(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G11B 20/10

(45) 공고일자 2005년11월02일
(11) 등록번호 10-0525813
(24) 등록일자 2005년10월26일

(21) 출원번호 10-2003-0079188
(22) 출원일자 2003년11월10일

(65) 공개번호 10-2005-0045211
(43) 공개일자 2005년05월17일

(73) 특허권자 (주)잉카엔트웍스
서울 강남구 역삼동 747-2 해성빌딩 5층

(72) 발명자 범재룡
경기도 용인시 기흥읍 영덕리 928 세종그랑시아 106-204 11통 10반

안성민
서울특별시 강서구 화곡동 1113-19 2층 201호

(74) 대리인 김도형

심사관 : 장대교

(54) 호스트 플레이어를 위한 콘텐츠 보안처리 시스템 및 그 방법

요약

본 발명은 플래시메모리를 내장하지 않는 형태의 디지털 오디오 재생장치인 호스트 플레이어를 사용함에 있어서 외부 시스템으로부터 제공되는 디지털 콘텐츠 파일에 대한 불법복제를 방지함으로써 상기 디지털 콘텐츠 파일에 일체된 저작권을 보호할 수 있는 콘텐츠 보안처리 시스템에 관한 것이다. 본 발명에 따르면 플래시메모리를 내장하지 않는 형태의 디지털 오디오 재생장치인 호스트 플레이어를 사용함에 있어서 표준 UMS 규격의 플래시디스크 상에 저장된 디지털 콘텐츠 파일의 불법복제를 효과적으로 방지함으로써 디지털 콘텐츠 파일에 일체된 저작권을 보호할 수 있고, 인증데이터의 버전관리와 무결성 검사를 수행함으로써 보안장치가 해킹되더라도 조속하게 이에 대응하는 새로운 버전의 인증데이터를 유포시킴으로써 상기 해킹의 피해확산을 방지할 수 있다는 장점이 있다.

대표도

도 2

색인어

호스트 플레이어, MP3 데이터, 저작권 보호, 보안처리, 인증데이터

명세서

도면의 간단한 설명

도 1은 본 발명의 콘텐츠 보안처리 시스템이 적용되는 호스트 플레이어의 내부구성을 개념적으로 도시하는 도면.

도 2는 본 발명에 따른 콘텐츠 보안처리 시스템의 내부구성의 실시예를 도시하는 도면.

도 3은 본 발명에 따른 콘텐츠 보안처리 시스템에서 호스트 플레이어의 동작 실시예를 도시하는 흐름도.

도 4는 본 발명에 따른 콘텐츠 보안처리 시스템에서 관리자 프로그램의 동작 실시예를 도시하는 흐름도.

도 5는 본 발명에 따른 콘텐츠 보안처리 시스템에서 사용가능한 인증서파일 및 내장인증서의 실시예를 도시하는 도면.

<도면의 주요 부분에 대한 부호의 설명>

210 : 호스트 플레이어 211 : 제어모듈

212 : 보안모듈 213 : 디코딩모듈

214 : 복호화모듈 215 : 보안메모리

230 : 플래시디스크 231 : 플래시메모리

250 : 관리자 프로그램 251 : USB 자동검출모듈

252 : 인증데이터 관리모듈 253 : 암호화모듈

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 플래시메모리를 내장하지 않는 형태의 디지털 오디오 재생장치인 호스트 플레이어를 사용함에 있어서 외부의 시스템으로부터 제공되는 디지털 콘텐츠 파일에 대한 불법복제를 효과적으로 방지함으로써 상기 디지털 콘텐츠 파일에 일체된 저작권을 보호할 수 있는 호스트 플레이어를 위한 콘텐츠 보안처리 시스템에 관한 것이다.

종래로 플래시메모리 내장형 MP3 플레이어, 하드디스크 내장형 MP3 플레이어, 또는 CDP형 MP3 플레이어 등과 같은 다양한 형태의 디지털 오디오 재생장치가 사용되어 왔으며, 본 특허출원의 공동출원인인 (주)넥스트웨이는 대한민국 실용신안등록출원 제20-2002-0021305호와 미공개 상태인 대한민국 특허출원 제10-2003-0040147호에서 플래시디스크나 하드디스크와 같은 비휘발성 공간을 내장하지 않고 표준 UMS 규격에 따른 USB 저장장치, 소위 "플래시디스크"를 사용할 수 있는 호스트 플레이어의 개념을 제시한 바 있다.

