(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04N 7/16 (2006.01)

(45) 공고일자 2006년09월12일
(11) 등록번호 10-0622964
(24) 등록일자 2006년09월05일

(21) 출원번호 10-2001-7000729
(22) 출원일자 2001년01월17일
번역문 제출일자 2001년01월17일
(86) 국제출원번호 PCT/US1999/016188
국제출원일자 1999년07월15일

(65) 공개번호 10-2001-0053558
(43) 공개일자 2001년06월25일
(87) 국제공개번호 WO 2000/04717
국제공개일자 2000년01월27일

(81) 지정국 국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 가나, 감비아, 세르비아 앤 몬테네그로, 짐바브웨, 인도네시아, 시에라리온, 그라나다, 크로아티아, 인도,

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 가나, 감비아, 짐바브웨, 시에라리온,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀란드, 사이프러스,

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고, 기니 비사우,

(30) 우선권주장 60/093,223 1998년07월17일 미국(US)

(73) 특허권자
톰슨 라이센싱
프랑스 92648 블로뉴 세데 께 알퐁스 르 갈로 46

(72) 발명자
에스키시오글루아멧무르싯
미국인디아나주46250인디아나폴리스레이크쇼어트레일8235아파트먼트125

베이어즈윌리암웨슬리
미국인디아나주46032카멜애로우우드드라이브1075

헤레디아에드윈아르투로
미국인디아나주46250인디아나폴리스레이크쇼어서클#40158356

이젯이젯헤크멧
미국인디아나주46033카멜이스트151번가2249-6

니짐유세프와세프
미국인디아나주46250인디아나폴리스론테르.#2비8680

(74) 대리인 김진회
김태홍
김두규

심사관 : 김영태

(54) 디지털 텔레비전 방송의 이벤트 액세스 관리 방법

요약

본 발명은 다수의 서비스 제공자(방송 텔레비전 네트워크, 케이블 텔레비전 네트워크, 디지털 위성 시스템)로부터 수신한 스크램블된 방송 또는 전송 이벤트에의 액세스를 관리하는 방법에 관한 것이다. 각각의 서비스 제공자는 동일한 공개키를 사용하여 액세스 정보 메시지를 디스크램블하므로, 사용자로 하여금 스마트 카드를 교환하기 않고서 다수의 서비스 제공자로부터의 이벤트에 액세스할 수 있도록 한다. 또한, 본 발명의 방법은 방송 이벤트의 스크램블된 패키지에의 액세스를 관리하는 영역으로까지 확장될 수 있다.

대표도

도 2

명세서

기술분야

본 발명은 단일의 소비자 전자 장치, 예컨대 셋탑 박스 또는 디지털 텔레비전에 의한 조건부 액세스를 다수의 방송 사업자에게 제공하는데 채용될 수 있는 시스템에 관한 것이다. 각 장치는 다양한 방송원으로부터의 방송 또는 전송 스트림을 수신할 수 있다.

배경기술

오늘날의 NTSC 텔레비전은 다양한 서비스 제공자로부터 방송 서비스를 수신한다(도 1 참조). 대부분의 텔레비전 수상기(12)는 스크램블되지 않은 정보 또는 프로그램을 방송 네트워크(22), 위성 네트워크(26) 및 케이블 네트워크(24)로부터 직접 수신할 수 있다. 통상적으로, 스크램블되거나 암호화된 프로그램을 제공하는 케이블 네트워크(24)는 그 프로그램을 디스크램블하거나 암호 해독하기 위한 별개의 독립형 장치(16a)(예컨대, 셋탑 박스)를 필요로 한다. 유사하게, 디지털 위성 시스템도 대개, 별개의 셋탑 박스(16b)를 필요로 하는, 스크램블되거나 암호화된 프로그램을 제공한다. 이들 셋탑 박스들은 필요한 암호 해독 알고리즘 및 키를 포함하는 탈착 가능한 스마트 카드(18a)를 사용할 수 있다. 통상적으로, 각 서비스 제공자마다 별개의 셋탑 박스가 필요하다.

근 미래에, 방송 디지털 텔레비전 서비스는 5 내지 20 개의 지역 채널을 포함할 수 있으며, 각각의 채널은 최대 10 개의 동시 프로그램을 방영할 수 있고, 이들 프로그램 중 일부는 페이퍼뷰(pay-per-view : 지불 방식의 일종, 이하 PPV라 약칭함) 프로그램 일 수 있다. 사용자는 상이한 서비스 제공자들 중 일부 서비스 제공자로부터의 혼합된 서비스를 원할 수도 있다. 예컨대, 사용자는 지역 채널 4에서는 인디아나 대학팀의 농구 경기 전부를 구입하길 원하고, 채널 13에서는 노틀담팀

의 풋볼 경기 전부를 구입하길 원하며, 채널 8에서는 인디아나폴리스 콜트팀의 풋볼 경기 전부를 구입하길 원할 수 있다. 이들 서비스의 각각마다 고유하게 스크램블되어 있는 경우에는, 사용자는 다수의 조건부 액세스 스마트 카드를 구입하고, 사용자가 채널을 돌릴 때 스마트 카드를 바꿔줘야 하는 부담을 안게 된다.

발명의 상세한 설명

본 발명은 부분적으로는 전술한 문제를 인식한 것이며, 부분적으로는 전술한 문제에 대한 해결책을 제공할 것이다. 보안 모듈을 교체하지 않은 채로 복수의 서비스 제공자의 함께 사용될 수 있는 단일의 조건부 액세스 시스템이 제공된다. 이러한 범용의 조건부 액세스 시스템은 하나의 프로그램이 구입될 때 사용자의 계정에서 직불 처리하는 것과, 모든 구입을 기록하는 것과, 요금 정산을 위해서 이 기록을 서비스 제공자에게 전송하는 것을 자동으로 수행하는 개념을 채용하는 것이다. 원하는 융통성을 획득하기 위하여 상기 시스템은 모든 서비스 제공자들에 의해 사용되는 범용의 공개키, 즉 모든 스마트 카드에 통용되는 공개키를 채용한다. 이 스마트 카드에는 대응하는 개인키가 로딩된다. 본 발명의 교시 내에서, 보안이 깨질 충격을 최소화하기 위해서 하나 이상의 공개/개인키의 쌍이 사용될 수 있다는 것은 쉽게 알 수 있을 것이다.

본 명세서에 설명하는 이벤트 또는 프로그램은 다음의 열거하는 항목 중 어느 하나를 포함한다: (1) 영화, 주간 "텔레비전" 쇼, 다큐멘터리 등과 같은 오디오/비디오 데이터; (2) 전자 잡지, 신문, 날씨 뉴스 등과 같은 텍스트 데이터; (3) 컴퓨터 소프트웨어; (4) 이미지 등과 같은 바이너리 데이터; 또는 (5) HTML 데이터(예컨대, 웹페이지) 등. 서비스 제공자로는 이벤트를 방송하는 제공자라면 어떠한 제공자도 포함될 수 있는데, 예컨대, 통상의 방송 텔레비전 네트워크, 케이블 네트워크, 디지털 위성 네트워크, 전자 프로그램 가이드 제공자와 같은 전자 이벤트 목록 제공자, 어떤 경우에는 인터넷 서비스 제공자 등이 있다.

