(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년11월04일
(11) 등록번호 10-0867033
(24) 등록일자 2008년10월29일

(51) Int. Cl.
H04N 7/167 (2006.01)
(21) 출원번호 10-2003-7001755
(22) 출원일자 2003년02월07일
심사청구일자 2007년06월05일
번역문제출일자 2003년02월07일
(65) 공개번호 10-2003-0023740
(43) 공개일자 2003년03월19일
(86) 국제출원번호 PCT/IB2002/002138
국제출원일자 2002년06월06일
(87) 국제공개번호 WO 2002/102075
국제공개일자 2002년12월19일
(30) 우선권주장
01202194.5 2001년06월08일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
EP1097589 A1
US05590197 A1
KR1020020025642 A
KR1020010082592 A
전체 청구항 수 : 총 9 항

(73) 특허권자
이르데토 아인드호벤 비.브이.
네덜란드 에이치디 후프도르프 2132 주피터스트라트 42
(72) 발명자
쉬퍼로버트
네덜란드엔엘-5656에이에이아인드호펜홀스트란6
(74) 대리인
김원준, 김창세

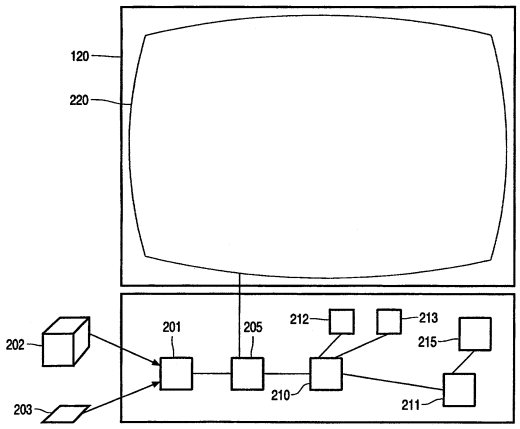
심사관 : 조남신

(54) 제어 워드를 사용하여 암호화된 서비스로 선택적으로액세스를 공급하기 위한 장치 및 방법과 스마트 카드

(57) 요 약

제어 워드를 사용하여 암호화되는 서비스(202)에 선택적으로 액세스를 공급하기 위한 장치(120), 스마트 카드(300) 및 방법이 제공된다. 서비스(202)는 인증 데이터 및 인증 데이터의 유효 기간의 지정자를 포함하는 자격 제어 메시지(ECM)(203)와 함께 수신된다. ECM(203)이 유효하게 밝혀지는 경우에만 서비스가 해독된다. 서비스(202)는 DVD와 같은 저장 매체에 저장될 수 있다. ECM 변환 부호화 모듈(211)은 ECM(203)으로부터 인증 데이터를 획득하고, 인증 데이터를 포함하는 장치-지정 ECM을 기록 수단(215)에 공급한다. 장치-지정 ECM은 장치(120)에 지정한 키로 암호화되고/되거나 장치(120)를 위한 식별자를 포함할 수 있다.

대 표 도



(81) 지정국

국내특허 : 중국, 일본, 대한민국, 미국

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

특허청구의 범위

청구항 1

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 장치로서,

인증 데이터 및 상기 인증 데이터의 유효 기간의 지정자(specifier)를 포함하는 자격 제어 메시지(ECM;entitlement control message)와 상기 서비스를 수신하기 위한 수신 수단과,

상기 제어 워드를 사용하여 상기 서비스를 해독하기 위한 해독 수단과,

시간을 제공하기 위한 타이머와,

상기 인증 데이터 및 상기 인증 데이터의 상기 유효 기간의 상기 지정자를 상기 ECM으로부터 획득하고, 상기 인증 데이터의 검증(verification)과 상기 시간이 상기 유효 기간 내에 있는지의 판정에 의존하여 상기 제어 워드를 상기 해독 수단에 제공하기 위한 조건적 액세스 수단과,

상기 ECM으로부터 상기 인증 데이터를 획득하고, 상기 인증 데이터를 포함하는 장치-지정(device-specific) ECM을 기록(writing) 수단에 공급하기 위한 ECM 변환 부호화(transcoding) 수단을 포함하는 것을 특징으로 하는

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 장치.

청구항 2

제 1 항에 있어서,

상기 조건적 액세스 수단은 상기 제어 워드가 상기 인증 데이터 내에 있으면 상기 제어 워드를 제공하도록 배치되는

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 장치.

청구항 3

제 1 항에 있어서,

상기 ECM 변환 부호화 수단은 스마트카드 내에 포함되는

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 장치.

청구항 4

제 1 항에 있어서,

상기 장치-지정 ECM은 장치의 그룹을 위한 식별자(identifier)를 포함하고, 상기 장치는 상기 그룹의 요소인

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 장치.

