 불법적으로 유료 방송 서비스의 시청이 가능하고, 예측하지 못한 상황을 발생시킬 수 있고 또한, 셋탑박스에 탑재될 보안모듈이 헤드엔드 시스템에 위치한 인증서버를 인증하지 않을 경우 인증서버(111)를 가장한 제3의 서버로부터 공격을 받을 수가 있기 때문에 상기 다운로드 가능한 제한수신 시스템을 개발하기 위해서는 인증서버와 셋탑박스에 탑재될 보안모듈 간의 상호인증이 수행되어야 한다.

<6> 따라서, 다운로드 가능한 제한수신 시스템에서 전술한 바와 같은 보안상의 문제점을 해결하기 위한 효과적인 상호 인증 방법이 요구되고 있다.

발명의 내용

해결 하고자하는 과제

<7> 본 발명은 케이블 네트워크에서 헤드엔드의 인증서버와 DCAS 호스트의 보안모듈 간의 상호 인증 프로토콜을 제공하여, 스마트 카드 또는 케이블 카드와 같은 하드웨어 기반의 실체 인증이 필요 없는 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및 그 장치를 제공하고자 하는 것이다.

<8> 또한, 본 발명은 다운로드 가능한 제한수신시스템에서 CAS 소프트웨어를 전송하는 과정 중 발생하는 트래픽 데이터 암호화/복호화, 메시지 인증, 또는 장치 인증과 같은 다양한 보안 프로세스의 처리가 가능한 효과적인 상호 인증 프로토콜을 제공하고자 하는 것이다.

<9> 또한, 본 발명은 실체 인증이 필요없는 다운로드 가능한 제한수신 시스템에서의 상호 인증 방법을 제공하여 인증 프로세스에 소요되는 운용비용을 절감하고, 제한수신시스템에서의 결함 발생 시에 빠른 시스템 갱신이 가능한 다운로드 가능한 제한수신 시스템에서의 상호 인증 방법 및 그 장치를 제공하고자 하는 것이다.

과제 해결수단

<10> 상기의 목적을 이루고 종래기술의 문제점을 해결하기 위하여, 본 발명은 보안모듈에서의, 다운로드가능한 제한수신시스템의 상호 간을 인증하기 위한 방법에 있어서, 인증서버로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하는 단계; 상기 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증 메시지를 상기 인증서버로 전송하는 단계; 상기 인증서버로부터 상기 서명검증 메시지로부터 생성된 제2 공유세션키에 대한 서명검증확인 메시지를 수신하는 단계; 및 상기 서명검증확인 메시지로부터 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상호인증결과 정보를 생성하고, 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하는 단계를 포함하는 것을 특징으로 하는 상호 인증 방법을 제공한다.

<11> 본 발명의 일측에 따르면, 인증서버에서의, 다운로드가능한 제한수신시스템의 상호 간을 인증하기 위한 방법에 있어서, 인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, 보안모듈로 상기 세션키 생성 정보를 전송하는 단계; 상기 보안모듈로부터 상기 세션키 생성 정보로부터 생성된 제1 공유세션키에 대한 서명검증 메시지를 수신하는 단계; 및 상기 서명검증 메시지로부터 제2 공유세션키를 생성하고, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송하는 단계를 포함하는 것을 특징으로 하는 상호 인증 방법이 제공된다.

<12> 본 발명의 다른 일측에 따르면, 다운로드 가능한 제한수신시스템에서의 상호 간을 인증하기 위한 장치에 있어서, 인증기관으로부터 수신한 공유세션키 생성을 위한 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증 메시지를 생성하는 보안모듈; 및 상기 서명검증 메시지를 수신하고 상기 서명검증 메시지로부터 제2 공유세션키를 생성하며, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송하는 인증서버를 포함하고, 상기 보안모듈은 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상기 판단 결과로부터 상호인증결과 정보를 생성하고, 생성된 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하는 것을 특징으로 하는 상호 인증 장치가 제공된다.

효 과

<13> 본 발명에 의하면 케이블 네트워크에서 헤드엔드의 인증서버와 DCAS 호스트의 보안모듈 간의 상호 인증 프로토콜을 제공하여, 스마트 카드 또는 케이블 카드와 같은 하드웨어 기반의 실체 인증이 필요 없는 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및 그 장치를 제공할 수 있다.

<14> 또한, 본 발명에 의하면 다운로드 가능한 제한수신시스템에서 CAS 소프트웨어를 전송하는 과정 중 발생하는 트래픽 데이터 암호화/복호화, 메시지 인증, 또는 장치 인증과 같은 다양한 보안 프로세스의 처리가 가능한 효과적인 상호 인증 프로토콜이 제공된다.

<15> 또한, 본 발명에 의하면 실체 인증이 필요 없는 다운로드 가능한 제한수신 시스템에서의 상호 인증 방법을 제공하여 인증 프로세스에 소요되는 운용비용을 절감하고, 제한수신시스템에서의 결함 발생 시에 빠른 시스템 갱신이 가능한 다운로드 가능한 제한수신 시스템에서의 상호 인증 방법 및 그 장치가 제공된다.

발명의 실시를 위한 구체적인 내용

<16> 이하 첨부된 도면을 참조하여 본 발명에 따른 다운로드 가능한 제한수신시스템에서의 상호 인증 방법 및 그 장치를 상세히 설명한다. 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 바람직한 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

<17> 본 발명의 'CAS 호스트' 또는 'DCAS 호스트'는 가입자 단말기를 지칭한다.

<18> 또한, 본 발명의 인증기관, 인증서버 및 보안모듈사이에 송수신되는 메시지에 대한 규약 및 절차에 관한 통신 메커니즘을 DCAS 프로토콜이라 정의한다.

<19> 도 1은 본 발명의 일실시예에 의한 상호 인증 장치를 포함하는 다운로드 가능한 제한수신시스템을 도시한 것이다.

<20> 도 1을 참조하면, 본 발명의 다운로드 가능한 제한수신시스템(DCAS)는 헤드엔드 시스템(110), DCAS 호스트(120), 및 인증기관(130)을 포함한다. DCAS 호스트(120)의 보안모듈(121)은 헤드엔드 시스템(110)의 인증서버(111)와 인증에 필요한 정보를 관리하기 위해 케이블 사업자가 아닌 제3의 인증기관(130)을 활용함으로써 셋탑박스(STB), 셋탑 디바이스(STD), 또는 모바일 또는 휴대용 장치를 포함하는 다른 고객 댁내 장치(CPE, Consumer Premise Equipment)(140)에 개선된 비디오 및 미디어 기술을 보호하기 위한 CAS 소프트웨어를 DCAS 호스트(120)로 공급한다.

<21> 인증기관(120)은 헤드엔드 시스템(110)의 인증서버(111)와 안정한 통신을 수행하며 인증에 필요한 정보를 제공한다. 인증서버(111)는 인증기관(130)으로부터 전송 받은, 인증에 필요한 세션키 생성을 위한 정보를 케이블모뎀종단시스템(CMTS, Cable Modem Termination System)(112)을 경유하여 보안모듈(109)로 전송한다. 상호 인증

과정에서 발생하는 모든 키 정보는 키 관리 서버(114)에서 관리되고, 상호 인증이 정상적으로 완료된 후에는 CAS 소프트웨어가 다운로드 서버(113) 및 CMTS(112) 를 통하여 보안모듈(121)로 전송된다.