이러한 시스템은 공개키 기술에 근거한 것이다. 하나의 공개키(넘버)는 모든 서비스 제공자가 사용할 수 있다. 이것은 모든 스마트 카드에 대한 공개키이다. 각각의 스마트 카드에는 공개키로 암호화한 메시지를 암호 해독할 수 있는 비밀 개인키가 저장되어 있다. 서비스 제공자는 서비스 제공자의 명칭, 프로그램의 명칭, 시간 및 가격, 프로그램 스크램블화에 사용되는 키를 암호 해독하는 키를 포함하는 CA 자격 메시지를 공개키로 암호화한 전송 스트림으로 전송한다. 스마트 카드는 그 메시지를 암호 해독하고, 각 이벤트마다 적절한 정보가 스마트 카드 내에 저장된다. 스마트 카드는 은행이 부여한 일정액의 구매 신용을 갖는다. 이 신용 한도를 넘지 않는 한은 프로그램은 시청자에 의해서 구입이 가능하다. 미리 계획된 어떤 적절한 시간에, 스마트 카드는 전화로 CA 센터를 호출하게 된다. CA 센터는 또 다른 세트의 공개 및 개인키를 사용하여 은행의 협조 하에 스마트 카드로부터 요금 정보를 수신하고 추가의 신용을 제공한다. 은행은 그 정보 및 신용을 적절한 서비스 제공자에게 전송한다.

일반적으로, 본 발명은 제한된 방송 또는 전송 이벤트에 조건부 액세스를 제공하는 방법을 정의한다. 먼저, 방송 이벤트에 관련이 있는 암호화된 액세스 정보가 수신된다. 다음에, 이 액세스 정보는 암호 해독(또는 디스크램블)되고, 상기 방송 이벤트의 가격이 사전 저장된 캐쉬 준비금보다 적은 지의 여부를 결정하도록 확인된다. 이어서, 스크램블된 방송 이벤트가 서비스 제공자로부터 수신되어 스크램블링을 해독된다.

본 발명의 한 형태에 따르면, 복수의 서비스 제공자들 중 하나의 서비스 제공자로부터의 제한된 방송 또는 전송 이벤트에의 액세스를 관리하는 방법은 상기 전송 이벤트에 관련된 복수의 액세스 정보 메시지를 수신하는 단계를 포함한다. 각각의 액세스 정보 메시지는 상이한 공개키를 사용하여 스크램블되고, 상기 전송 이벤트의 가격에 대응하는 데이터를 포함한다. 이어서, 이 방법은, 서비스 제공자에 관련된 사전 저장 개인키를 사용하여 액세스 정보 메시지들 중 하나의 메시지를 암호 해독 또는 디스크램블하고, 사전 저장된 캐시 준비금 보다 전송된 이벤트의 가격이 적은 지의 여부를 확인하는 단계를 포함한다. 이 방법은, 마지막으로, 하나의 서비스 제공자로부터 스크램블된 전송 이벤트를 수신하여 디스크램블링 키를 사용하여 전송 이벤트를 디스크램블하는 단계를 포함한다.

본 발명의 다른 형태에 따르면, 제한된 전송 이벤트 패키지에의 액세스를 관리하는 방법은 이벤트 패키지에 관련된 디지털 서명의 액세스 정보를 직접 채널을 통해서 수신하고 단계를 포함하고, 이 디지털 서명의 액세스 정보는 이벤트 패키지의 가격에 대응하는 정보를 구비하고 있다. 액세스 정보상의 서명은 공개키를 사용하여 확인된다. 즉, 패키지의 가격의 검사는 사전 저장된 캐쉬 준비금보다 적은지를 보장하기 위해서 행해진다. 이 패키지에 속하는 스크램블된 방송 이벤트들 중의 어느 하나가 서비스 제공자로부터 수신되는 경우, 방송 이벤트의 액세스 정보는 암호 해독되어 디스크램블링 키를 획득하게 된다.

본 발명의 또 다른 형태에 따르면, 제한된 전송 이벤트에의 액세스를 관리하는 방법은 은행으로부터 캐쉬 준비금을 스마트 카드로 전송하는 단계와, 서비스 제공자로부터 암호화된 이벤트 키 및 이벤트의 가격을 수신하는 단계와, 이벤트 키 및 구입 정보를 디지털 비디오 장치에 연결된 스마트 카드로 전송하는 단계를 포함한다. 다음에, 이 이벤트의 가격이 저장된 캐

쉬 준비금 보다 적은 지의 여부를 결정하기 위해서 이벤트 가격이 확인되고 이 가격만큼 공제된다. 암호화된 이벤트 키는 암호 해독되고, 스크램블된 이벤트가 수신되어, 이것이 암호 해독된 이벤트 키를 이용하여 디스크램블되는 스마트 카드로 전송된다. 마지막으로, 디스크램블된 이벤트는 디지털 비디오 장치로 전송된다.

본 발명의 이들 및 다른 특징들은 첨부 도면에 도시된 본 발명의 바람직한 실시예를 참조하여 설명될 것이다.

도면의 간단한 설명

도 1은 소비자의 전자 장치를 다양한 서비스 제공자에 연결하는 종래의 구성을 도시한 블록도.

도 2는 일반적인 디지털 텔레비전을 복수의 지상파 방송 공급자에 인터페이스시키는 일 구조를 도시한 블록도.

도 3은 본 발명에 따라 소정의 장치에의 액세스를 관리하는 시스템을 예시적으로 실시한 블록도.

실시예

본 발명은 이 시스템이 복수의 소스중 하나의 소스로부터 서비스를 받는데 사용될 수 있는 조건부의 액세스 시스템을 제공한다. 디지털 텔레비전(DTV) 또는 셋탑 박스 등의 내부에 구현되는 조건부 액세스 시스템에 의해서, 사용자는 조건부 액세스 모듈 또는 스마트 카드를 교체하지 않은 채로 하나 이상의 서비스 제공자로부터 스크램블된 이벤트를 수신할 수 있다. 별법으로, 스마트 카드의 기능은 DTV에 내장될 수도 있다. 이러한 조건부 액세스 시스템은 서비스들에의 액세스를 위한 톨 브릿지로서 동작함으로써, DTV 제조자가 그의 DTV의 사용에 기초하여 요금을 징수하는 메키니즘을 가능하게 한다. 유사하게, 본 발명은 셋탑 박스 내부에서 구현될 수도 있다. 편의상, 하기의 본 발명에서는 디지털 텔레비전 및 이에 연결된 스마트 카드를 사용하여 수행하는 것에 관하여 설명할 것이다.

도 2에서, 시스템(30)은 디지털 텔레비전(DTV)(40a, 40b)에 대한 액세스를 관리하는 일반적인 구조를 보여준다. 이하, 설명의 편의상, 단일 DTV(40a)에 한정하여 설명할 것이다. 유사한 구성요소 참조 번호는 동일한 기능적 구성요소를 규정한다. 스마트 카드(SC)(42a)는 DTV(40a)의 스마트 카드 판독기(도시되지 않음)에 삽입되거나 결합되고, 버스(45)는 DTV(40a)와 SC(42a)를 상호 연결하여 이들 사이에 데이터 전송이 가능하게 한다. 이러한 스마트 카드로는, 예컨대 국립 재생가능 안전 표준(National Renewable Security Standard; NRSS) 파트 A를 따르는 ISO 7816 카드, 또는 NRSS 파트 B를 따르는 PCMCIA 카드 등에 있다. 본 발명의 개념은 스마트 카트 자체에 한정되지 않고, 조건부 액세스 모듈과 함께 이용될 수 있다. 개념상으로, 이러한 스마트 카드가 스마트 카드 판독기에 결합되는 경우, 이 스마트 카드의 기능은 디지털 텔레비전의 기능의 일부로서 간주될 것이므로, 스마트 카드의 물리적 카드 몸체에 의해 생성된 "경계"가 사라지게 된다.