청구항 5

제 1 항에 있어서,

상기 장치-지정 ECM은 상기 장치를 위한 식별자를 포함하는

제어 워드를 사용하여 암호화되는 서비스에 액세스를 선택적으로 공급하기 위한 장치.

청구항 6

제 1 항에 있어서,

상기 장치-지정 ECM은 암호화 키로 암호화되고, 상기 장치는 대응 해독키를 갖는 ECM 해독 모듈을 구비하는

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 장치.

청구항 7

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 방법으로서,

인증 데이터 및 상기 인증 데이터의 유효 기간의 지정자를 포함하는 자격 제어 메시지(ECM)와 상기 서비스를 수신하는 단계와,

상기 인증 데이터의 검증과 상기 ECM으로부터 획득되는 상기 유효 기간 내의 시간인지의 판정에 의존하여 상기 제어 워드를 제공하는 단계와,

상기 제어 워드를 사용하여 상기 서비스를 해독하는 단계를 포함하고,

상기 ECM으로부터 상기 인증 데이터를 획득하고, 상기 인증 데이터를 포함하는 장치-지정 ECM을 기록 수단에 공급하는 것을 특징으로 하는

제어 워드를 사용하여 암호화된 서비스에 선택적으로 액세스를 공급하기 위한 방법.

청구항 8

인증 데이터를 ECM으로부터 획득하고 상기 인증 데이터를 포함하는 장치-지정 ECM을 기록 수단에 공급하기 위한 ECM 변환 부호화 수단을 포함하는

제 1 항의 장치에서 사용하기 위한 스마트카드.

청구항 9

제 8 항에 있어서,

상기 인증 데이터의 유효 기간의 지정자를 ECM으로부터 획득하고, 상기 인증 데이터의 검증과 상기 유효 기간 내의 시간인지의 판정에 의존하여 해독 수단에 제어 워드를 제공하기 위한 조건적인 액세스 수단을 추가적으로 포함하는

스마트카드.

명 세 서

기 술 분 야

<1> 본 발명은 제어 워드를 사용하여 암호화된 서비스에 대한 액세스를 선택적으로 공급하기 위한 장치에 관한 것으로, 그 장치는 인증 데이터 및 인증 데이터의 유효 기간의 지정자를 포함하는 자격 제어 메시지(ECM: Entitlement Control Message) 및 서비스를 수신하기 위한 수신 수단과, 제어 워드를 사용하여 서비스를 해독하기 위한 해독 수단과, 시간을 제공하는 타이머와, ECM으로부터 인증 데이터의 유효 기간의 지정자와 인증 데이터를 획득하고 인증 데이터의 검증 및 그 시간이 유효 기간 내에 있는지의 판정에 의존하여 해독 수단에 제어 워드를 제공하는 조건적 액세스 수단을 포함한다.

<2> 또한, 본 발명은 제어 워드를 사용하여 암호화된 서비스에 대한 액세스를 선택적으로 공급하는 방법에 관한 것으로, 그 방법은 인증 데이터 및 인증 데이터의 유효 기간의 지정자를 포함하는 자격 제어 메시지(ECM) 및 서비스를 수신하는 단계와, 인증 데이터의 검증과 ECM으로부터 획득된 유효 기간 내의 시간인지의 판정에 의존하여 제어 워드를 제공하는 단계와, 제어 워드를 사용하여 서비스를 해독하는 단계를 포함한다.

배 경 기 술

<3> 서두에 따른 장치는 미국 특허 번호 제 6,005,938호로부터 알 수 있다. 예약 기반 텔레비전 제공자와 같은 서비스 제공자는, 통상적으로, 그들의 서비스의 일부로 배포하는 정보가 그 서비스에 대한 요금을 지불하지 않은 사용자에 의해 액세스되는 것을 방지하는데, 그 방지는 정보를 암호화함으로써 달성된다. 서비스를 액세스하기 원하는 사용자는 서비스를 액세스하기 위하여 인증 데이터를 포함하는, 소위 자격 제어 메세지(ECM)를 획득해야 한다. ECM은 통상적으로 암호화된 서비스를 해독하는데 사용될 수 있는 제어 워드 또는 해독키를 포함할 것이다. 대안적으로, 제어 워드는 사용자가 이전에 구매하고, 그가 그의 텔레비전이나 셋-톱 박스에 삽입할 필요가 있는 스마트 카드에 저장될 수 있다. 이러한 경우에, ECM은 스마트카드가 제어 워드를 해독 모듈에 제공할 수 있게 하는 인증 데이터를 포함한다. 제어 워드를 사용하여, 해독 모듈은 서비스를 해독하고, 사용자가 그것을 액세스할 수 있게 한다. 이러한 방법으로, 사용자는 예약 기반 텔레비전을 시청하거나 대화식 서비스를 액세

스할 수 있다.