<22> 따라서, 상기 CAS 소프트웨어를 다운로드(또는 업데이트)한 보안모듈(121)은 스크램블되어 전송되는 방송 신호에 대한 시청허가를 획득하여 가입자에게 CPE(140)를 통해 유료방송 서비스를 제공할 수 있다.

<23> 상술한 인증기관(130), 인증서버(111) 및 보안모듈(121)사이에 송수신되는 메시지에 대한 규약 및 절차에 관한 통신 메커니즘을 DCAS 프로토콜이라고 정의하고, 상기 DCAS 프로토콜을 기반으로 인증기관(130), 인증서버(111) 및 보안모듈(121) 사이에 송수신되는 메시지에 대한 보안 및 이들 간의 상호 인증이 수행된다. 상술한 상기 DCAS 프로토콜에 대해서는 도 3을 참조하여 상세히 설명하기로 한다.

<24> 도 3은 본 발명의 일실시예에 의한 DCAS 프로토콜 계층을 포함하는 다운로드 가능한 제한수신시스템에서의 프로토콜을 도시한 것이다.

<25> 도 3을 참고하면, 본 발명의 다운로드 가능한 제한수신시스템에서의 프로토콜은 케이블 네트워크를 통한 DOCSIS 계층(320), IP 계층(330), 및 UDP/ TCP 계층(340)과는 독립적으로 동작하는 DCAS 프로토콜 계층(350)을 포함한다.

<26> DCAS 프로토콜을 기반으로 본 발명의 상호 인증 장치는 CAS 소프트웨어를 DCAS 호스트의 보안모듈로 안전하게 전송하기 위하여, 상기 전송 전에 상기 인증서버와 상기 보안 모듈 간의 상호 인증을 수행한다. 상기 상호 인증을 위한 상호 인증 장치에 대해서는 도 2를 참조하며 상세히 설명하기로 한다.

<27> 도 2는 본 발명의 일실시예에 의한 다운로드 가능한 제한수신시스템에서의 상호 인증 장치의 구성을 도시한 것이다.

<28> 도 2를 참조하면, 본 발명의 상호 인증 장치(100)는 보안모듈(121), 및 인증서버(111)를 포함한다.

<29> 보안모듈(121)은 인증기관(130)으로부터 수신한 공유세션키 생성을 위한 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증(ClientSignOn) 메시지를 생성한다. 보안모듈(121)은 DCAS 호스트(120) 내에 위치할 수 있다. 인증서버(111)는 보안모듈(121)로부터 상기 서명검증 메시지를 수신하여 상기 서명검증 메시지로부터 제2 공유세션키를 생성하며, 상기 제2 공유세션키에 대한 서명검증확인(ClientSignOnConfirm) 메시지를 보안모듈(121)로 전송한다. 즉, 보안모듈(121)은 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상기 판단 결과로부터 상호인증결과 정보를 생성하고, 생성된 상기 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신한다.

<30> 구체적으로는, 보안모듈(121) 및 인증서버(111)는 서로 공유하기 위한 공유세션키를 생성하기 위하여, 보안모듈(121)은 인증서버(111)로부터 인증서버(111)의 인증서(AP_Certificate) 정보, 및/또는 상기 CAS 소프트웨어의 버전 정보(SM Client Version)를 포함하는 인증표시(SecurityAnnounce) 메시지를 수신하고, 상기 인증표시(SecurityAnnounce) 메시지로부터 인증서버(111)의 공개키를 획득하여 상기 인증표시(SecurityAnnounce) 메시지를 검증한다. 이에 인증서버(111)는 상기 CAS 소프트웨어의 업데이트를 위한 스케줄 정보(DownloadSchedule), 세션 키 요청 정보(KeyRequest_REQ), 또는 구매내역기록 요청 정보(PurchaseReport_REQ)를 포함하는 다운로드(DCASDownload) 메시지를 보안모듈(121)로 전송한다.

<31> 이후, 보안모듈(121)은 인증서버(111)로 보안모듈(121)의 인증서(SM_Certificate) 정보 및/또는 세션키생성유도정보(KeyPairingID)를 포함하는 세션키요청(KeyRequest) 메시지를 전송하고, 인증서버(111)는 상기 세션키요청 메시지를 인증기관(130)으로 전송하고, 인증기관(130)에서 생성된 제1 랜덤 값(RAND_TA), 및/또는 인증기관(130)에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값(Kc)를 포함하는 세션키응답(KeyResponse) 메시지를 수신한다. 상기 시드 값(Kc)은 보안모듈(121) 및 인증기관(111)이 사전에 공유하고 있는 사전공유키(PSK, Pre-shared Key)를 입력 값으로 하여 상기 키 생성 알고리즘을 통하여 생성된다.

<32> 또한, 보안모듈(121)은 상술한 여러 정보 및 값들을 이용하여 공유세션키를 생성하는데, 구체적으로 인증서버(111)는 보안모듈(121)로 상기 제1 랜덤 값(RAND_TA)을 포함하는 상기 세션키응답 메시지를 전송하고, 보안모듈(121)은 DCAS 호스트(120)의 고유 정보(SM_ID), 상기 시드 값(Kc), 보안모듈(121)에서 생성된 제2 랜덤 값(NONCE_SM), 또는 보안모듈(121)의 하드웨어/소프트웨어에 대한 버전 정보(HW_SW_Version)로부터 상기 제1 공유세션키를 생성한다. 즉, 보안모듈(121)은 상기 고유 정보(SM_ID), 상기 제2 랜덤 값(NONCE_SM), 상기 하드웨어/소프트웨어의 버전 정보(HW_SW_Version), 또는 상기 시드 값(Kc)을 입력 값으로 하는 해쉬 함수(hash function)를 수행하고, 상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수(random

function)를 수행하며, 상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 제1 공유세션키로 선택하게 된다.

<33> 인증서버(111) 역시 보안모듈(121)과 세션키를 공유하기 위하여 보안모듈(121)로부터 서명검증 메시지(ClientSignOn) 수신하고, 상기 고유 정보(SM_ID), 상기 제2 랜덤 값(NONCE_SM), 또는 상기 하드웨어/소프트웨어의 버전 정보(HW_SW_Version)를 포함하는 상기 서명검증 메시지로부터 제2 공유세션키를 생성하고, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송하는데, 구체적으로는 상기 서명검증 메시지, 상기 시드 값(Kc) 및 상기 제1 랜덤 값(RAND_TA)으로부터 제2 공유세션키를 생성한다.

<34> 즉, 인증서버(111)는 상기 고유 정보(SM_ID), 상기 제2 랜덤 값(NONCE_SM), 상기 하드웨어/소프트웨어의 버전 정보(HW_SW_Version), 또는 상기 시드 값(Kc)을 입력 값으로 하는 해쉬 함수(hash function)를 수행하고, 상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수(random function)를 수행하며, 상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 제2 공유세션키로 선택하게 된다.