도 1은 본 발명의 콘텐츠 보안처리 시스템이 적용되는 호스트 플레이어(110)의 내부구성을 개념적으로 도시하는 도면이다. 호스트 플레이어(110)는 표준 UMS 규격을 지원하고 USB 호스트 모드로 동작하는 USB 인터페이스(112), 시스템 동작을 제어하는 제어모듈(111), 디지털 오디오 데이터를 특정 규격에 따라 디코딩하는 디코딩모듈(113)을 포함하여 구성되며, 이중에서 제어모듈(111)과 디코딩모듈(113)은 통상 표준 DSP 및 펌웨어로서 구성된다. 전술한 바와 같이 호스트 플레이어(110)는 디지털 오디어 파일을 저장하기 위한 플래시메모리나 하드디스크 등의 비휘발성 공간을 내장하지 않으며, 대신 외부의 플래시디스크(130)로부터 상기 디지털 오디어 파일을 제공받는다.

즉, 통상의 플래시디스크(130)는 표준 UMS 규격을 지원하고 USB 디바이스 모드로 동작하는 USB 인터페이스(132) 및 디지털 오디어 파일을 저장하기 위한 비휘발성 메모리 공간을 제공하는 플래시메모리(131)를 포함하여 구성되며, 호스트 플레이어(110)는 USB 인터페이스(112, 132)를 통하여 플래시메모리(131)를 액세스함으로써 상기 저장된 디지털 오디어 파일을 판독하여 디코딩모듈(113)에서 디코딩하도록 동작한다. 상기 도시된 호스트 플레이어(110)의 내부구성은 개념적인 것에 불과하며 실제 호스트 플레이어(110)는 도시된 것보다 더 많은 구성요소를 포함하여 구성되는 것으로 이해되어야 한다.

이러한 호스트 플레이어(110)에 있어서 디지털 오디오 파일은 통상의 플래시디스크(130)를 사용하는 것으로 가정하고 있으므로 상기 오디오 파일의 불법복제에 대해서는 아직 무방비 상태이다. 따라서, 표준 UMS 규격에 따른 통상의 플래시디스크(130)와 함께 호스트 플레이어(110)를 사용하되 상기 플래시디스크(130)에 저장된 디지털 오디오 파일의 불법복제를 방지할 수 있는 콘텐츠 보안처리 시스템 및 그 방법이 요망된다.

발명이 이루고자 하는 기술적 과제

이에, 본 발명은 플래시메모리를 내장하지 않는 형태의 디지털 오디오 재생장치인 호스트 플레이어를 사용함에 있어서 외부 시스템으로부터 제공되는 디지털 콘텐츠 파일에 대한 불법복제를 방지함으로써 상기 디지털 콘텐츠 파일에 일체된 저작권을 보호할 수 있는 호스트 플레이어를 위한 콘텐츠 보안처리 시스템을 제공하는 데에 그 목적이 있다.