<4> 이러한 장치에서는, 사용자자 서비스 제공자로부터 수신하는 ECM을 기록하고, 서비스를 다시 한번 액세스하기 위해 그것을 다시 사용할 수 있다. 이에 따라 사용자는 그것에 대한 비용 지불 없이 서비스를 액세스할 수 있게 된다. 이것을 방지하기 위하여, 서비스 제공자는 ECM의 유효 기간의 지정자(specifier)를 ECM에 삽입하는 경우가 있다. ECM을 수신하는 스마트카드나 셋-톱 박스는 사용자가 서비스를 액세스하기 원하는 시간에 대해 지정자 또는 유효 기간을 검사하고, 현재 시간이 유효 기간을 벗어나 있으면 제어 워드를 해독 모듈에 제공하는 것을 거절할 것이다.

<5> 일부 애플리케이션의 경우에는, 서비스에 관련되는 정보의 로컬 저장이 요구된다. 예를 들면, 사용자는 나중에 편할 때 텔레비젼 프로그램을 볼 수 있도록 예약 기반 텔레비전 서비스를 통해 제공되는 텔레비전 프로그램을 녹화하길 원할 수 있다. 그러나, 정보가 간단한 형태로 저장되면, 액세스 제어는 무용지물이다. 엑세스 제어가 변함없이 유지되도록 보장하기 위하여, 정보는 암호화된 형태로 저장된다. 사용자가 저장된 정보를 나중에 액세스할 수 있도록 하기 위하여, ECM도 저장될 필요가 있다. 그러나, ECM의 유효 기간의 지정자 때문에, 유효 기간이 만료된 이후에 사용자가 그것을 재생하기 원할 때, 저장된 정보를 액세스할 수 없게 된다. 이것은 사용자가 구매했던 정보를 그가 선택한 시간에 액세스할 수 없다는 것을 의미한다.

<6> 발명의 개요

<7> 본 발명의 목적은 서두에 따른 장치를 제공하는 것으로, 그 장치는 서비스에 액세스를 제공하는 것과 관련하여 보다 높은 가요성을 가진다 .

<8> 상술한 목적은 ECM으로부터 인증 데이터를 획득하고, 인증 데이터를 포함하는 장치-지정 ECM을 기록 수단에 공급하기 위한 ECM 변환 부호화(transcoding)에 그 특징이 있는 본 발명에 따른 장치에 의해 달성된다. 장치-지정 ECM을 생성함으로써 언제라도 저장된 서비스 또는 정보를 액세스하는 것이 가능한데, 이는 장치-지정(device-specific) ECM이 유효 기간을 포함하지 않기 때문이다.

<9> 일 실시예에서, 제어 워드가 인증 데이터 내에 존재하는 경우, 조건적 액세스 수단은 그 제어 워드를 제공하기 위해 배치된다. 이러한 방법에서는, 장치가 제어 워드를 안전한 저장부의 어딘가에 저장할 필요가 없고 ECM에 있는 인증 데이터로부터 제어 워드를 간단히 획득할 수 있다.

<10> 다른 실시예에서, ECM 변환 부호화 수단은 스마트카드 내에 포함된다. 조건적 액세스 수단이 안전한 방식으로 저장되어 악질적인 사용자가 그것을 조절할 수 없게 하는 것이 바람직하다. ECM 변환 부호화 수단에 대해서도 물론 마찬가지이다. 스마트 카드 안에 이들 수단들을 넣음으로써, 다른 장치에 대한 장치-지정 ECM을 획득하기 위해, 악질적인 사용자가 그것을 조절하는 것이 훨씬 더 어렵게 된다.

<11> 다른 실시예에서, 장치-지정 ECM은 장치들의 그룹에 대한 식별자를 포함하는데, 그 장치는 그룹의 한 요소이다. 장치-지정 ECM을 하나의 특정 장치로 제한하지 않음으로써 더 큰 가요성이 획득될 수 있다. 대신에 장치-지정 ECM은 특정 장치의 그룹 식별자 또는 다수의 식별자를 구비할 수 있다. 이에 따라 사용자는, 가령, 하나의 장치상에 암호화된 서비스를 기록하고 그것을 다른 장치에서 다시 구동할 수 있게 된다.

<12> 다른 실시예에서, 장치-지정 ECM은 장치를 위한 식별자를 포함한다. 사용자가 다른 장치에 있는 그 장치-지정 ECM을 사용하지 못하도록, 그 장치에 대한 식별자는 장치-지정 ECM에 기록된다. 이러한 방법으로, 사용자는 그 특정 장치에서만 장치-지정 ECM을 사용할 수 있다.