DTV(40a)는, 예컨대 텔레비전 방송국(SPs)(50, 52), 케이블 텔레비전(도시되지 않음) 및 위성 시스템(도시되지 않음)과 같은 복수의 서비스 제공자(SP)로부터 서비스를 수신할 수 있다. 본 발명은 지상파 방송에 이점이 있다. 인증 기관(CA)(75)은 서비스 제공자 또는 DTV(40a)중 어느 쪽에도 직접적으로 연결되지 않고, 디지털 인증서와 한 쌍의 공개키와 개인키를 발행하는데 이에 대해서는 후술한다. 서비스 제공자가 DTV(40a) 제조업자와 협력하여 인증 기관(75)의 역할을 수행할 수도 있다는 것은 본 발명의 범주 내에 있는 것이다. 요금 정산소(70)는 사용자의 계정을 관리하는데 사용되고, 사용자가 추가의 서비스를 구매할 준비를 했을 때에, 그리고 그 서비스를 소비 또는 이용했을 때에 갱신된 정보를 제공받는다.

DTV 방송 기술용으로 설계된 이러한 조건부 액세스(CA) 시스템은 전송 기반 시스템이다. 이것은 특정 방송 사업자에 대한 CA 정보가 그 자신의 RF 채널상에서만 전송된다는 것을 의미한다. 각각의 방송 사업자는 그 자신의 정보에 대해 책임이 있으므로, 몇몇 방송 사업자들 간에 정보를 조정 및/또는 동기화 하기 위하여 운용 규약을 사전 설정할 필요는 없다. 또한, CA 시스템은 E-cash(전자 화폐) 카드의 충전에 기초한다. 사용자는 (직불 또는 신용 계정으로부터) 일정 금액을 사전에 충전하고, 그 후에 그 카드를 사용하여 이벤트 패키지를 구입하거나 월단위 가입료를 지불하거나 PPV 방식으로 특정 프로그램을 구입한다. 이벤트 패키지로, 예컨대 좋아하는 프로 스포츠 프랜차이즈의 경기 전부 또는 하나 이상의 가상 채널 상의 심야 일요영화 전부 등이 있다.

방송 채널은 서비스 및 이 서비스에의 액세스 정보를 전달하는 데에만 사용된다. 나머지 모든 트랜잭션은 리턴 채널(즉, 모뎀 및 전화 연결)에 의해 수행된다. 어드레스 지정 가능한 메시지의 방송은 필요하지 않다. 방송 서비스는 공통 스크램블링 알고리즘에 의해 보호된다. 이러한 프로세스 및 이벤트 구입 정보에 사용되는 키들은 범용 공개키에 의해 암호화되어 MPEG-2 스트림을 통해 사용자에게 전달된다. 이벤트 패키지의 경우, 패키지 인증서가 CA 서버(60a)로부터 리턴 채널을

통해 사용자에게 전송된다. 하기에 보다 상세하게 설명되는 바와 같이, 인증서는 일반적으로 인증서의 무결성을 보장하기 위하여 서명된다. 즉, 진정한 인증서가 전송측으로 부터 수신되는 것을 보장하기 위한 것이다. 서비스는 갱신 가능한 보안 모듈, 즉 스마트 카드를 통해 액세스 된다.

대칭키 암호화 기법은 알고리즘 및 암호화과 암호 해독 모두에 동일한 키를 이용한다. 공개키 암호화 기술은 2개의 관련된 키, 즉 공개키와 개인키를 사용하는 것을 기초로 한다. 개인키는 비밀키이며, 공개적으로 사용되는 공개키로부터 개인키를 도출하는 것은 계산상으로 불가능하다. 누구든지 공개키로 메시지를 암호화할 수 있지만, 미리 종결된 관련된 개인키를 가진 개인 또는 장치만이 그 메시지를 암호 해독할 수 있다. 유사하게, 메시지는 개인키로 암호화될 수 있으며, 공개키에 액세스할 수 있는 개인은 이 암호화된 메시지를 암호 해독할 수 있다. 개인키를 사용하여 메시지를 암호화하는 것은 "서명하는 것(signing)"으로 볼수있는데, 그 이유는 공개키를 가지고 있다면 누구든지 그 메시지가 개인키를 가진 당사자에 의해 전송된 것임을 검증할 수 있기 때문이다. 이와 같은 착상은 문서상의 서명을 확인하는 것과 유사하다.

디지털적으로 서명된 메시지는 서명이 첨부되어 명문으로(즉, 암호화되지 않고) 전송되는 메시지이다. 첨부된 서명은 메시지 자체 또는 메시지의 개요 중 어느 하나를 암호화함으로써 생성되며, 메시지의 개요는 메시지를 해싱(hashing)함으로써 획득된다. [해싱은 메시지를 암호화하기 전에, 론 리베스트(Ron Rivest)가 개발한 MD5 또는 미국 국립표준 기숙 연구소(NIST)와 미국 국가 안전국(NSA)에서 개발한 SHA-1과 같은 단방향 해싱 알고리즘으로 메시지를 처리하는 것을 포함한다.] 따라서, 서명된 메시지의 수신자는 메시지의 무결성(즉, 소스 또는 출처)을 확인할 수 있다. (비교하여 보면, 공개키 인증서 또는 디지털 인증서는 서명이 첨부되어 명문으로 전송되는 공개키를 포함하는 메시지이다.) 서명 확인은 암호 해독함에 의해 서명을 체크하는 것을 포함한다.

전술한 바와 같이, CA 시스템의 5개의 필수적인 구성 요소는 방송 사업자, CA 벤더, 요금 정산소(예컨대, 은행), 최종 사용자, 및 인증 기관이다. 도 2는 전체 시스템 구조를 도시하며, 이들 5개의 구성 요소와 이것들의 통신 링크 및 데이터 흐름을 보여준다.

최종 사용자는 전화 라인과 같은 점대점 링크를 통해 인증서를 다운로드 받기 위하여 CA 벤더와 통신한다. 전화 라인은 자동 트랜잭션 용으로 그리고 필요한 경우 음성 연결용으로 사용된다. 자동 트랜잭션의 경우, 가능한 프로토콜 중 하나는 점대점 프로토콜(PPP)이다. 보안은 애플리케이션 계층(레이어)에서 사설 프로토콜에 의해 구현된다.

CA 벤더와 방송 사업자 사이의 통신은 근거리 통신망(LAN) 또는 광역 통신망(WAN)을 통해 성립될 수 있다. 전술한 바와 같이, 보안은 기존의 상호 네트워킹 프로토콜을 통해 실행되는 개별적으로 정의된 프로토콜에 의해 애플리케이션 레벨에서 구현된다. 방송 스트림을 보호하는데 필요한 방송 설비는 다수의 CA 벤더로부터 입수 가능한 출하 제품일 수 있다.