발명의 구성 및 작용

전술한 바와 같은 본 발명의 목적을 달성하기 위해서, 본 발명은 (1) 내장인증서를 저장하기 위한 보안메모리; 외장장치와 결합되기 위한 디지털 접속부; 상기 보안메모리 내에 유효한 내장인증서가 존재하는지 여부를 검사하여 ① 존재한다면 상기 내장인증서에 기초하여 제1 인증서파일을 생성하여 상기 외장장치 내에 기록하고 ② 존재하지 않는다면 상기 외장장치 내에 특정 포맷의 인증요청서 파일을 기록하며 ③ 상기 내장인증서에 기초하여 복호화-키를 획득하기 위한 보안모듈; 상기 외장장치로부터 판독한 디지털 콘텐츠 파일의 데이터를 재생하기 위한 디코딩모듈; 및 상기 디지털 콘텐츠 파일이 암호화된 경우 상기 복호화-키를 이용하여 상기 디지털 콘텐츠 파일의 데이터를 복호화 처리하기 위한 복호화모듈을 구비하는 호스트 플레이어; 및 (2) 디지털 접속을 통해 외장장치가 접속되는 것을 자동검출하기 위한 UMS 자동검출모듈; 상기 외장장치 내에 유효한 제3 인증서파일이 존재하는지 여부를 검사하여 ① 존재한다면 상기 제3 인증서파일에 기초하여 암호화 키를 획득하고 ② 존재하지 않는다면 상기 외장장치에 저장된 특정 포맷의 인증요청서 파일에 기초하여 제4 인증서파일을 생성하여 상기 외장장치 내에 기록하고 상기 제4 인증서파일에 기초하여 암호화-키를 획득하는 인증데이터 관리모듈; 및 상기 암호화 키를 사용하여 상기 디지털 콘텐츠 파일의 데이터를 암호화 처리하기 위한 암호화모듈을 구비하는 관리자 프로그램을 포함하여 구성되는 콘텐츠 보안처리 시스템을 제공한다.

이하, 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

도 2는 본 발명에 따른 콘텐츠 보안처리 시스템의 내부구성의 실시예를 도시하는 도면이다.

본 발명에 따른 호스트 플레이어(210)는 도 1을 참조하여 전술한 바 종래의 호스트 플레이어(110)와 기본적인 구성에 있어서 동일하며, 다만 제어모듈(211)에서의 시스템 동작, 특히 디지털 콘텐츠의 보안처리 동작에 있어서 상이하고 또한 상기 디지털 콘텐츠의 보안처리 동작을 보조하기 위하여 보안모듈(212), 복호화 모듈(214), 보안메모리(215)를 구비하는 점에서 상이하다. 상기 보안모듈(212), 복호화 모듈(214), 보안메모리(215)는 하드웨어 및/또는 펌웨어, 혹은 양자의 결합으로서 선택적으로 구현될 수 있다.

상기 보안메모리(215)에는 본 발명에 따른 콘텐츠 보안처리를 위한 내장인증서가 저장되어 있는데, 그 저장내용을 사용자가 삭제할 수도 없고 외부에서 판독할 수도 없을 뿐만 아니라 장치(210)를 분해하여 메모리 모듈을 탈거하더라도 그 내용을 해독하지 못하도록 구성되는 것이 바람직하다. 보안메모리(215)는 저장내용에 대한 사용자 삭제 및 외부판독을 물리적으로 방지하기 위해서 소위 배드블록(bad block)으로 설정될 수 있다.

다만, 호스트 플레이어(210)는 디지털 콘텐츠 파일을 저장하기 위한 데이터 공간이 플래시메모리(231)와 같이 외부에 형성되어 있고 관리자 프로그램(250)과 직접 인터페이스할 경우도 없으므로 별도의 EEPROM을 사용하거나 혹은 펌웨어를 저장하는 NOR 메모리 공간을 활용하여 보안메모리(215)를 구성할 수도 있다. 또한, 메모리 모듈을 탈거하더라도 외부에서 그 저장된 내용을 해독하지 못하도록 하기 위해서는 상기 보안메모리(215)의 저장내용이 소위 사이퍼텍스트(ciphertext)의 형태로 저장되는 것이 바람직하다. 보안메모리(215)에 관한 상기 내용은 본 발명의 호스트 플레이어(210)에 대한 선택적 사항이다.

상기 내장인증서는 상태코드, 호스트 플레이어의 식별자, 디지털 콘텐츠를 암호화/복호화하기 위한 키 값(key value), 상기 키 값을 생성하는 데에 사용할 수 있는 난수(random number), 상기 내장인증서의 데이터 무결성을 체크하기 위한 소정의 체커 필드의 전부 또는 일부를 포함하여 구성된다. 상기 내장인증서의 일 실시예에 대해서는 도 5를 참조하여 후술한다. 한편, 상기 보안메모리(215) 영역은 호스트 플레이어(210)의 초기 출시 상태에서는 NULL로 채워져 있을 수도 있고 혹은 특정의 유효한 내장인증서가 기록되어 있을 수도 있으며, 이에 대해서는 도 3 및 도 4를 참조하여 후술한다.