<35> 보안모듈(121)은 상기 서명검증확인 메시지로부터 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여 헤드엔드 시스템(110)으로부터 CAS 소프트웨어를 수신하게 되는데, 즉, 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부로부터 상호 인증의 성공 여부가 판단된다. 즉, 상호 인증이 성공하는 경우, 보안모듈(121)은 CAS 소프트웨어를 다운로드하게 된다.

<36> 구체적으로는, 인증서버(111)에서 상기 제2 공유세션키 및 초기 벡터 값(IV, Initial Vector)를 입력으로하여 소정의 대칭키 암호 알고리즘을 통하여 상기 고유 정보(SM_ID), 클라이언트 정보(SM_Client_Info_Set)를 암호화하고, 상기 고유 정보(SM_ID), 상기 클라이언트 정보(SM_Client_Info_Set), 또는 상기 초기 벡터 값을 포함하는 상기 서명검증확인(ClientSignOnConfirm) 메시지를 생성하여 보안모듈(121)로 전송한다. 보안모듈(121)은 상기 초기 벡터 값 및 상기 제1 공유세션키로 암호화된 상기 서명검증확인 메시지를 대칭키 암호 알고리즘을 통하여 복호화하여 상호인증결과 정보(Success/Failure)를 생성하여, 상기 상호인증결과 정보를 상기 인증서버로 전송하고, 인증서버(111)는 상기 상호인증결과 정보를 분석하고, 상기 상호인증결과 정보가 성공(success)인 경우, 상기 CAS 소프트웨어의 다운로드를 위한, 상기 CAS 소프트웨어가 저장된 서버의 IP 어드레스(DS_IP), 소프트웨어 식별정보(FN), 프로토콜 정보(TM), 또는 구매내역기록 요청 정보(PurchaseReport_REQ)를 포함하는 다운로드 정보(DownloadInfo) 메시지를 보안모듈(121)로 전송하게 된다. 이후, 보안모듈(121)은 상기 다운로드 정보 메시지로부터 상기 CAS 소프트웨어를 다운로드 서버로부터 다운로드하게 된다.

<37> 도 4a는 본 발명의 일실시예에 의한 다운로드 가능한 제한수신시스템에서의 상호 인증 방법을 도시한 흐름도이다.

<38> 도 4a를 참조하면, 우선 헤드엔드 시스템에 포함되는 인증서버는 인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, DCAS 호스트에 포함되는 보안모듈은 상기 인증서버로부터 상기 세션키 생성 정보를 수신한다(단계(S410)). 이후, 상기 보안모듈은 상기 세션키 생성 정보로부터 제1 공유세션키를 생성하고, 상기 생성된 제1 공유세션키에 대한 서명검증(ClientSignOn) 메시지를 상기 인증서버로 전송한다(단계(s420)). 이후, 상기 인증서버는 상기 서명검증 메시지로부터 제2 공유세션키를 생성하고, 상기 제2 공유세션키에 대한 서명검증확인(ClientSignOnConfirm) 메시지를 상기 보안모듈로 전송한다(단계(S430)). 이후, 상기 보안모듈은 상기 서명검증확인 메시지로부터 상기 제1 공유세션키와 상기 제2 공유세션키의 동일 여부를 판단하여, 상호인증결과 정보를 생성하고, 상기 상호인증결과 정보를 기반으로 상기 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신하게 된다(단계(S440)). 본 발명의 상호 인증 과정은 도 5에서 보다 상세히 설명하기로 한다.

<39> 도 4b는 본 발명의 일실시예에 의한 보안모듈에서 수행되는 다운로드 가능한 제한수신시스템에서의 상호 인증을 설명하기 위한 흐름도이다.

<40> 도 4b를 참조하면, 우선, 인증서버로부터 인증표시 메시지를 수신하고, 상기 인증표시 메시지로부터 상기 인증서버의 공개키를 획득하여 상기 인증표시 메시지를 검증한다(단계(S451)). 이후, 상기 인증서버로부터 다운로드 메시지를 수신하여, 상기 다운로드 메시지에 대한 서명 검증을 수행하고, 상기 인증서버로 세션키요청 메시지를 전송한다(단계(S452)). 전술한 바와 같이, 상기 인증표시 메시지는 상기 인증서버의 인증서 정보, 또는 상기 CAS 소프트웨어의 버전 정보를 포함하고, 상기 다운로드 메시지는 상기 CAS 소프트웨어의 업데이트를 위한 스케줄 정보, 세션 키 요청 정보, 또는 구매내역기록 요청 정보를 포함한다. 또한, 상기 세션키요청 메시지는 보안모듈의 인증서 정보 및/또는 세션키생성유도 정보를 포함한다.

<41> 이후, 상기 인증서버로부터, 상기 인증기관에서 생성된 제1 랜덤 값, 및 상기 인증기관에서 소정의 키 생성 알

고리즘을 통하여 생성된 시드 값을 포함하는 세션키응답 메시지를 수신한다(단계(S453)).

<42> 이후, 상기 DCAS 호스트의 고유 정보, 상기 시드 값, 보안모듈에서 생성된 제2 랜덤 값, 또는 상기 보안모듈의 하드웨어/소프트웨어에 대한 버전 정보로부터 상기 제1 공유세션키를 생성한다(단계(S454)). 상기 제1 공유세션키의 생성은 구체적으로는 상기 고유 정보, 상기 제2 랜덤 값, 상기 하드웨어/소프트웨어의 버전 정보, 또는 상기 시드 값을 입력 값으로 하는 해쉬 함수를 수행하고, 상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수를 수행하며, 상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 제1 공유세션키로 선택하게 된다.

<43> 이후, 초기 벡터 값 및 상기 제1 공유세션키로 암호화된 상기 서명검증확인 메시지를 대칭키 암호 알고리즘을 통하여 복호화하여 상호인증결과 정보를 생성하며, 상기 상호인증결과 정보를 상기 인증서버로 전송한다(단계(S455)).

<44> 이후, 상기 인증서버로부터 상기 CAS 소프트웨어의 다운로드를 위한 다운로드 정보 메시지를 수신하고, 상기 다운로드 정보로부터 상기 CAS 소프트웨어를 다운로드 서버로부터 다운로드한다(단계(S456)). 상기 다운로드 정보 메시지는 상기 CAS 소프트웨어가 저장된 서버의 IP 어드레스, 소프트웨어 식별정보, 프로토콜 정보, 또는 구매내역기록 요청 정보를 포함함은 전술한 바와 같다.

<45> 이후, 상기 CAS 소프트웨어에 대한 다운로드상태 정보를 포함하는 다운로드확인 메시지 및 구매내역기록 정보를 포함하는 구매내역 메시지를 상기 인증서버로 전송한다(단계(S457)).

<46> 도 4c는 본 발명의 일실시예에 의한 인증서버에서 수행되는 다운로드 가능한 제한수신시스템에서의 상호 인증을 설명하기 위한 흐름도이다.