<13> 다른 실시예에서, 장치-지정 ECM은, 장치가 대응하는 해독키를 가지는 암호키로 암호화된다. 장치-지정 ECM을 암호화함으로써, 사용자는 장치-지정 ECM을 생성했던 장치가 아닌 임의의 장치를 사용하여 장치-지정 ECM을 액세스할 수 없을 것이다. 이에 따라 장치-지정 ECM의 사본이 인증되지 않은 제 3자에게 배포되는 것이 방지된다.

<14> 본 발명의 다른 목적은 서두에 따른 방법을 제공하는 것으로, 그 방법은 서비스에 액세스를 공급하는 것과 관련하여 보다 나은 가요성을 제공한다.

<15> 상술한 목적은 ECM으로부터 인증 데이터를 획득하고, 인증 데이터를 포함하는 장치-지정 ECM을 기록 수단에 공급하는 단계에 그 특징이 있는 본 발명에 따른 방법에 의해 달성된다. 장치-지정 ECM을 생성함으로써, 언제라도 저장된 서비스 또는 정보를 액세스하는 것이 가능한데, 그 이유는 장치-지정 ECM이 유효 기간을 포함하지 않기 때문이다.

<16> 본 발명의 다른 목적은 서비스에 액세스를 제공하는 것과 관련하여 장치에 보다 큰 가요성을 제공하는 본 발명

에 따른 장치에서 사용하기 위한 스마트카드를 제공하는 것이다.

<17> 상술한 목적은 ECM으로부터 인증 데이터를 획득하고, 인증 데이터를 포함하는 장치-지정 ECM을 기록 수단에 공급하는 ECM 변환 부호화 수단에 그 특징이 있는 스마트 카드에 의해 달성된다. ECM 변환 부호화 수단을 스마트 카드 상에 저장함으로써, ECM 변환 부호화에 대한 보다 월등한 레벨의 보안이 달성된다. 더 나아가, 사용자는 그것을 수신할 수 있으며, 따라서, ECM 변환 부호화 수단을 가지는 하나의 특정 장치에 제한되지 않는 임의 장치를 가진 그의 스마트 카드를 이용할 수 있다.

<18> 일 실시예에서, 스마트 카드는 ECM으로부터 인증 데이터의 유효 기간의 지정자를 획득하고 인증 데이터의 검증과 유효 기간 내의 시간인지의 판정에 의존하여 해독 수단에 제어 워드를 제공하는 조건적 액세스 수단을 추가적으로 포함한다. 또한 조건적 액세스 수단을 스마트카드 상에 제공함으로써, 스마트카드는 스마트카드 판독 수단이 구비된 임의 장치에서 사용될 수 있는 단일 조건적 액세스 메카니즘으로서 스마트 카드가 사용될 수 있게 된다.

발명의 상세한 설명

<23> 도면 전체를 통하여, 같은 참조 번호는 유사한 특징부나 대응하는 특징부를 가리킨다. 도면에 나타나 있는 일부 특징부들은 통상적으로 소프트웨어로 구현되고, 그 경우, 소프트웨어 모듈 또는 객체와 같은 소프트웨어 엔티티를 나타낸다.

<24> 도 1은 인터넷 또는 케이블 텔레비전 망과 같은 망(110)을 통하여 연결되는 서비스 오퍼레이터 (101) 및 수신 장치(120)를 포함하는 장치(100)를 도시한다. 망(110)을 사용하여, 서비스 제공자(101)는, 수신 장치(120)의 사용자가 예약 기반 텔레비전 서비스를 액세스할 수 있게 함으로써 수신 장치(120)에 서비스의 인스턴스(instances of a service)를 제공할 수 있다. 수신 장치(120)는 셋-톱 박스, 텔레비전, 라디오, 개인용 컴퓨터 등과 같은 많은 형태를 취할 수 있다. 서비스 제공자(101)는 많은 방법으로 서비스를 제공할 수 있다. 일부 경우에, 서비스 제공자는 망을 통하여 연결되는 모든 수신 장치에 암호화된 서비스를 방송하며, 적당한 디스크램블링(descrambling) 수단을 가진 수신 장치만 서비스를 디스크램블링하고 액세스 할 수 있다. 다른 경우에는, 서비스 제공자(101)는 특정 영화나 텔레비전 프로그램과 같은 서비스의 인스턴스를 그것을 요구한 특정 가입자에게 제공한다.