상기 보안모듈(212)은 본 발명의 콘텐츠 보안처리에 따른 특정의 암호화 알고리즘을 수행하기 위한 펌웨어 혹은 집적회로를 포함하여 구성된다. 먼저, 보안모듈(212)이 제공하는 특정의 암호화 알고리즘은 Diffie-Helman, RSA, ECC 등과 같은 공개키 기반의 암호화 알고리즘이 바람직하나 호스트 플레이어(210)의 시스템 성능을 고려하여 쉐어드-키나 키선택 벡터 기반의 암호화 알고리즘을 채용할 수도 있으며, 이러한 알고리즘은 펌웨어 형태로 제공될 수 있고 혹은 집적회로의 형태로 제공될 수 있다. 이러한 암호화 알고리즘을 통해 본 발명에 따른 디지털 콘텐츠의 보안처리 시스템의 보안성을 제고할 수 있으며, 제어모듈(211)은 본 발명에 따라 수행하는 특정의 암호화 알고리즘을 상기 보안모듈(212)을 통하여 효율적이고도 신속하게 수행한다.

상기 복호화모듈(214)는 통하여 플래시디스크(230)로부터 판독한 디지털 콘텐츠 파일이 관리자 프로그램(250)에 의해 암호화 처리된 상태인 경우에 이에 대응하여 복호화 처리를 수행하기 위한 것으로서, 상기 복호화모듈(214)에서 사용하기 위한 복호화-키(descrambling key)는 상기 보안메모리(215)에 저장된 내장인증서에 기초하여 제어모듈(211)과 보안모듈(212)의 협조동작을 통하여 획득된다. 본 명세서에서는 암호화 모듈(253)과 복호화모듈(214)에서 사용하는 암호화/복호화 알고리즘에 대해서는 특정하지 않으며, DES, MD-5 등과 같은 공지기술의 알고리즘을 사용하여 구현할 수 있다.

본 발명에 따른 관리자 프로그램(250)은 호스트 플레이어(210)에 대해 디지털 콘텐츠 보호처리를 수행하기 위하여 개인용 컴퓨터에 설치되는 일종의 소프트웨어로서, USB 등과 같은 디지털 접속을 통해 플래시디스크(230)를 액세스하여 플래시메모리(231)에 데이터를 기록할 수도 있고 플래시메모리(231) 내의 데이터를 판독할 수도 있다. 본 발명의 디지털 콘텐츠 보호처리 시스템에 따르면, 관리자 프로그램(250)은 플래시디스크(230)로부터 인증서파일을 판독한 후 이에 기초하여 암호화-키를 생성하며 상기 암호화-키를 사용하여 디지털 콘텐츠 파일을 암호화한 후 플래시디스크(230)로 복사하는 기능을 담당한다.

관리자 프로그램(250)은 USB 자동검출모듈(251), 인증데이터 관리모듈(252), 및 암호화모듈(253)을 포함하여 구성된다. 먼저, USB 자동검출모듈(251)은 플래시디스크(230)가 USB를 통하여 접속된 경우, 상기 디지털 접속을 감지하여 플래시디스크(230)를 표준 UMS 규격에 따른 대용량 저장장치(UMS 장치)로 인식하도록 동작한다. 또한, 인증데이터 관리모듈(252)은 플래시메모리(231)에 로딩된 인증서파일을 전송받아 그 유효성을 판단하고 만일 유효하다면 상기 인증서파일에 기초하여 암호화-키를 생성하며, 만일 인증서파일이 존재하지 않고 인증요청서 파일이 로딩되어 있는 경우에는 상기 인증요청서 파일에 기초하여 인증서파일을 신규 발행하고 상기 플래시메모리(231)에 기록하는 기능을 수행한다. 한편, 암호화모듈(253)은 플래시디스크(230)로 전송하는 디지털 콘텐츠 파일의 데이터를 특정의 암호화-키 값에 따라 암호화 처리하는 기능을 수행한다.