<47> 도 4c를 참조하면, 우선 인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, 보안모듈로 상기 세션키 생성 정보를 전송하게 되는데, 구체적으로는 상기 인증기관에서 생성된 제1 랜덤 값, 및/또는 상기 인증기관에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값을 포함하는 세션키응답 메시지를 수신하고, 상기 세션키응답 메시지를 상기 보안모듈로 전송한다(단계(S461)). 상기 시드 값은 상기 보안모듈 및 상기 인증기관이 사전에 공유하고 있는 사전공유키를 입력 값으로 하여 상기 키 생성 알고리즘을 통하여 생성된 것임은 전술한 바와 같다.

<48> 이후, 상기 인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, 상기 세션키 생성 정보로부터 생성된 제1 공유세션키에 대한 서명검증 메시지를 수신한다(단계(S462)). 상기 서명검증 메시지는 상기 고유 정보, 상기 보안모듈에서 제2 랜덤 값, 또는 상기 하드웨어/소프트웨어의 버전 정보를 포함한다.

<49> 이후, 상기 서명검증 메시지로부터 제2 공유세션키를 생성하고, 상기 제2 공유세션키에 대한 서명검증확인 메시지를 상기 보안모듈로 전송한다(단계(S463)). 상기 제2 공유세션키는 상기 서명검증 메시지, 시드 값, 및 상기 제1 랜덤 값으로부터 생성되는데, 구체적으로는 상기 고유 정보, 상기 제2 랜덤 값, 상기 하드웨어/소프트웨어의 버전 정보, 또는 상기 시드 값을 입력 값으로 하는 해쉬 함수를 수행하고, 상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수를 수행하며, 상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 제2 공유세션키로 선택함으로써 생성된다.

<50> 도 5는 본 발명의 일실시예에 의한 다운로드 가능한 제한수신시스템에서의 보안모듈 및 인증서버 상호 간을 인증하는 과정을 도시한 흐름도이다.

<51> 도 5를 참조하면, 인증서버(111)는 보안모듈(121)로 인증서버의 인증서(AP_Certificate) 정보, 및/또는 상기 CAS 소프트웨어의 버전 정보를 포함하는 인증표시(SecurityAnnounce) 메시지를 인증서버(111)의 개인키로 서명하여 전송한다(단계(S501)).

<52> 이후, CAS 소프트웨어가 보안모듈(121)에 이미 설치된 경우 인증서버(111)는 상기 CAS 소프트웨어의 업데이트를 위한 스케줄 정보(DownloadSchedule), 세션 키 요청 정보(KeyRequest_REQ), 또는 구매내역기록 요청 정보(PurchaseReport_REQ)를 포함하는 다운로드(DCASDownload) 메시지를 인증서버(111)의 개인키로 서명하여 상기 보안모듈로 전송한다(단계(S502)). 상기 세션 키 요청 정보는 보안모듈(121)이 세션키를 재생성을 수행하기 위한 키 요청을 수행할 것인지에 대한 정보를 포함하고, 상기 구매내역기록 요청 정보는 보안모듈(121)에 저장된 IPPV(Impulse Pay Per View) 구매내역에 대한 기록 수집을 위한 요청 정보를 포함한다.

<53> 이후, 보안모듈(121)은 인증서버(111)로 보안모듈(121)의 인증서(SM_Certificate) 정보 및/또는 세션키생성유도정보(KeyPairingID)를 포함하는 세션키요청(KeyRequest) 메시지를 전송하고(단계(S503)), 상기 세션키생성유도

정보는 세션키 생성을 유도하기 위하여 필요한 정보를 포함한다. 인증서버(111)는 인증서(SM_Certificate) 정보를 먼저 획득하고 보안모듈(121)의 공개키를 획득하여, 서명된 상기 세션키요청 메시지를 검증하고 다시 상기 세션키생성유도 정보(KeyPairingID) 만을 포함하는 상기 세션키요청 메시지를 인증서버(111)의 개인키로 서명하여 인증기관(130)으로 전송한다(단계(S504)).

<54> 이후, 인증서버(111)는 상기 인증기관에서 생성된 제1 랜덤 값(RAND_TA), 및/또는 인증기관(130)에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값(Kc)를 포함하는 세션키응답(KeyResponse) 메시지를 수신하고(단계(S505)), 상기 제1 랜덤 값(RAND_TA)을 포함하는 상기 세션키응답 메시지를 인증서버(111)의 개인키로 서명하여 보안모듈(121)로 전송한다(단계(S506)). 상기 제1 랜덤 값(RAND_TA)은 인증서버(111) 및 보안모듈(121)이 공유하기 위한 세션키 생성을 위한 필요한 임의의 수이고, 상기 시드 값(Kc)은 보안모듈(121) 및 인증기관(130)이 사전에 공유하고 있는 사전공유키(PSK, Pre-shared Key)를 입력 값으로 하여 소정의 키 생성 알고리즘을 통하여 생성된다. 또한, 인증기관(130)으로부터 수신되는 상기 세션키응답 메시지는 인증기관(130)의 개인키로 서명된다.

<55> 이후, 보안모듈(121)은 DCAS 호스트의 고유 정보(SM_ID), 상기 시드 값(Kc), 보안모듈(121)에서 생성된 제2 랜덤 값(NONCE_SM), 또는 보안모듈(121)의 하드웨어/소프트웨어에 대한 버전 정보(HW_SW_Version)로부터 제1 공유세션키를 생성한다(단계(S507)).

<56> 이후, 보안모듈(121)은 상기 고유 정보(SM_ID), 상기 제2 랜덤 값(NONCE_SM), 또는 상기 하드웨어/소프트웨어의 버전 정보(HW_SW_Version)를 포함하는 서명검증 (ClientSignOn) 메시지를 보안모듈(121)의 개인키로 서명하여 인증서버(111)로 전송한다(단계(S508)).

<57> 이후, 인증서버(111)는 상기 서명검증 메시지, 상기 시드 값(Kc) 및 상기 제1 랜덤 값(RAND_TA)으로부터 제2 공유세션키를 생성하고(단계(S509)), 상기 인증서버에서 상기 제2 공유세션키 및 초기 벡터 값(IV, Initial Vector)를 입력으로 하여 소정의 대칭키 암호 알고리즘을 통하여 상기 고유 정보(SM_ID), 클라이언트 정보(SM_Client_Info_Set)를 암호화하여 상기 고유 정보(SM_ID), 상기 클라이언트 정보(SM_Client_Info_Set), 또는 상기 초기 벡터 값을 포함하는 상기 서명검증확인(ClientSignOnConfirm) 메시지를 생성하며 인증서버(111)의 개인키로 서명하여 보안모듈(121)로 전송한다(단계(S510)). 상기 클라이언트 정보는 CAS 소프트웨어 이외에 DRM 소프트웨어 또는 ASD 소프트웨어 등과 같은 DCAS 호스트의 보안모듈(121)로 다운로드될 수 있는 정보를 포함한다.

<58> 상기 제1 공유세션키 또는 상기 제2 공유세션키를 생성하는 과정은 도 6을 참조하여 상세히 설명하기로 한다.

<59> 도 6은 본 발명의 일실시예에 의한 DCAS 호스트의 보안모듈 및 헤드엔드 시스템의 인증서버에서 수행될 수 있고, 상호 인증을 위한 공유세션키를 생성하는 과정을 도시한 흐름도이다.