<25> 통상적으로, 수신 장치(120)의 사용자는 요금을 지불했다면 서비스를 액세스하는 것만이 가능해야만 한다. 액세스를 제한하기 위하여, 서비스 제공자(101)는 그가 수신 장치(120)로 배포한 서비스 또는 그의 인스턴스를 암호화한다. 그 후, 수신 장치(120)의 사용자는 서비스를 해독하는데 필요한 적당한 제어 워드를 획득해야 한다. 사용자에게 제어 워드의 배포가 용이해질 수 있는 많은 방법이 있다. 제어 워드는 수신 장치(120)에 저장될 수 있으며 또는 사용자로부터 비용 지불 시서비스 제공자(101)에 의해 수신 장치(120)로 배포될 수 있다. 제어 워드는 망(110)을 통하여 배포되거나, 사용자가 수신 장치(120)에 삽입할 수 있는 스마트카드 상에 저장될 수 있다.

<26> 제어 워드가 수신 장치(120)에 저장되면, 서비스를 액세스하기 위하여 제어 워드를 사용하도록 서비스 제공자(101)가 수신 장치에 인증을 송신해야 한다. 수신된 인증이 없다면, 수신 장치는 서비스의 해독을 거절해야 한다. 그 인증은 소위, 자격 제어 메세지(ECM)의 형태로 배포된다. 서비스를 액세스하는 유효 인증을 수신하면, 장치는 서비스에 사용자 액세스를 제공하기 위해 제어 워드를 사용한다. 제어 워드가 수신 장치(120) 그 자체에서 이용될 수 없고, 스마트 카드 상에서도 이용할 수 없으면, 서비스 제공자(101)는 제어 워드를 ECM의 일부로 송신해야 한다.

<27> 도 2는 수신 장치(120)를 더 상세히 도시한다. 그 장치는 서비스 또는 그것의 인스턴스(202)와 ECM(203)을 서비스 제공자(101)로부터 수신하는 수신 모듈(201)을 포함한다. 인스턴스(202)는 서비스 해독 모듈(205)에 입력되며, 해독 모듈은 제어 워드를 사용하여 인스턴스(202)를 해독하고, 텔레비전 스크린과 같은 랜더링 모듈(220)에 해독된 인스턴스를 입력한다. 이러한 방법으로, 사용자는 서비스를 액세스하거나 인스턴스(202)를 볼 수 있다.

<28> 조건적 액세스 모듈(210)에 의해 서비스 해독 모듈(205)에 제어 워드가 제공된다. 조건적 액세스 모듈(210)은 인증 데이터 및 인증 데이터의 유효 기간의 지정자를 ECM(203)으로부터 획득한다. 먼저, 조건적 액세스 모듈(210)은 인증 데이터의 유효성을 검사한다. 서비스 제공자(101)는 가령, ECM(203)을 디지털적으로 서명할 수 있고, 그 후 조건적 액세스 모듈(210)은 디지털 서명을 검증한다. 추가적으로, ECM(203)이 실제로 수신된 인스턴스(202)와 함께 사용하기 위한 것인지를 체크할 필요가 있다.

<29> 또한, 조건적 액세스 모듈(210)은 ECM(203)이 여전히 유효한지를 검증할 필요가 있다. 이러한 목적을 위하여 장

치(120)는 실시간 클럭과 같이 조건적 액세스 모듈(210)에 현재의 시간을 제공하는 타이머(212)를 구비한다. 그 후, 조건적 액세스 모듈(210)은 시간이 ECM에 표시된 유효 기간 내에 있는지의 여부를 판정한다. 시작 날짜 또는 소정 날짜까지의 종료 기간 및 어떤 기간을 나타내는 유효 기간의 조합으로 또는 단순히 어떤 기간을 나타내는 값에 의해 유효 기간이 ECM(203)에서 특정될 수 있다. 추가적으로, 유효 기간은 사용자가 서비스의 인스턴스를 수신하지 못하는 기간을 특정할 수도 있다.

<30> ECM(203)이 유효하고, 현재의 시간이 유효 기간 내에 있음을 조건적 액세스 모듈(210)이 발견한다면, 조건적 액세스 모듈(210)은 서비스 해독 모듈(205)에 제어 워드를 제공한다. 제어 워드는 ECM(203) 내에 있을 수 있고 또는 그것은 장치(120) 자체 내에 저장될 수 있다.