한편, 도 2에서는 호스트 플레이어(210)가 플래시디스크(230)를 사용하는 것으로 도시되어 있으나, 본 발명의 사상은 이에 한정되지 않으며 널리 일반적인 외장장치를 사용하는 경우에 대한 것으로 해석되어야 한다. 또한, 도 2에 도시된 호스트 플레이어(210)는 디지털 콘텐츠 파일을 저장하기 위한 비휘발성 메모리를 내장하지 않는 것으로 도시되어 있으나, 본 발명의 사상은 이에 한정되지 않으며 널리 디지털 인터페이스를 통해 외장장치(230)를 호스팅하여 이로부터 디지털 콘텐츠 파일을 판독하여 재생할 수 있는 기능을 갖는 장치에 대한 것으로 해석되어야 한다. 또한, 도 2에는 USB 인터페이스를 이용하는 것으로 되어 있으나, 본 발명의 사상은 이에 한정되지 않으며 널리 디지털 인터페이스를 이용하는 것으로 해석되어야 한다.

도 3은 본 발명에 따른 콘텐츠 보안처리 시스템에서 호스트 플레이어(210)의 동작 실시예를 도시하는 흐름도이다.

본 발명에 따른 호스트 플레이어(210)는 파워-온(ST301)되면, 전술한 보안메모리(215) 내에 내장인증서가 존재하는지 여부를 체크(ST302)하여 만일 존재하면 내장인증서의 무결성을 검사(ST303)하고, 그 결과 유효한 것으로 판단되면 플래시디스크(230)의 접속을 대기(ST305)한다. 전술한 내장인증서의 바람직한 실시예는 도 5의 필드포맷 (d)에 도시된다. 본 발명의 실시예에 따르면 상기 내장인증서는 보안메모리(215) 내에 저장되는데, 상기 호스트 플레이어(210)는 제품 출시시에 보안메모리(215) 내에 내장인증서를 가진 상태로 제조될 수도 있고 아니면 NULL로 채워져 출시될 수도 있다.

상기 무결성 검사(ST303)는 다양한 방식으로 이루어질 수 있는데, 가장 간단하게는 내장인증서 내에 에러체킹(error checking) 필드를 마련하여 이를 통해 상기 내장인증서가 유효한 것인지 여부를 체크하는 것이며, 이에 대해서는 도 5를 참조하여 상세히 후술한다. 상기 무결성 검사(ST303)는 어떠한 요인에 의해 보안메모리(215) 내에 잘못된 내장인증서가 있을 수 있는 가능성을 제거하기 위함이며, 이러한 요인으로는 애초에 잘못된 값이 기록된 경우, 외부 충격에 의해 메모리 모듈이 손상된 경우, 메모리 모듈이 불량한 경우, 시스템 수리를 통해 신규의 메모리 모듈이 장착된 경우 등을 가정할 수 있다.

호스트 플레이어(210)는 플래시디스크(230)가 접속되면 플래시메모리(231) 내에 인증서파일을 기록(ST306)하는데, 상기 인증서파일은 전술한 내장인증서에 기초하여 호스트 플레이어(210)가 생성하는 것으로서, 상기 인증서파일의 바람직한 실시예는 도 5의 필드포맷 (a)에 도시된다. 도 5에 도시된 필드포맷[(a), (d)]을 참조하면, 내장인증서에 기초하여 인증서파일을 생성하는 것이 가능하다. 플래시디스크(230)에 인증서파일을 기록(ST306)함으로써 호스트 플레이어(210)와 플래시디스크(230) 간의 상호결합이 이루어지는데, 상기 기록된 인증서파일의 용도에 대해서는 도 4를 참조하여 상세히 설명한다.