방송 사업자는 (1) 서비스 및 (2) 자격 메시지의 전달에 대한 책임이 있다. 자격 메시지는 하기에 보다 상세하게 설명되는 바와 같이 사용자에게 서비스 구입을 허용하는 액세스 정보 메시지(AIM)[또는 별법으로 자격 제어 메시지 및 자격 관리 메시지]를 포함한다. 그러므로, 방송 사업자와 사용자 사이의 통신은 방송 기술 중의 점대다중점 모델을 따라 수행된다. 방송 AIM들은 각 사용자 또는 가입자 마다 고유한 어드레스를 포함하고 있는 것은 아니며, 이것은 위성 또는 케이블 시스템에서는 전형적이다.

DTV(40a)가 CA 서버와 통신하는데 필요한 역방향 채널 접속 기능을 보유하고 있지 않은 경우, 카드에 캐쉬를 충천하기 위해서는 사용자가 역방향 채널을 지원하는 DTV 유닛에 액세스 하거나, 카드를 충전하러 특정 장소(은행, ATM, 벤더의 지역 사무소)에 가야만 한다. CA 오퍼레이터는 카드 소지자 또는 사용자의 은행과 같은 역할을하는 반면에, 요금 정산소는 머천트 뱅크와 같은 역할을 한다. 카드 회사는 CA 오퍼레이터와 방송 사업자의 은행간의 중계자 역할을 하여 거래 결제 서비스를 제공할 수 있다. 스마트 카드 또는 조건부 액세스 모듈에 충전된 고정액의 "캐쉬"는 방송 사업자가 제공하는 서비스에 대한 비용을 지불하는 데에 사용될 수 있다.

어떤 캐쉬 전송 메커니즘이 사용되던 간에, 사용자는 지정 금액이 신용 또는 직불 계정으로부터 CA 카드로 전송되도록 요청한다. 대상물의 아이덴티티와 사용자 자원의 유효성이 적절히 확인된 이후에, 거래(트랜잭션)가 인증되고, 명목상의 금액이 CA 카드에 저장된다.

돈이 카드내로 충전되면, 사용자는 방송 사업자가 제공하는 서비스를 몇개라도 구입할 수 있다. 매 구입시마다 서비스 가격 만큼 카드내의 사용가능한 금액이 줄어든다. 방송 사업자가 제공하는 서비스들은 2개의 카테고리, 즉 PPV 이벤트와 패키지로 분류될 수 있다. 이벤트는 프로그램 가이드에서 할당된 시간대를 갖는 TV 프로그램이며, 패키지는 이벤트들의 단순한 집합이다. 패키지의 예는 다음과 같은 예를 들 수 있다. (1) 소정의 시즌내의 모든 NBA 게임. (2) 하나 이상의 가상 채

널 상의 심야 일요영화. (3) HBO와 같은 특정 가상 채널에의 가입. 모든 이벤트들은 공통 대칭키 알고리즘에 의해 스크램블된 오디오 비디오 스트림 중 하나 이상을 갖는다. 구입 정보 및 디스크램블링 키를 포함하는 자격 패키지는 공통 공개키 알고리즘에 의해 암호화되어야 한다.

이벤트를 구입하는 경우, 기록이 스마트 카드에 저장된 후, 이 기록이 CA 벤더로 전송될 수 있다. 저장된 구입 정보가 CA 데이터베이스로 전송되면, CA 벤더는 제공된 서비스에 대한 비용을 방송 사업자에게 지불할 수 있다. 또한, 스마트 카드는 후술하는 정보를 저장하기 위하여 불휘발성 메모리를 갖는다.

32 비트 필드는 카드의 일련 번호를 나타낸다. 128 비트의 BCD 필드는 사용자 (신용 또는 직불) 카드 번호를 나타낸다. 10 바이트 필드는 CA 서버의 전화 번호를 나타내고, 10 바이트 필드는 다른 CA 서버의 전화 번호를 나타낸다. 40 비트 BCD 필드는 사용자가 사용할 수 있는 돈의 양을 저장한다. 소정의 필드는 최종의 E-cash 인증서 상의 서명을 나타낸다. 8 비트 필드는 사용자에게 사용가능한 E-cash가 기설정된 임계값보다 작음을 알리거나, 돈을 추가하기 위해서 CA 서버에 대한 자동 콜백(automaioc call back)을 개시하는 임계값을 저장하기 위한 것이다. 40 비트의 BCD 필드는 E-cash가 임계값보다 적은 경우 사용자의 개입 없이 카드에 충전되는 돈의 양을 나타낸다. 이 돈의 양은 사용자에 의해 결정되며, 카드가 활성화되어 있는 동안 CA 서버로 전송된다. 이 값이 제로인 경우, 자동 E-cash 충전은 허용되지 않을 것이다. 2개의 768 비트 필드는 AIM들을 암호 해독하기 위하여 개인키를 저장하고, 인증서 상에 서명을 확인하기 위한 공개키를 저장할 용도로 사용된다. 21 바이트의 필드는 방송 서비스를 디스크램블하기 위한 DES 키를 저장할 용도로 사용된다. 2개의 96 바이트 필드는 현재의 개인키를 대체하기 위한 키를 저장하고, 현재의 확인키를 대체하기 위한 키를 저장하기 위한 것이다. CA 서버와의 보안 통신을 위한 대칭 DES 키를 저장할 용도의 8 바이트의 필드가 제공된다. 스크램블링 알고리즘이 DES와는 다른 암호(cipher)일 수도 있다는 것은 본 발명의 범주에 포함된다.

카드는 사용자가 구입한 PPV 이벤트에 대한 정보 및 패키지들의 정보를 저장해야 한다. 카드 메모리가 가득 찬 경우, 사용자는 추가적인 이벤트 구입이 허용되지 않을 것이다.

카드와 호스트 사이의 데이터 상호 교환은 잘 규정된 공통 인터페이스, 즉 국립 재생가능 안전 표준(NRSS)의 EIA-679 파트 A 또는 파트 B에 기초한다. 전화선은 폭넓게 사용 가능한 물리적인 링크이므로 CA 서버와 호스트 사이에서 선택된 프로토콜은 보안이 점대점 프로토콜(PPP) 데이터그램 내에 제공되는 표준 51로서 채용된 점대점 프로토콜(PPP)의 RFC 1548이다. 본 명세서에 기술된 기술적인 혁신은 리턴 채널 상에서 PPP와 상이한 다른 프로토콜을 사용하는 것을 배제하지 않는다.

PPP는 ISO의 HDLC 표준에 따르는 프로토콜로서, ITU-T가 X.25 시스템용으로 채용되고 있다. 다수의 프로토콜로부터 점대점 링크를 통해 데이터그램을 전송하는 방법이 IETF에 의해 개발되었다. 이 프레임 포맷은 16비트의 프로토콜 필드(RFC 1700, 즉 "할당된 번호"에서 규정됨)이며, 이어서 가변 길이의 정보 필드가 오고, 뒤이어 수신 프로토콜이 필요로 하는 경우 프레임 길이를 조정하기 위해 추가되는 선택적인 바이트를 포함하는 패딩 필드가 온다.