<60> 도 6을 참조하면, 상기 보안모듈 또는 상기 인증서버는 인증기관을 통하여 공유세션키 생성에 필요한 값인 제1 랜덤 값(RAND_TA) 및/또는 상기 인증기관에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값(Kc)을 수신한다(단계(S610)).

<61> 이후, 상기 고유 정보(SM_ID), 상기 제2 랜덤 값(NONCE_SM), 상기 하드웨어/소프트웨어의 버전 정보(HW_SW_Version), 또는 상기 시드 값(Kc)을 입력 값으로 하는 해쉬 함수(hash function)를 동작시킨다(단계(S620)). 이 경우, 상기 시드 값(Kc)은 상기 인증기관과 상기 인증서버 간의 보안 정책(Security Policy)에 따라 하나 이상이 입력 될 지 결정될 수 있고, 입력되는 수만큼 키 생성을 위한 파라미터로서 사용가능하다.

<62> 이후, 상기 해쉬 함수로부터 출력된 마스터 키 값을 입력 값으로 하는 랜덤 함수(random function)를 수행하고(단계(S630)), 상기 랜덤 함수로부터 출력된 키 값의 임의의 비트를 상기 공유세션키로 선택하게 된다(단계(S640)).

<63> 상술한 과정을 통해 생성된 공유세션키가 상기 보안모듈에서 생성된 경우에는 제1 공유세션키가, 상기 인증서버에서 생성된 경우에는 제2 공유세션키에 해당할 것이다.

<64> 다시 도 5를 참조하면, 계속하여 단계(S511)에서 보안모듈(121)은 초기 벡터 값 및 상기 제1 공유세션키로 암호화된 상기 서명검증확인 메시지를 대칭키 암호 알고리즘을 통하여 복호화하여 상호인증결과 정보(Success/Failure)를 생성하여, 상기 상호인증결과 정보를 보안모듈(121)의 개인키로 서명하여 인증서버(111)로 전송한다. 이후, 인증서버(111)는 상기 상호인증결과 정보를 분석하고, 상기 상호인증결과 정보가 성공(success)인 경우, 상기 CAS 소프트웨어의 다운로드를 위한 다운로드 정보(DownloadInfo) 메시지를 보안모듈

(121)로 전송한다(단계(S512)). 상기 다운로드 정보(DownloadInfo)는 상기 CAS 소프트웨어가 저장된 다운로드 서버의 IP 어드레스(DS_IP), 소프트웨어 파일이름과 같은 소프트웨어 식별정보(FN), 프로토콜 정보(TM), 또는 구매내역기록 요청 정보(PurchaseReport_REQ)를 포함한다.

<65> 상기 다운로드정보 메시지로부터 보안모듈(121)은 상기 다운로드 서버로부터 상기 CAS 소프트웨어를 다운로드 받게 된다. 또한 이 경우 이미 상기 CAS 소프트웨어가 보안모듈(121)에 설치된 경우라면 상기 CAS 소프트웨어를 업데이트하게 될 것이다. 보안모듈(121)은 상기 다운로드 정보로부터 상기 CAS 소프트웨어를 다운로드 서버로부터 다운로드한 이후, 상기 CAS 소프트웨어에 대한 다운로드 결과, 즉 다운로드상태 정보(Download Status)를 포함하는 다운로드확인(DownloadConfirm) 메시지를 인증서버(111)로 전송한다(단계(S513)).

<66> 또한, 상기 보안모듈은 상기 단계(S512)에서 구매내역기록 요청 정보(PurchaseReport_REQ)가 송부된 경우라면, IPPV의 구매내역기록 정보(Purchase Info)를 포함하는 구매내역(PurchasesReport) 메시지를 인증서버(111)로 전송함으로써, 상호 인증 절차를 종료한다(단계(S514)).

<67> 본 발명에 따른 다운로드 가능한 제한수신시스템에서의 상호 인증 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD 와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 계층으로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

<68> 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

도면의 간단한 설명

<69> 도 1은 본 발명의 일실시예에 의한 상호 인증 장치를 포함하는 다운로드 가능한 제한수신시스템을 도시한 것이다.

<70> 도 2는 본 발명의 일실시예에 의한 다운로드 가능한 제한수신시스템에서의 상호 인증 장치의 구성을 도시한 것이다.

<71> 도 3은 본 발명의 일실시예에 의한 DCAS 프로토콜 계층을 포함하는 다운로드 가능한 제한수신시스템에서의 프로토콜을 도시한 것이다.

<72> 도 4a는 본 발명의 일실시예에 의한 다운로드 가능한 제한수신시스템에서의 상호 인증 방법을 도시한 흐름도이다.

<73> 도 4b는 본 발명의 일실시예에 의한 보안모듈에서 수행되는 다운로드 가능한 제한수신시스템에서의 상호 인증을 설명하기 위한 흐름도이다.

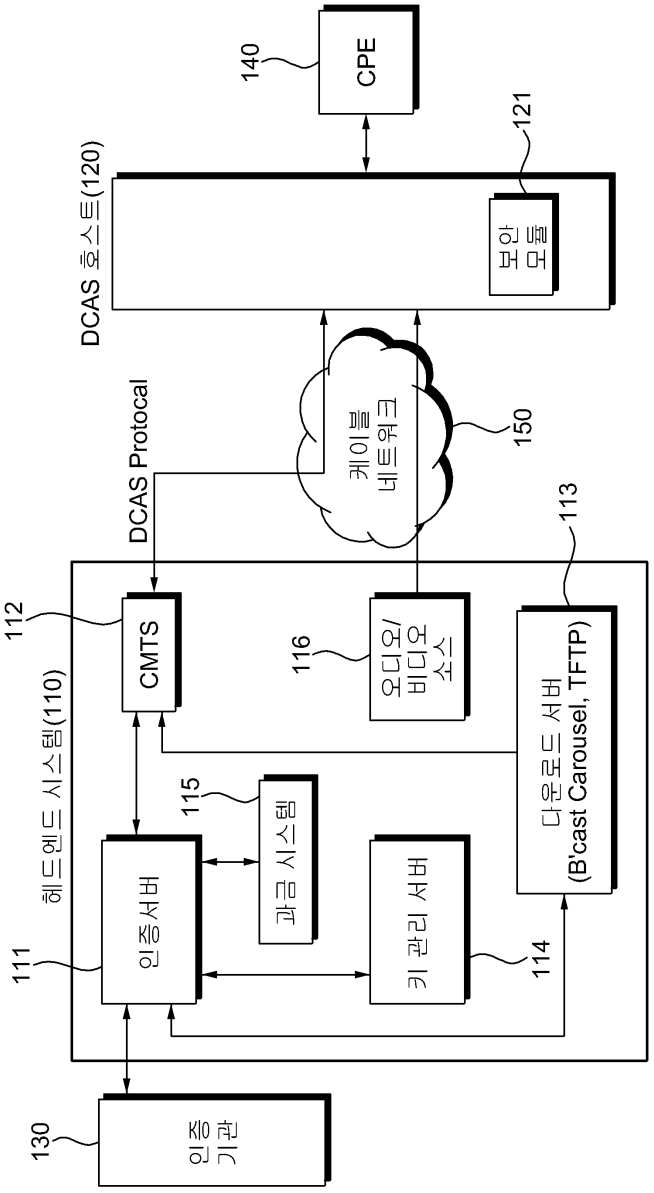
<74> 도 4c는 본 발명의 일실시예에 의한 인증서버에서 수행되는 다운로드 가능한 제한수신시스템에서의 상호 인증을 설명하기 위한 흐름도이다.