다만, 본 발명에서 채용하는 플래시디스크(230)는 보안성이 없는 통상의 외장장치이므로, 제3자가 인증서파일의 내용을 판독하여 본 발명의 콘텐츠 보안처리 시스템을 해킹하는 것을 방지하기 위해 인증서파일은 호스트 플레이어(210)와 관리자 프로그램(250)만 해독할 수 있는 형태로 암호화 처리되는 것이 바람직하며, 구체적인 방법은 공개키 암호화 방식이나 대칭키 암호화 방식 등의 공지된 암호화 기법을 이용하여 구현할 수 있다. 다만, 본 발명에 따른 호스트 플레이어(210)에서 사용하는 외장장치(230)가 자체적으로 충분한 보안성을 갖춘 경우에는 상기와 같은 별도의 암호화 처리는 생략될 수 있다. 한편, 본 명세서에서는 플래시디스크(230)에 하나의 인증서파일이 기록되는 것으로 가정되어 있으나, 플래시디스크(230)에 대해서 자료관리 등의 기법을 적용하면 복수 개의 인증서파일을 기록하여 관리하는 것도 가능하다.

단계(ST306)에서 호스트 플레이어(210)가 플래시디스크(230)에 인증서파일을 기록하는데, 때로는 플래시디스크(230) 내에 이미 동일한 내용의 인증서파일이 이미 기록되어 있을 수도 있다. 이는 호스트 플레이어(210)와 플래시디스크(230) 간의 상호결합이 이전에 이루어졌던 경우로서, 도 4를 참조하여 후술하는 바와 같이 상기 인증서파일에 기초하여 획득가능한 암호화-키(scrambling key)를 이용하여 관리자 프로그램(250)이 디지털 콘텐츠 파일을 암호화 처리하여 플래시디스크(230)에 기록하였을 수 있다. 이에, 호스트 플레이어(210)는 상기 내장인증서에 기초하여 복호화-키(descrambling key)를 획득(ST307)하고, 플래시디스크(230)로부터 디지털 콘텐츠 파일을 판독(ST308)하며, 상기 디지털 콘텐츠 파일에 대한 복호화 처리 및 디코딩 처리를 수행한다.

한편, 앞의 설명에서는 호스트 플레이어(210)가 내장인증서에 기초하여 복호화-키를 획득한다고 기술하였으나, 내장인증서와 인증서파일은 서로 매칭만 이루어지면 실질적인 내용에서 차이가 없으므로 "내장인증서에 기초하여 복호화-키를 획득"하는 것은 "인증서파일에 기초하여 복호화-키를 획득"하는 것과 그 내용에 있어서 사실상 동일하다. 전술한 바, 내장인증서와 인증서파일이 서로 매칭이 이루어졌는지의 여부는, 도 5의 필드포맷 (a)를 참조하면 명백한 바와 같이, 인증서파일에 기록되어 있는 특정 정보, 예컨대 모델명이나 플레이어 식별자를 참조하여 검사할 수 있다.

도 5의 필드포맷 (a)와 (d)를 참조하면, 호스트 플레이어(210)는 내장인증서 또는 인증서파일의 "키 값" 필드로부터 바로 복호화-키를 획득할 수 있으며, 보다 보안성을 높이기 위해서는 내장인증서 또는 인증서파일의 특정 필드에 대해서 소정의 연산을 수행함으로써 획득할 수도 있다. 또한, 단계(ST309)에서 호스트 플레이어(210)는 플래시디스크(230)로부터 판독한 디지털 콘텐츠 파일을 검사하여 암호화 처리된 상태인지 여부를 판단하고, 암호화 처리된 상태이면 복호화-키를 사용하여 디지털 콘텐츠 파일의 데이터에 대해서 복호화 처리를 수행한 후 디코딩을 수행하고, 암호화 처리되지 않은 상태이면 복호화 처리는 불필요하므로 바로 디코딩을 수행한다. 디지털 콘텐츠 파일이 암호화 처리된 상태인지 여부의 판단은 다양한 형태로 이루어질 수 있는데, 예컨대 파일의 확장자로부터 판단할 수도 있고, 파일의 특정 헤더포맷으로부터 판단할 수도 있다.