카드와 CA 서버간의 데이터를 교환하기 위하여 0x00FF 값의 프로토콜 필드를 갖는 새로운 프로토콜이 규정된다. 이 새로운 프로토콜의 경우에는 패딩 필드의 값은 항상 제로이다. 이 새로운 프로토콜은 긍정 응답(ACK) 메시지와 부정 응답(NACK) 메시지를 이용한 신뢰성 있는 전송을 제공하는데 이들 메시지는 정보 필드의 제1 바이트 내에 삽입되며 8비트 uimsbf포맷을 사용한다.

ACK 다음으로는 회답으로서 전송되는 정보(피기백 긍정 응답)가 올 수 있다. 수신 종단이 손상된 메시지를 검출하는 경우, NACK를 응답하고, 전송측에 재전송을 요구하게 된다.

전술한 프로토콜을 사용하여 스마트 카드는 다음 조건 중 어느 하나의 조건 하에서 CA 서버에 대한 콜백을 개시한다.

1. 카드가 처음으로 DTV 내에 삽입된 경우

2. 사용자가 디스플레이된 메뉴를 사용하여 진보된 패키지 구입의 요구를 입력한 경우

3. 스마트 카드 메모리가 가득 찬 경우

4. 지역 시간이 기간 [1am-6am] 내에 있고, 전송된 새로운 기록이 있는 경우

5. 카드가 새로운 개인키 또는 확인키에 대한 통지를 수신한 경우

6. 스마트 카드의 금액이 특정 임계값 보다 작고, 자동 E-cash 충전이 가능한 경우

7. 사용자가 디스플레이된 메뉴를 사용하여 금액을 요청한 경우

8. 사용자가 패키지 구입의 취소를 요청한 경우
이 조건에 따라 카드는 초기 경고 메시지를 전송하여 사용자와 콜의 목적에 대하여 CA 서버에 알린다.

사용자가 카드를 처음으로 DTV에 삽입하면, 그 카드에 특유한 정보가 CA 서버로 전송되어 등록된다. 이 정보는 Kcallback에 의해 암호화된다.

카드 -> CA 서버 : 경고 메시지(alert_type = 0x01)

카드 <- CA 서버 : ACK 메시지

카드 -> CA 서버 : 카드 정보 메시지

카드 <- CA 서버 : ACK 메시지

진보된 구입은 디스플레이된 메뉴를 활용하여 성취될 수 있다. 사용자 요청에 응답하여 CA 서버는 카드 내에 저장될 패키지 인증서를 전송한다.

카드 -> CA 서버 : 경고 메시지(alert_type = 0x02)

카드 <- CA 서버 : ACK 메시지 | 서명된 패키지 인증서 메시지

카드 -> CA 서버 : ACK 메시지

패키지 인증서 포맷은 다음의 필드들을 포함한다. 8 비트 필드는 패키지 인증서 메시지를 나타낸다. 2개의 값이 가능한데, 하나는 갱신 가능한 패키지 가입이며, 다른 하나는 갱신 불가능한 패키지 가입이다. 32 비트 필드는 provider_index 필드에 값을 할당하는 등록 기관을 나타낸다. 16 비트 필드는 콘텐츠 제공자를 식별한다. 이 유일한 번호는 format_identifier에 의해 식별되는 등록 기관에 등록된다. 16 비트 필드는 이벤트를 반송하는 전송 스트림을 식별한다. 16 비트 필드는 패키지 식별자를 나타낸다. 8 비트 필드는 타이틀 필드로 사용된다. 가변 길이 필드는 Latin-1 확장자와 함께 ASCII를 사용하는 패키지의 타이틀용으로 사용된다. 40 비트의 필드는 BCD의 포맷으로 패키지의 가격을 나타낸다. 24 비트 필드는 패키지의 유효 기간을 나타낸다.

PPV 이벤트 구입 기록들은 이벤트 방송 이후까지 카드 내에 일시적으로 저장된다. 이 기록들은 사용자의 개입 없이 하기의 경우 중 어느 하나의 경우에 CA 서버로 전송된다.

(i) 카드 메모리가 더 이상의 기록을 저장할 수 없는 경우

(ii) 지역 시간이 기간 [1am-6am] 내에 있고, 전송될 새로운 기록이 있는 경우
모든 기록들은 Kcallback에 의해 암호화된다.

삭제

(i) 스마트 카드 메모리가 가득 찬 경우

카드 -> CA 서버 : 경고 메시지(alert_type = 0x03)

카드 <- CA 서버 : ACK 메시지

카드 -> CA 서버 : 가변수의 암호화된 PPV 이벤트 구입 기록

카드 <- CA 서버 : ACK 메시지

(ii) 지역 시간이 기간 [1am-6am] 내에 있고, 전송될 새로운 기록이 있는 경우

카드 -> CA 서버 : 경고 메시지(alert_type = 0x04)

카드 <- CA 서버 : ACK 메시지

카드 -> CA 서버 : 가변수의 암호화된 PPV 이벤트 구입 기록

카드 <- CA 서버 : ACK 메시지

개인키 또는 확인키가 대체될 필요가 있는 경우, 통지가 방송 채널을 통해 카드로 전송된다. 이어서, 각 사용자는 새로운 키를 수신하기 위하여 콜백을 개시할 필요가 있다.

카드 -> CA 서버 : 경고 메시지(alert_type = 0x05)

카드 <- CA 서버 : ACK 메시지 | 키 대체 메시지

카드 -> CA 서버 : ACK 메시지

다음의 경우에, 금액이 카드에 추가된다.

1. 스마트 카드의 돈이 특정 임계치보다 적은 경우, 또는

2. 사용자가 디스플레이된 메뉴를 사용하여 금액을 요구하는 경우, 또는

3. 지역 전화 연결이 되어 있지 않은 경우에 카드가 원거리 위치에 있는 경우

모든 경우에 있어서, 돈을 제공하는 실체는 신용 카드 또는 직불 카드 정보를 확인하여 E-cash 인증서(ECC)를 생성시키고 이 생성된 ECC를 카드에 전송한다. ECC 메시지 포맷은 8 비트 필드가 메시지 타입을 나타내고 40 비트 필드가 스마트 카드에 추가될 금액의 BCD 값을 유지하기 위한 것이다.

1) 자동 E-cash 충전은 다음에 의해서 가능해진다.

카드 -> CA 서버 : 경고 메시지(alert_type = 0x06)

카드 <- CA 서버 : ACK 메시지

카드 -> CA 서버 : E-cash 에 대한 서명

카드 <- CA 서버 : ACK | 서명된 E-cash 인증서 메시지

카드 -> CA 서버 : ACK 메시지

2) E-cash 인증서가 미리 규정되고 고정된 금액의 E-cash를 포함한다. 자동 E-cash 충전은 불가능하다. 사용자는 다음과 같이 진행한다.

카드 -> CA 서버 : 경고 메시지(alert_type = 0x07)

카드 <- CA 서버 : ACK 메시지

카드 -> CA 서버 : E-cash에 대한 서명 | E-cash 금액 메시지

카드 <- CA 서버 : ACK 메시지 | 서명된 E-cash 인증서 메시지

카드 -> CA 서버 : ACK 메시지

사용자는 스크린 상에 디스플레이된 메뉴를 사용하여 구입을 취소할 수 있다. 카드에 의해서 취해지는 액션은 구입의 형태에 따라 달라진다.