<75> 도 5는 본 발명의 일실시예에 의한 다운로드 가능한 제한수신시스템에서의 보안모듈 및 인증서버 상호 간을 인증하는 과정을 도시한 흐름도이다.

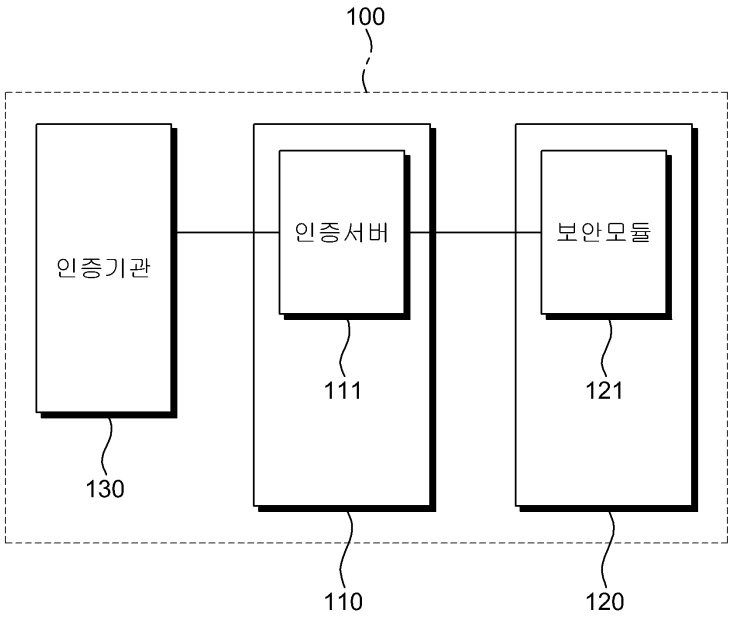
<76> 도 6은 본 발명의 일실시예에 의한 DCAS 호스트의 보안모듈 및 헤드엔드 시스템의 인증서버에서 수행될 수 있고, 상호 인증을 위한 공유세션키를 생성하는 과정을 도시한 흐름도이다.

도면

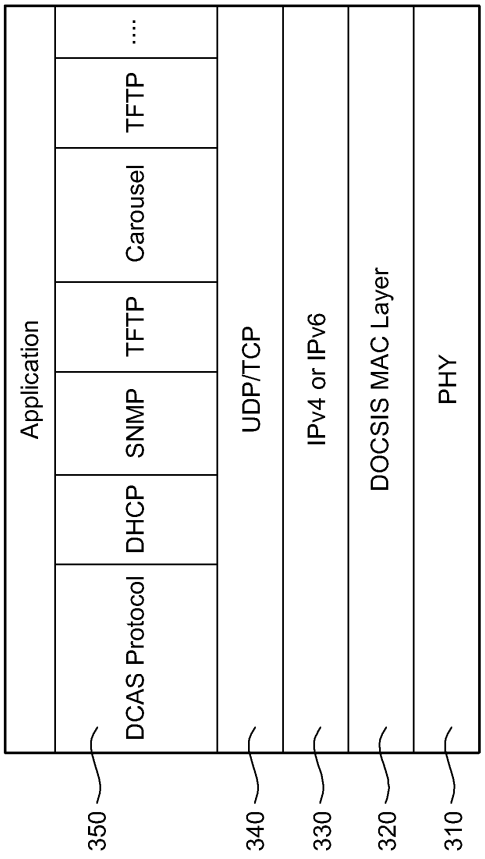
도면1


140
CPE
121
DCAS 호스트(120)
보안 모듈
DCAS Protocal
케이블 네트워크
150
113
112
CMTS
116
오디오/비디오 소스
다운로드 서버 (B'cast Carousel, TFTP)
헤드엔드 시스템(110)
115
과금 시스템
인증서버
111
키 관리 서버
114
130
인증 기관