한편, 호스트 플레이어(210)의 보안메모리(215) 내에 내장인증서가 존재하지 않거나 혹은 내장인증서가 유효하지 않는 경우에는, 먼저 플래시디스크(230)의 접속을 대기(ST310)하고 접속된 플래시디스크(230) 내에 신규발행 인증서파일이 존재하는지 여부를 판단(ST311)한다. 이 때, 신규발행 인증서파일이란 도 4를 참조하여 후술하는 바와 같이 본 발명에 따른 관리자 프로그램(250)이 신규로 발행하여 플래시디스크(230)에 기록한 인증서파일을 말하며, 도 5의 필드포맷 (c)에 실시예를 도시하였다.

만일 신규발행 인증서파일이 존재하는 경우에는, 먼저 무결성 검사를 수행하고 유효하다면 자신이 이전에 요청하였던 내용과 매칭되는지 여부를 판단(ST312)한다. 그 결과, 매칭성이 확인되면 상기 신규발행 인증서파일에 기초하여 내장인증서를 작성하여 보안메모리(215) 내에 기록(ST314)한다.

상기 신규발행 인증서파일은 호스트 플레이어(210)가 발행을 요청하고 이에 대응하여 관리자 프로그램(250)이 신규로 발행한 것으로서, 호스트 플레이어(210)는 상기 발행요청에 관한 자료를 내부에 보유하고 있다. 호스트 플레이어(210)는 인증서파일의 신규발행을 요청할 때 바람직하게는 난수를 발생시켜 상기 인증요청서 파일에 삽입하여 전달하고, 관리자 프로그램(250)은 상기 난수를 신규발행 인증서파일에 역시 삽입하여 호스트 플레이어(210)로 전달하므로 상기 난수 값을 비교하면 상기 매칭성을 판단(ST312)할 수 있다.

이러한 인증요청서 파일 및 신규발행 인증서파일의 실시예는 도 5의 필드포맷 (b) 및 (c)에 도시되어 있으며, 도시된 바와 같이 인증요청서 파일과 신규발행 인증서파일에는 난수 필드가 마련되어 있다. 한편, 난수를 사용하지 않고 플레이어 식별자를 이용하여 매칭성을 판단할 수도 있으나, 하나의 호스트 플레이어(210)가 인증서파일의 신규발행을 다수 회 요청하였을 수 있으므로 난수를 이용하는 것이 안전하다. 그러나, 플레이어 식별자를 이용하여 매칭성을 판단하는 것도 장점이 있으므로 난수 이용의 여부는 선택적인 것으로 해석되어야 한다. 한편, 전술한 바 호스트 플레이어(210)는 인증서파일의 신규발행 요청에 대한 정보를 저장하고 있는데, 그 저장장소로는 보안메모리(215)가 바람직하며 도 5의 필드포맷 (e)는 상기 저장되는 정보의 실시예를 도시한다.

한편, 신규발행 인증서파일이 존재하지 않거나 존재하더라도 매칭성이나 무결성에 문제가 있는 경우에는 호스트 플레어이(210)는 플래시디스크(230)의 플래시메모리(231) 내에 인증요청서 파일을 기록(ST315)하는데, 상기 인증요청서 파일에 대해서는 전술한 바와 같다.

도 4는 본 발명에 따른 콘텐츠 보안처리 시스템에서 관리자 프로그램(250)의 동작 실시예를 도시하는 흐름도이다.

본 발명에 따른 관리자 프로그램(250)은 실행(ST401)되면 USB 등의 디지털 접속을 통한 플래시디스크(230)의 접속을 대기(ST402)하고, 플래시디스크(230)가 접속되면 내부의 플래시메모리(231)에 특정의 인증서파일이 존재하는지 여부를 검사(ST403)한다. 도 3을 참조하여 전술한 바와 같이, 인증서파일은 단계(ST306)에서 호스트 플레이어(210)가 기록하는 것으로서 그 바람직한 실시예는 도 5의 필드포맷 (a)에 도시된 바와 같다.

상기 검사(ST403) 결과, 플래시디스크(230) 내에 인증서파일이 존재하면 상기 인증서파일의 무결성을 검사(ST404)하고, 그 결과 유효라고 판단되면 상기 인증서파일에 기초하여 암호화-키를 획득(ST406)한다. 관리자 프로그램(250)은 상기 획득된 암호화-키를 사용하여 암호화모듈(253)에서 디지털 콘텐츠 파일의 데이터에 대한 암호화 처리를 수행(ST407)하며, 암호화 처리가 완료된 디지털 콘텐츠 파일을 플래시디스크(230)로 복사한다.