(i) 패키지 구입 : CA 서버에 콜개시.

카드 -> CA 서버 : 경고 메시지(alert_type = 0x08)

카드 <- CA 서버 : ACK 메시지

카드 -> CA 서버 : 취소된 패키지 구입 기록

카드 <- CA 서버 : ACK 메시지 | 서명된 E-cash 인증서 메시지

카드 -> CA 서버 : ACK 메시지

(ii) PPV 이벤트 구입 : 이벤트 취소 데드라인에 도달하지 않은 경우, 선택된 기록은 모두 삭제된다.

AIM들은 비디오 데이터를 반송하는 전송 스트림 패킷의 적응 필드로 개인 데이터로서 반송된다. 이들 AIM은 또한 MPEG-2로 ECM 전송이 가능한 도구 및 기능을 사용하여 PID가 상이한 전송 스트림으로 반송될 수도 있다. 이 adaptation_field_control 비트는 '10' 비트(적응 필드만, 페이로드 없음) 또는 '11' 비트(적응 필드가 있고, 뒤이어 페이로드가 있음)일 것이다. 동일한 AIM_id를 갖는 AIM 메시지의 최대 사이클 시간은 500ms가 될 것이다.

액세스 정보 메시지의 비트 스트림 신택스는 다음과 같은 필드를 포함한다. 이 액세스 정보 메시지의 고유한 8비트 식별자. AIM_id 필드는 적응 필드의 개인 데이터 부분의 제2 바이트이다. 제1 바이트는 AIM을 보호하는 데에 사용되는 공개키를 식별할 용도로 할당된다(다수의 공개키들이 소정의 DMA에 사용되는 경우). AIM_length 필드가 다음에 바로 AIM의 바이트 수를 규정하는 8비트 필드가 온다. 32 비트 필드는 값들을 provider_index 필드에 할당하는 등록 기관을 식별하기 위한 것이다. 16 비트 필드는 콘텐츠 제공자를 식별하기 위한 것이다. 이 고유 번호는 format_identifier에 의해 식별되는 등록 기관에 등록된다. 24 비트 필드는 특정 TV 프로그램 또는 이벤트를 식별하기 위한 것이다. provider_index에 의해 식별되는 콘텐츠 제공자에 의해 할당되면, 콘텐츠 제공자 데이터베이스에 등록된 이들 프로그램들을 모두 고유하게 식별한다. 16 비트 필드는 이벤트를 전송하는 전송 스트림을 식별하기 위한 것이다. 16 비트 필드는 이벤트를 전송하는 특정 서비스를 고유하게 식별하기 위한 것이다. 14 비트 필드는 이 전송 스트림의 소정 서비스 내에서 특정 이벤트를 고유하게 식별하기 위한 것이다. program_event_id가 콘텐츠 제공자의 이벤트를 식별해내는 값인 반면에, event_id는 이벤트의 프로그램 가이드 인덱스이다. 콘텐츠 제공자로서의 역할도 함께하는 방송 사업자는 양자 번호가 동일하기를 원할 수 있지만, 이것은 경우에 따라서는 유효하지 않을 수도 있다. 32 비트 필드는 이벤트 시작 시간을 나타낸다. 20 비트 필드는 초 단위로 측정된 이벤트의 길이를 나타낸다. 10 바이트 필드는 이 메시지를 기술하는 이벤트에 대한 영문 타이틀의 처음 10개의 문자를 저장하기 위한 것이다. 실제 타이틀이 10개 미만의 문자를 갖는 경우에는, 이 타이틀 세그먼트는 이 필드에 다른 것을 포함하기 전에 ESC 문자로 채워야한다. 5 바이트 BCD 필드는 이벤트의 가격을 나타낸다. 16 비트 필드는 이 이벤트가 속하는 패키지를 나타낸다. 최상위 비트는 1번째 패키지에 대응하는 반면에, 최하위 비트는 16번째 패키지에 대응한다. 이벤트가 k번째 패키지에 속하는 경우, 이 필드의 k번째 비트는 1로 설정될 것이다. 다수의 패키지에 속하는 소정의 이벤트를 나타내기 위해서 하나 이상의 비트가 1로 설정될 수 있다. 64 비트 필드는 고려중인 이벤트의 비디오 신호 및 오디오 신호를 디스크램블하는데 필요한 DES키용으로 사용된다(TDES키용으로는 168 비트의 필드). 40 비트 필드는 사용자가 CA 서버를 호출함에 의해 새로운 개인키 또는 확인키를 획득할 필요가 있음을 나타낸다. 플래그가 1로 설정되어 있는 경우, 이 키는 지정된 데드라인까지 대체될 필요가 있다. 8비트 필드는 이어지는 AIM 디스크립터 리스트의 총길이(바이트 단위)를 식별할 용도로 사용된다.

본 발명의 일 실시예에서, 자격 제어 메시지(ECM)가 AIM 대신에 사용될 수 있다. ECM의 포맷은 MPEG-2 및 ATSC 규격에 따라 개별적으로 정의된다. 특정 포맷은 8 비트 테이블 식별 필드, 인디케이터 3비트, 12 비트 섹션 길이 필드, 8 비트

프로토콜 버전 필드, 5 비트 버전 번호 필드, 2개의 섹션 번호 필드, 공개키 필드, 전송 스트림 식별 필드, 주 및 부 채널 번호 필드, 2개의 이벤트 식별 필드, 스트림 PID 및 디스크립터 길이 필드, 암호 체크 필드, 기타(스터핑) 바이트 필드 및 32 비트 CRC 필드를 포함할 수 있다.

시스템의 보안은 광범위하게 수용되는 표준 공개키 및 대칭키 알고리즘에 기초한다. 선택된 알고리즘은 공개키 암호를 위한 RSA와, 대칭키 전체 스크램블링을 위한 TDES 및/또는 DES이다. 전체 시스템에는 범용 RSA 공개/개인키의 쌍(Kpub/Kpri)이 존재한다. 공개키는 모든 방송 사업자에 의해 공유되며, 대응하는 개인키는 CA 제공자에 의해 소비자에게 분배되는 부정 행위 방지 NRSS-A 기반의 스마트 카드에 위치하게 된다. 이 공개키는 헤드 엔드에서 발생된 AIM을 보호하는데 사용된다.

공개키 하에서 암호화된 AIM들은 ECB 모드에서 오디오/비디오 콘텐츠를 스크램블하는데 사용되는 대칭 DES 키(KDES)인 제어 워드(CW)들을 반송한다. AIM을 그의 개인키로 암호 해독한 이후에, 스마트 카드는 DES 키를 획득하여 오디오/비디오 스트림을 디스크램블한다. 헤드 엔드에서, 스크램블링은 E_{KDES}(A/V 스트림)이고, 암호화는 E_{Kpub}(AIM)이다. 스마트 카드상에서, 암호 해독은 $D_{Kpri}(E_{Kpub}(AIM))$이고, 디스크램블링은 $D_{KDES}[E_{KDES}(A/V 스트림)]$이다.