<31> 장치(120)의 사용자가 수신된 인스턴스(202)를 하드디스크, DVD+RW 또는 CD-RW와 같은 저장 매체에 저장하기를 원할 수 있다. 이 목적을 위하여, 장치(120)는 비디오 기록기, DVD(Digital Versatile Disc) 작성기, 또는 콤팩트디스크(CD) 작성기와 같은 기록 모듈(215)을 포함한다. 이에 따라 사용자는 나중에 보기 위하여 수신된 인스턴스를 저장할 수 있게 된다. 기록 모듈(215)은 ECM(203)에 존재하는 인증 데이터를 저장해야 한다. 수신된 인스턴스(202)를 저장하기 위해서는 서비스 오퍼레이터(101)로부터의 승인이 필요하다. 이러한 승인은 가령, ECM(203) 자체 내에 주어지거나 또는 다른 자격 메세지내에 주어질 수 있다.

<32> 제어 워드가 ECM(203) 내에 있다면, 그 제어 워드는 저장 매체에 저장될 필요가 있다. 제어 워드가 없으면, 저장된 인스턴스(202)를 액세스할 수 없다. 인스턴스(202)는 암호화된 형태로 저장된다.

<33> ECM 변환 부호화(transcoding) 모듈(211)은 ECM(203)으로부터 인증 데이터를 획득하고, 인증 데이터를 포함하는 장치-지정 ECM(203)을 기록 모듈(215)에 공급한다. 장치-지정 ECM이 지정자 또는 유효 기간을 포함하지 않기 때문에, 장치-지정 ECM의 유효성은 제한되지 않는다. 이러한 방법으로, 사용자는 그가 선택하는 임의의 시간에 인스턴스를 다시 재생할 수 있고, 이는 이러한 장치를 매우 융통성 있게 만든다.

<34> 그러나, 장치-지정 ECM에 저장되는 인증 데이터는 인증되지 않은 사용에 대해 소정 방법으로 보호되는 것이 바람직하다. 예를 들면, 사용자는 장치-지정 ECM의 사본을 저장 매체로부터 만들고, 그것들을 배포하며, 그에 따라 많은 사람들이 저장된 인스턴스를 액세스할 수 있게 된다. 서비스 오퍼레이터(101)는 액세스에 대해 모든 사용자에게 정상적으로 요금을 부과하기 때문에, 이것은 바람직하지 않다.

<35> 장치-지정 ECM이 이러한 오용에 대해 보호받을 수 있는 다양한 방법들이 있다. 바람직한 실시예에서, 장치-지정 ECM은 장치(120)에 대한 식별자를 추가적으로 포함한다. 추후에, 수신 모듈(201)이 저장 매체로부터 인스턴스를 수신하면, 조건적 액세스 모듈(210)은 장치-지정 ECM에 저장된 인증 데이터를 획득할 것인데, 그 인증 데이터는 장치에 대한 식별자를 포함한다. 그 후, 조건적 액세스 모듈(210)은 장치-지정 ECM에 저장된 장치에 대한 식별자를 장치(120)에 대한 소정 식별자와 비교한다. 두 개의 식별자가 일치한다면, 조건적 액세스 모듈(210)은 장치-지정 ECM에 저장된 제어 워드를 서비스 해독 모듈(205)에 제공한다.

<36> 장치에 대한 식별자는, 장치(120)가 상기 그룹의 요소라면, 장치의 그룹에 대한 식별자로서 실현될 수 있다. 그 후, 조건적 액세스 모듈(210)은, 장치-지정 ECM이 장치(120)에 제공될 때, 그 장치(120)가 그룹의 구성요소임을 검증해야 한다.

<37> 장치-지정 ECM의 오용을 방지하기 위하여, 그것은 장치(120)가 대응하는 해독키를 가지는 암호화 키로 암호화된다. 그러한 방법으로, 장치(120)만 암호화된 장치-지정 ECM을 해독하고, 그 안의 인증 데이터를 액세스할 수 있을 것이다. 물론, 비밀-키 방식이 사용될 수도 있으나, 이는 공개 키 암호 기법으로도 실현될 수 있다. 공공/전용(public/private) 키 쌍은 장치(120)에 저장된다. ECM 변환 부호화 모듈(211)은 키 쌍의 공공 부분을 액세스하고, 그것으로 장치-지정 ECM를 암호화한다. 나중에, 조건적 액세스 모듈(210)은 키 쌍의 전용 부분을 액세스하고, 그것으로 장치-지정 ECM를 해독한다.

<38> 장치(120)는 ECM 해독 모듈(213)을 포함할 수 있고, 그 안에, 적어도 키의 전용 부분이 저장된다. 이러한 방법에서는, 악질적인 사용자가 암호화된 장치-지정 ECM를 해독하기 위하여 전용 부분의 사본을 만들어서 불법적으로 인증 데이터를 액세스할 수 없다. ECM 해독 모듈(213)은 암호화된 장치-지정 ECM 자체를 해독하거나, 또는 필요할 때, 조건적 액세스 모듈(210)에 키 쌍의 전용 부분을 제공하도록 배치될 수 있다.