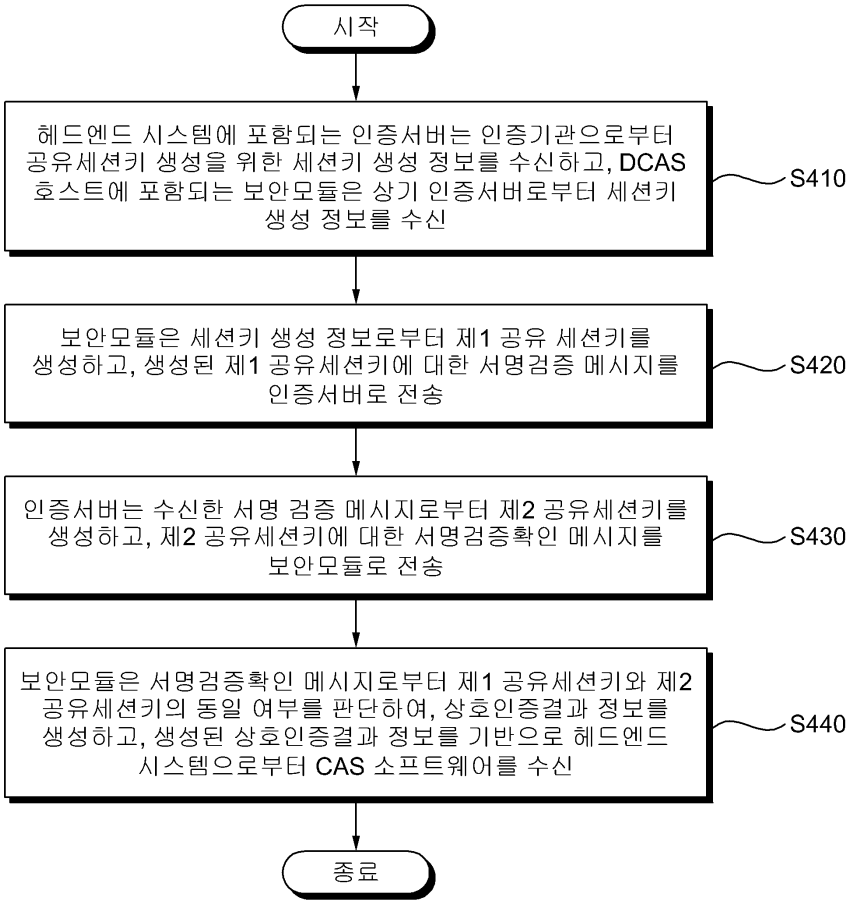
도면2


100
인증기관
인증서버
보안모듈
111
121
130
110
120

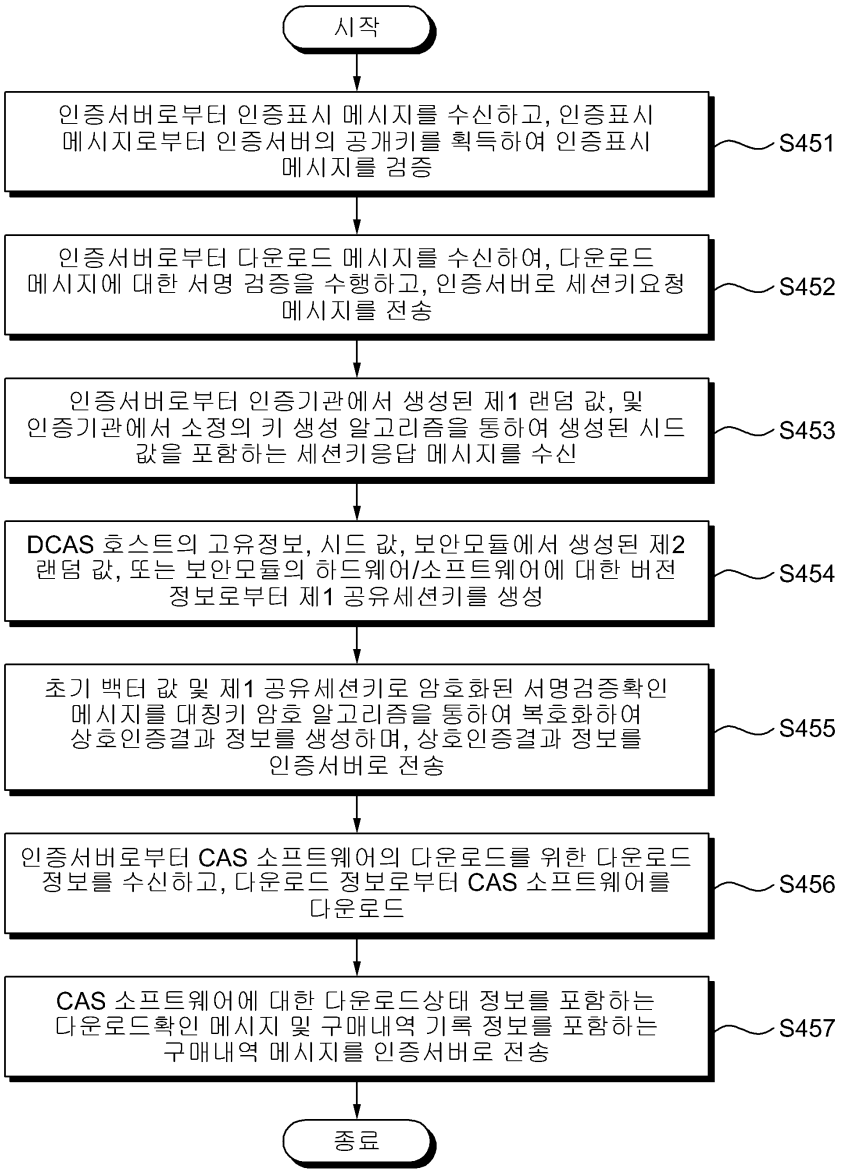
도면3


Application
DCAS Protocol
DHCP
SNMP
TFTP
Carousel
TFTP
....
UDP/TCP
IPv4 or IPv6
DOCSIS MAC Layer
PHY
350
340
330
320
310

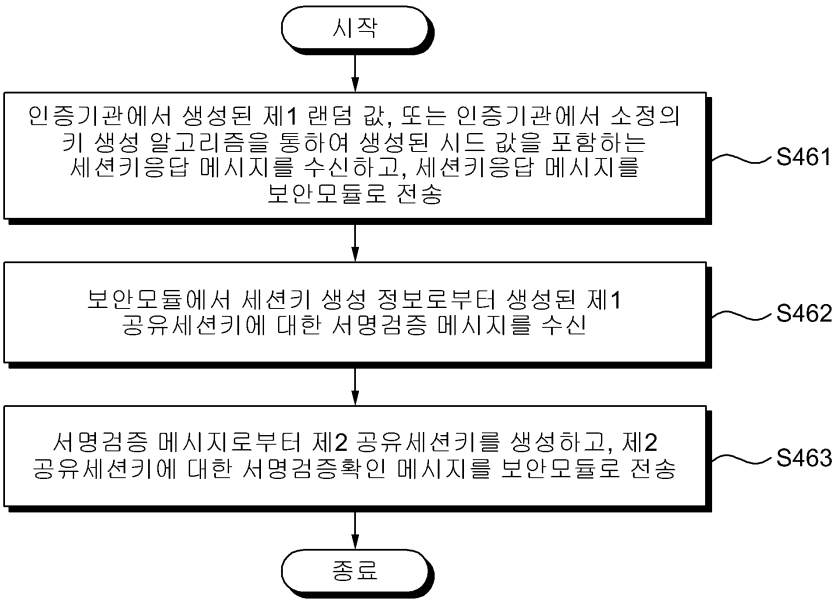
도면4a


시작
헤드엔드 시스템에 포함되는 인증서버는 인증기관으로부터 공유세션키 생성을 위한 세션키 생성 정보를 수신하고, DCAS 호스트에 포함되는 보안모듈은 상기 인증서버로부터 세션키 생성 정보를 수신
S410
보안모듈은 세션키 생성 정보로부터 제1 공유 세션키를 생성하고, 생성된 제1 공유세션키에 대한 서명검증 메시지를 인증서버로 전송
S420
인증서버는 수신한 서명 검증 메시지로부터 제2 공유세션키를 생성하고, 제2 공유세션키에 대한 서명검증확인 메시지를 보안모듈로 전송
S430
보안모듈은 서명검증확인 메시지로부터 제1 공유세션키와 제2 공유세션키의 동일 여부를 판단하여, 상호인증결과 정보를 생성하고, 생성된 상호인증결과 정보를 기반으로 헤드엔드 시스템으로부터 CAS 소프트웨어를 수신
S440
종료