시스템의 보안은 여러 가지 방법으로 개선될 수 있다. 하나의 적당한 방법에는 AIM을 암호화할 용도로 헤드 엔드에서 다수의 공개키를 사용하는 것이 있다. 이와 같이 다수의 공개키를 이용하면 시장이 중복되는 지역에서 장점을 찾을 수 있다. 예컨대 사용자는 더욱 중요한 시장으로부터 지상파 디지털 방송을 수신할 수 있다. 다른 예로는 소정의 DMA 내의 수신기 분포가 명백한 서브세트들로 나뉘고, 각 서브세트에는 상이한 개인키가 할당되며, 하나의 개인키에 대한 공격이 시스템을 악화시키지 않는 경우를 들 수 있다.

예컨대, 헤드 엔드에서의 암호화는 4개의 키, 즉 $E_{Kpub\ 1}$(AIM), $E_{Kpub\ 2}$(AIM), E_{Kpub3}(AIM) 및 $E_{Kpub\ 4}$(AIM)를 포함할 수 있다. 이어서, 스마트 카드 상에서의 암호 해독은 다음 4개의 키들 중 어느 하나에 기초하게 될 것이다. 여기서, 카드 형태 1은 $D_{Kpri\ 1}[E_{Kpub\ 1}(AIM)]$이고, 카드 형태 2는 $D_{Kpri\ 2}[E_{Kpub\ 2}(AIM)]$이며, 카드 형태 3은 $D_{Kpri3}[E_{Kpub3}(AIM)]$이고, 카드 형태 4는 $D_{Kpri\ 4}[E_{Kpub\ 4}(AIM)]$이다. AIM을 암호화하는데 사용되는 공개키는 적응 필드의 최초 바이트에 있는 식별자를 사용하여 식별된다. 이 필드는 AIM을 암호화시키는데 사용되는 공개키를 나타낸다. 이 값을 i라고 하면 활성 공개키는 Kpubi가 된다.

E-cash 인증서는 카드에 추가될 금액을 포함한다. 패키지 인증서는 고객에게 제공되는 패키지의 가격을 포함한다. 상기 2개의 인증서가 모든 민감한 데이터를 포함하기 때문에, 이들 메시지의 무결성을 보장하기 위한 서명 메커니즘을 필요로 한다. 따라서, 모든 인증서는 피드백 경로를 갖는 채널, 예컨대 모뎀을 이용한 백채널을 통해 전송된다.

패키지 인증서가 CA 서버로부터 정상적으로 전송되더라도, 카드에 E-cash를 충전하기 위한 상이한 소스(예컨대, ATM 또는 다른 특정 단말)가 있을 수 있다. 각각의 소스가 고유의 개인키로 서명되는 경우에는, DTV는 다수의 공개키를 유지할 필요가 있다. 본 발명의 CA 시스템은 하나만의 공개키를 이용하여 서명을 검증하는 ID 기반의 인증 방식을 채용한다.

전술한 바와 같이, 방송 사업자, CA 서버 및 스마트 카드는 스크램블링, 암호화 및 서명 프로토콜에 참여하기 위해서는 소정의 키를 저장할 필요가 있다. 그러한 모든 타입의 키를 저장하고 사용하는 것이 도 3에 요약되어 있다.

Kpub는 방송 사업자 사이트에 유지되고, A/V 스트림을 스크램블하도록 지역적으로 생성되는 DES키를 암호화하는데 사용된다. 스마트 카드는 DES키 복구용의 대응하는 Kpri를 갖는다.

Ksig는 패키지 및 E-cash 인증서를 서명하는데 사용된다. 서명된 인증서는 카드에 저장된 Kver에 의하여 확인된다. 섹션 8.2에서 설명한 ID 기반 방식에서, Ksig는 각 인증서 제공자(CA 벤더, ATM 등)에 대하여 고유한 것이지만, Kver은 모든 인증서 제공자에 대하여 공통인 것이다.

Kcallback은 카드와 CA 서버 사이에서 공유되며, 교환되는 민감한 감지 정보를 암호화하는데 사용된다. 카드로부터 CA 서버로 전송되는 정보는 지불 카드 번호, 고정된 E-cash 및 이벤트 구입 기록이다. 필요한 경우, Kpri 및 Kver은 CA 서버로 대체될 수 있다. Kcallback은 각 카드마다 고유할 수 있다. 따라서, 새로운 카드를 사용자에게 전송하는 것만이 이의 대체를 가능하게 할 수 있다.

본 발명은 몇 가지 실시예에 대해서 상세하게 설명되었지만, 전술한 상세한 설명을 읽고 이해하면 당업자에게, 전술한 실시예에 대한 다수의 변형예가 생길 것은 명백하고, 이러한 변형 예는 첨부된 특허청구범위의 범주에 포함한다는 것을 의도하는 바이다. 예컨대, 본 발명은 디지털 지상파 방송 및 전송 위성 디지털 신호 모두에 성공적으로 활용될 수 있다.

(57) 청구의 범위

청구항 1.

제한된 전송 이벤트에의 액세스를 관리하는 방법에 있어서,

복수 개의 서비스 제공자 중 하나의 서비스 제공자로부터 상기 전송 이벤트에 관련된 암호화된 액세스 정보 - 이 암호화된 액세스 정보는 상기 복수 개의 서비스 제공자간에 공유되는 공유 공개 키를 이용하여 암호화되고 상기 전송 이벤트의 가격에 대응하는 데이터를 포함함 - 를 수신하는 단계와;

상기 공유 공개 키와 관련된 개인 키를 이용하여 상기 액세스 정보를 조건부 액세스 모듈에서 암호 해독하는 단계와;

상기 조건부 액세스 모듈에서 상기 전송 이벤트의 가격이 사전 저장된 캐쉬 준비금보다 적은 지를 확인하는 단계와;

스크램블되어 있는 상기 전송 이벤트를 서비스 제공자로부터 수신하는 단계와;

상기 확인에 응답하여 상기 조건부 액세스 모듈에서 상기 전송 이벤트를 디스크램블하는 단계를 포함하는 것을 특징으로 하는 것인 이벤트 액세스 관리 방법.

청구항 2.

제1항에 있어서, 상기 액세스 정보는 이벤트 디스크램블링 키 및 구입 정보를 더 구비하고, 상기 구입 정보는 채널 식별 데이터, 이벤트 아이덴티티 데이터, 날짜 및 시간 스탬프 데이터, 요금청구 데이터를 포함하는 것인 이벤트 액세스 관리 방법.

청구항 3.

제2항에 있어서, 상기 이벤트 액세스 관리 방법은, 사용자의 계정 정보를 갱신하기 위해서 상기 구입된 전송 이벤트에 관련된 데이터를 상기 서비스 제공자에 전송하는 단계를 더 포함하는 이벤트 액세스 관리 방법.

청구항 4.

제3항에 있어서, 상기 조건부 액세스 모듈은 스마트 카드를 포함하는 것인 이벤트 액세스 관리 방법.

청구항 5.

삭제

청구항 6.

제4항에 있어서, 상기 스마트 카드는 카드 몸체를 구비하고, 이 카드 몸체의 표면에는 ISO 7816 규격과 PCMCIA 카드 규격에 따라 복수의 단말이 배치되는 것인 이벤트 액세스 관리 방법.