<39> 해독키는 장치(120)만 인증 데이터를 액세스할 수 있도록 장치(120)에 대해 유일하다. 또한 그것은 장치의 그룹에 의해 공유될 수도 있으며, 이에 따라 장치(120)는 그 그룹의 일부로 된다. 이에 따라 인증 데이터는 하나의 장치에 의해 저장되고 그룹의 다른 장치에 의해 액세스될 수 있게 된다.

<40> 장치-지정 ECM의 복수의 사본이 저장될 수 있으며, 각 사본은 그것을 액세스할 수 있는 모든 장치에 대해 한번씩 암호화된다. 그 후, 이러한 장치의 각각은 그 자신의 사본를 액세스할 수 있지만, 다른 장치는 장치-지정 ECM를 액세스할 수 없다.

<41> 다른 실시예에서, 서비스 제공자(101)는 "수신기 식별하기" 옵션을 활성화한다. 이러한 옵션은 ECM(203)의 전용 CA 파라메터 내에 존재한다. 이 옵션은 AND 마스크 및/또는 OR 마스크를 포함한다. 존재할 때, 마스크는 그룹 액세스가 가능하도록 수신 장치의 유일한 식별 패턴을 마스크하는데 사용된다. 이러한 실시예에서, 각 수신 장치는 유일한 식별 패턴 또는 식별자를 가질 필요가 있다.

<42> 그룹 식별을 생성하기 위하여, ECM 변환 부호화 모듈(211)은 수신 장치(120)에 대한 장치 식별자에 AND-마스크 및 OR-마스크를 적용한다. 예를 들면, 그룹 식별자는 (장치 식별자 및 AND-마스크 또는) OR-마스크로서 계산될 수 있다.

<43> 그 후, ECM 변환 부호화 모듈(211)은 장치-지정 ECM을 암호화하는 암호화 키를 생성하기 위하여 그룹 식별자를 상술한 암호화 키와 결합한다. 그 후, 장치-지정 ECM은 원래의 AND 및/또는 OR 마스크와 암호 키 결과를 포함한다.

<44> 장치-지정 ECM을 암호화하기 위한 암호화 키는 바람직하게는 그룹 식별자와 연관되고, 해싱 함수(hashing function)부에 입력된다. 해싱 함수부의 출력은 장치-지정 ECM을 검사하고, 생성하고, 해독하고 암호화하는데 사용되는 다각적인 키이다. 이러한 접근법의 이로운 점은 이러한 장치-지정 ECM가 그룹 내의 임의 장치에 의해서 즉시 지금 사용될 수 있다는 것이다. 더 나아가, 해싱 함수를 사용함으로써, 출력의 길이는 입력의 길이에 좌우되지 않는다.

<45> 도 3은 조건적 액세스 모듈(210)과, ECM 변환 부호화 수단(211)과, 보안 저장 모듈(301)을 포함하는 스마트카드(300)를 도시한다. 조건적 액세스 모듈(210) 및 ECM 변환 부호화 모듈(211)은 인증 데이터를 다루고, 사실상 사용자에게 서비스에 대한 액세스를 제공하기 때문에, 그것들은 가능한 최대의 보안이 제공되어야 한다. 이러한 모듈을 보호하는 효과적인 방법은 이들을 스마트카드 상에 구현하는 것이다. 스마트카드는 보통의 컴퓨터 또는 소프트웨어보다 손상시키기 훨씬 더 어려워서 조건적 액세스 서비스의 조건적 측면을 보호하는 더 좋은 방법을 제공한다. 그 후, 장치(120)에 스마트카드 판독 모듈(310)이 설비되고, 사용자가 스마트카드(300)를 그 모듈(310)에 삽입할 수 있다. 스마트카드 판독 모듈(310)은, 장치(120)에 구현되는 수신 모듈(201)과 서비스 해독 모듈(205) 사이, 및 스마트카드에 내장되는 조건적 액세스 모듈(210)과 ECM 변환 부호화 모듈(211) 사이의 통신을 촉진시킨다.

<46> 서비스를 해독하는데 필요한 제어 워드는 스마트 카드 상의 보안 저장 모듈(301)에 저장될 수 있다. 이러한 방법에서는, 사용자가 제어 워드를 획득하는 것이 매우 어려우며, 그에 따라 그에 대한 비용 지불 없이 그가 서비스를 액세스하는 것이 아주 어렵게 된다.