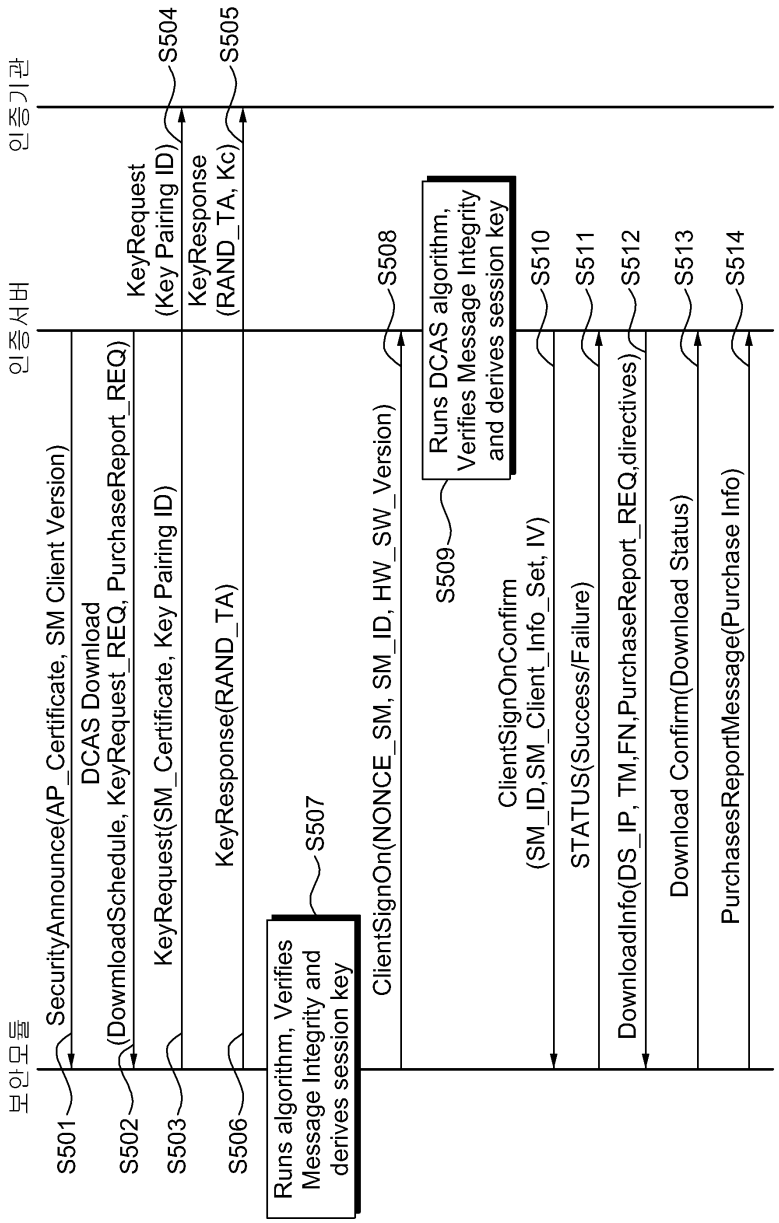
도면4b


시작
인증서버로부터 인증표시 메시지를 수신하고, 인증표시 메시지로부터 인증서버의 공개키를 획득하여 인증표시 메시지를 검증
S451
인증서버로부터 다운로드 메시지를 수신하여, 다운로드 메시지에 대한 서명 검증을 수행하고, 인증서버로 세션키요청 메시지를 전송
S452
인증서버로부터 인증기관에서 생성된 제1 랜덤 값, 및 인증기관에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값을 포함하는 세션키응답 메시지를 수신
S453
DCAS 호스트의 고유정보, 시드 값, 보안모듈에서 생성된 제2 랜덤 값, 또는 보안모듈의 하드웨어/소프트웨어에 대한 버전 정보로부터 제1 공유세션키를 생성
S454
초기 벡터 값 및 제1 공유세션키로 암호화된 서명검증확인 메시지를 대칭키 암호 알고리즘을 통하여 복호화하여 상호인증결과 정보를 생성하며, 상호인증결과 정보를 인증서버로 전송
S455
인증서버로부터 CAS 소프트웨어의 다운로드를 위한 다운로드 정보를 수신하고, 다운로드 정보로부터 CAS 소프트웨어를 다운로드
S456
CAS 소프트웨어에 대한 다운로드상태 정보를 포함하는 다운로드확인 메시지 및 구매내역 기록 정보를 포함하는 구매내역 메시지를 인증서버로 전송
S457
종료

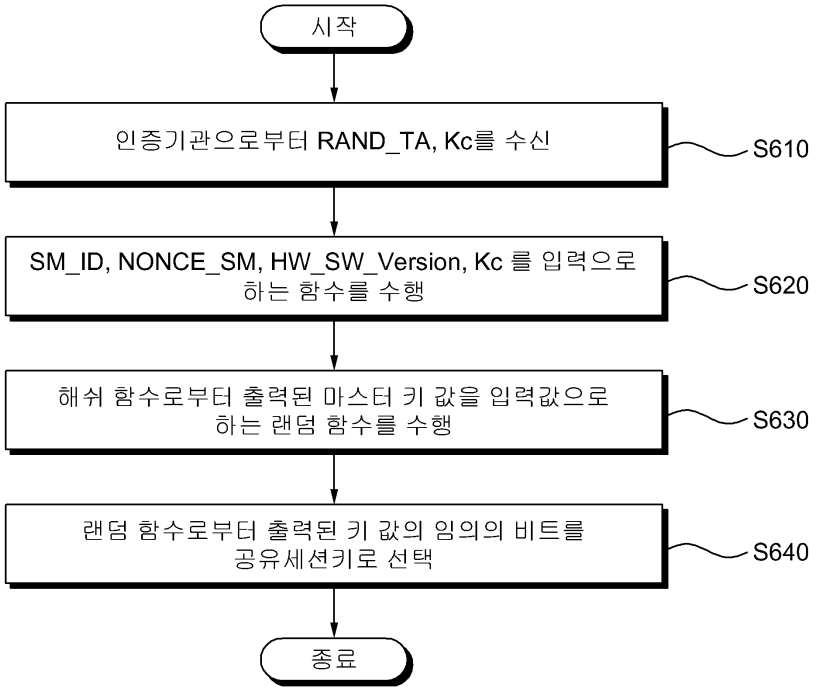
도면4c


시작
인증기관에서 생성된 제1 랜덤 값, 또는 인증기관에서 소정의 키 생성 알고리즘을 통하여 생성된 시드 값을 포함하는 세션키응답 메시지를 수신하고, 세션키응답 메시지를 보안모듈로 전송
S461
보안모듈에서 세션키 생성 정보로부터 생성된 제1 공유세션키에 대한 서명검증 메시지를 수신
S462
서명검증 메시지로부터 제2 공유세션키를 생성하고, 제2 공유세션키에 대한 서명검증확인 메시지를 보안모듈로 전송
S463
종료

도면5


보안모듈
인증서버
인증기관
S501
SecurityAnnounce(AP_Certificate, SM Client Version)
S502
DCAS Download
(DownloadSchedule, KeyRequest_REQ, PurchaseReport_REQ)
S503
KeyRequest(SM_Certificate, Key Pairing ID)
S504
KeyRequest
(Key Pairing ID)
S505
KeyResponse
(RAND_TA, Kc)
S506
KeyResponse(RAND_TA)
S507
Runs algorithm, Verifies
Message Integrity and
derives session key
S508
ClientSignOn(NONCE_SM, SM_ID, HW_SW_Version)
S509
Runs DCAS algorithm,
Verifies Message Integrity
and derives session key
S510
ClientSignOnConfirm
(SM_ID,SM_Client_Info_Set, IV)
S511
STATUS(Success/Failure)
S512
DownloadInfo(DS_IP, TM,FN,PurchaseReport_REQ,directives)
S513
Download Confirm(Download Status)
S514
PurchasesReportMessage(Purchase Info)

도면6


시작
인증기관으로부터 RAND_TA, Kc를 수신
S610
SM_ID, NONCE_SM, HW_SW_Version, Kc 를 입력으로 하는 함수를 수행
S620
해쉬 함수로부터 출력된 마스터 키 값을 입력값으로 하는 랜덤 함수를 수행
S630
랜덤 함수로부터 출력된 키 값의 임의의 비트를 공유세션키로 선택
S640
종료