청구항 7.
삭제

청구항 8.
삭제

청구항 9.
삭제

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

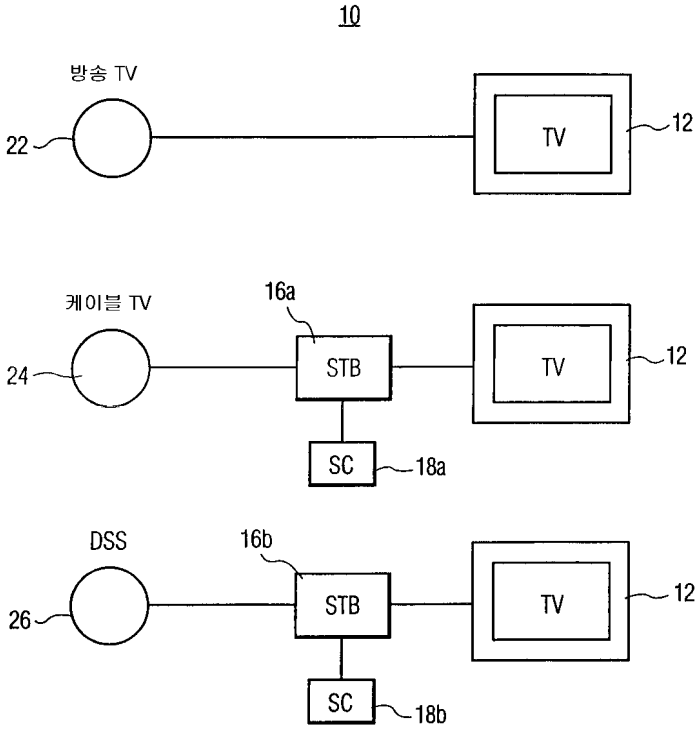
청구항 15.
삭제

청구항 16.
삭제

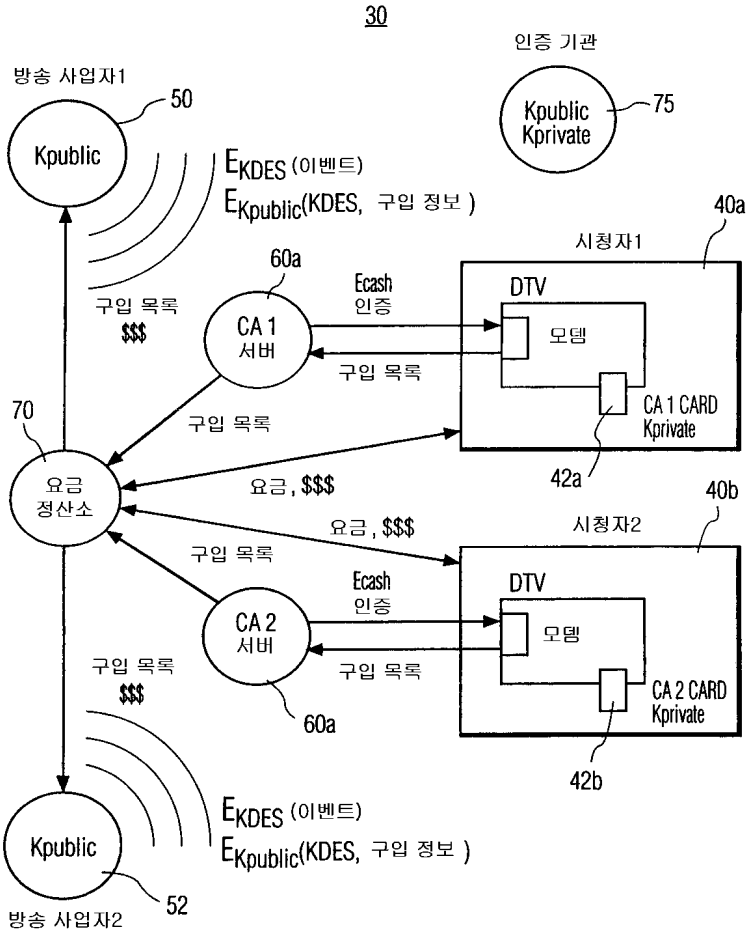
도면

도면1

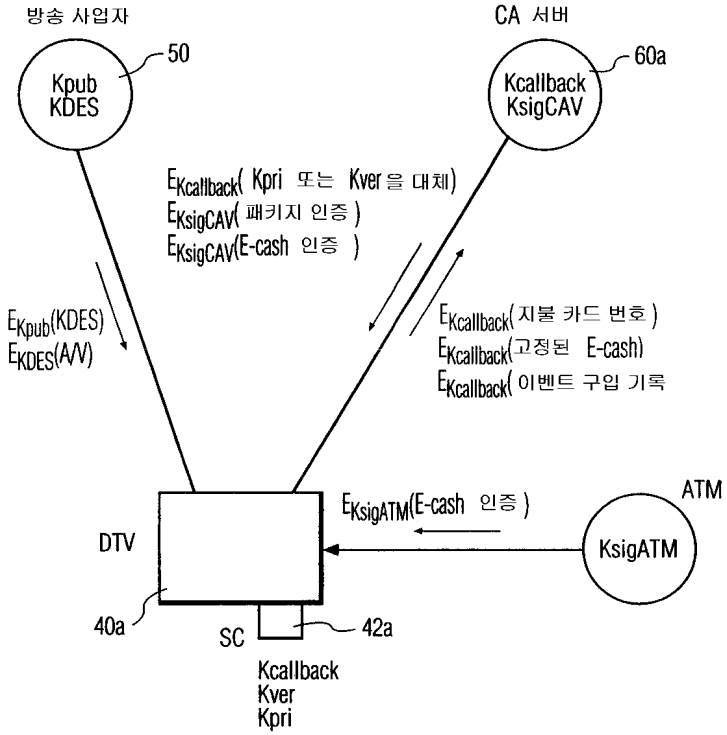
(종래 기술)


10
방송 TV
22
TV
12
케이블 TV
16a
24
STB
TV
12
SC
18a
DSS
16b
26
STB
TV
12
SC
18b

도면2


30
인증 기관
Kpublic
Kprivate
75
방송 사업자1
50
Kpublic
EKDES (이벤트)
EKpublic(KDES, 구입 정보)
40a
시청자1
60a
Ecash
인증
DTV
구입 목록
$$$
CA 1
서버
모뎀
구입 목록
CA 1 CARD
Kprivate
70
구입 목록
42a
요금 정산소
요금, $$$
40b
요금, $$$
시청자2
구입 목록
Ecash
인증
DTV
CA 2
서버
모뎀
구입 목록
구입 목록
$$$
CA 2 CARD
Kprivate
60a
42b
EKDES (이벤트)
EKpublic(KDES, 구입 정보)
Kpublic
52
방송 사업자2

도면3


방송 사업자
50
Kpub
KDES
CA 서버
60a
Kcallback
KsigCAV
EKcallback(Kpri 또는 Kver을 대체)
EKsigCAV(패키지 인증)
EKsigCAV(E-cash 인증)
EKpub(KDES)
EKDES(A/V)
EKcallback(지불 카드 번호)
EKcallback(고정된 E-cash)
EKcallback(이벤트 구입 기록
ATM
EKsigATM(E-cash 인증)
KsigATM
DTV
40a
SC
42a
Kcallback
Kver
Kpri