<47> 장치(120)는 단순히 서비스를 해독하는 것이 아니라, 대신에 제어 워드를 저장하거나 서비스 제공자(101)로부터의 승인 없이 암호화되지 않은 서비스를 저장하는 방법으로 조작되었을(tamper) 가능성이 있다. 이러한 변경된 장치가 제어 워드를 액세스하는 것을 방지하기 위하여, 스마트카드(300)는 인증 메카니즘을 이용하여 장치(120)가 조작되는지 여부를 검증한다. 이러한 인증 메커니즘은 가령, 스마트카드가 암호화된 "챌린지(challenge)"를 장치(120)에 발행하게 함으로써 실현되는데, 장치(120)는 이를 해독하고 스마트카드(300)에 다시 송신해야 한다. 장치(120)가 챌린지를 정확하게 해독할 수 없다면, 그것은 컴플라이언트(compliant) 장치가 아니며, 제어 워드에 대한 액세스를 얻을 수 없다. 이와 달리, 스마트카드(300)는 장치(120)에 의해 실행될 프로그램 코드의 일부의 무결성을 가령, 디지털 서명을 검증함으로써 검사할 수 있다.

<48> 제어 워드가 보안 저장 모듈(301)에 저장되지 않고 대신에 ECM(203)에 제공된다면, ECM(203)이 스마트카드(300)에 제공되고, 이에 따라 조건적 액세스 모듈(210)에 제공되며, 조건적 액세스 모듈(210)은 제어 워드를 ECM(203)으로부터 획득한다. 제어 워드는 ECM(203)내에 암호화된 형태로 존재할 수 있으며, 그 경우 조건적 액세스 모듈(210)은 제어 워드를 우선적으로 해독할 필요가 있을 것이다. 그 후, 제어 워드를 해독하는데 필요한 해독키는 보안 저장 모듈(301)에 저장될 수 있다.

<49> 다른 실시예에서의 스마트카드(300)는 ECM 해독 모듈(213)을 추가적으로 포함한다. 이에 따라 사용자는 스마트카드(300)와 함께 사용할 수 있는 임의 장치 상의 암호화 장치-지정 ECM을 액세스할 수 있게 된다. 그 후, 장치-지정 ECM을 암호화하는데 사용되는 암호 키는, 대응하는 해독키가 ECM 해독 모듈(213)에서 사용 가능한 키일 필요가 있다.

도면의 간단한 설명

<19> 본 발명의 이러한 측면들 및 다른 측면들은 도면에 도시되어 있는 실시예를 참조하여 명백해질 것이다.

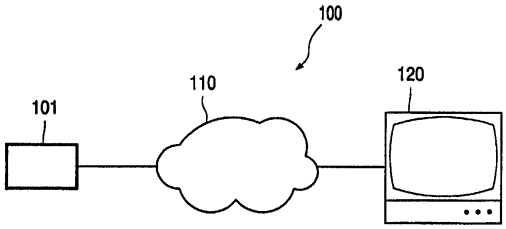
<20> 도 1은 서비스 오퍼레이터 및 수신 장치를 포함하는 본 발명에 따른 장치를 도시한다.

<21> 도 2는 본 발명에 따른 장치를 더 상세히 도시한다.

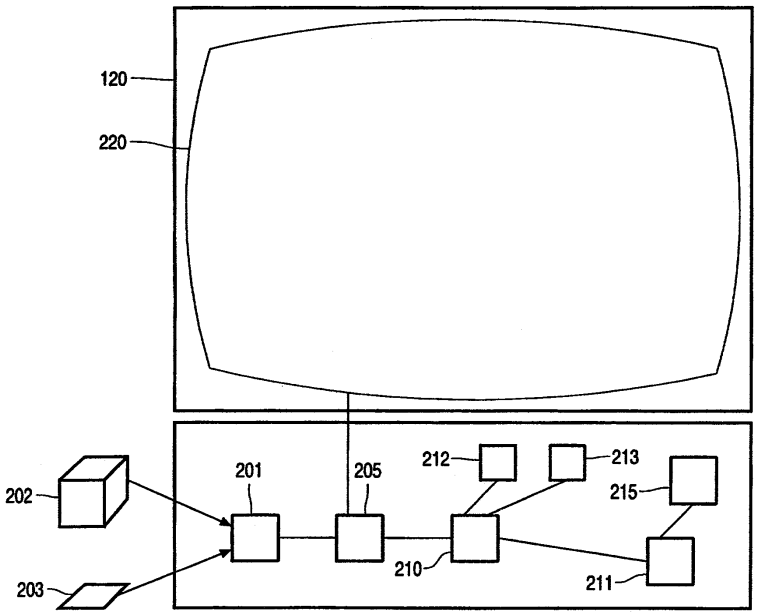
<22> 도 3은 본 발명에 따른 스마트카드를 더 상세히 도시한다.

도면

도면1



도면2



도면3