한편, 플래시디스크(230) 내에 인증서파일이 존재하지 않거나 혹은 무결성 검사(ST404)에서 인증서파일에 오류가 있는 것으로 드러난 경우에는, 관리자 프로그램(250)은 단계(ST408)로 진행하여 플래시디스크(230) 내에 유효한 인증요청서 파일이 존재하는지 여부를 검사하고, 만일 유효한 인증요청서 파일이 존재한다면 상기 인증요청서 파일에 기초하여 신규의 인증서파일을 생성(ST409)하여 플래시디스크(230) 내에 기록한다. 반면, 플래시디스크(230) 내에 유효한 인증요청서 파일이 존재하지 않는 경우에는 화면에 에러를 디스플레이하고 콘텐츠 보안처리 동작을 중단(ST410)한다.

바람직하게는, 관리자 프로그램(250)은 인증서파일을 신규로 발행하여 플래시메모리(230)에 기록한 경우에는 단계(ST406)로 진행하여 상기 신규발행 인증서파일에 기초하여 암호화-키를 획득하고 이어서 전술한 바와 같은 디지털 콘텐츠 파일에 대한 암호화 처리를 수행한다. 인증서파일, 인증요청서 파일, 신규발행 인증서파일의 필드포맷에 대해서는 도 5를 참조하여 후술한다.

도 5는 본 발명에 따른 콘텐츠 보안처리 시스템에서 사용가능한 인증서파일 및 내장인증서의 실시예를 도시하는 도면이다.

도 5에서 (a)와 (b)와 (c)는 플래시디스크(230)에 저장되는 각종 데이터의 필드포맷을 도시하며, (d)와 (e)는 호스트 플레이어(210)의 보안메모리(215) 내에 저장되는 내장인증서의 필드포맷을 도시한 것이다. 보다 상세히 설명하면, 상기 각종의 필드포맷[(a), (b), (c)]은 각각 호스트 플레이어가 기록하는 인증서파일의 필드포맷[(a)], 인증요청서 파일의 필드포맷[(b)], 그리고 관리자 프로그램(250)이 신규로 발행하여 전달하는 인증서파일의 필드포맷[(c)]를 나타낸다. 도시된 필드포맷은 바람직한 실시예에 불과한 것으로, 본 기술분야의 당업자는 본 발명의 범위 내에서 용이하게 이들 필드포맷을 변경할 수 있다.

도시된 각종 데이터의 필드포맷 (a)~(e)에서 "버전(version)" 필드는 호스트 플레이어(210)와 관리자 프로그램(250) 간의 버전 호환성을 맞추기 위해 사용되는 정보로서, 호스트 플레이어(210)가 인증서파일과 인증요청서 파일을 기록할 때 자신의 버전 값을 기록함으로써 이에 호환성을 갖도록 관리자 프로그램(250)이 암호화-키를 생성하거나 혹은 신규의 인증서파일을 발행할 수 있도록 한다. 또한, "상태코드(status code)" 필드는 이들 인증서파일, 인증요청서 파일, 신규 인증서파일이 정상상태인지 여부를 나타내는 정보이다. 또한, "모델명" 필드는 이들 인증서파일, 인증요청서 파일, 신규 인증서파일이 사용되는 호스트 플레이어(210)의 모델 번호를 나타내는 정보이다.

또한, "플레이어 식별자" 필드는 해당 호스트 플레이어(210)를 식별하기 위한 유일한 식별자일 수도 있고 혹은 일정한 호스트 플레이어 그룹을 식별하기 위한 정보일 수도 있다. 또한, "키 값" 필드는 플래시디스크(230)를 통하여 전달되는 디지털 콘텐츠 파일의 데이터를 암호화/복호화 하는 데에 사용될 수 있는 것으로서, 인증서파일 및 신규인증서 파일에는 이처럼 키 값이 표시되어 있으므로 바람직하게는 특정의 보안 알고리즘에 의하여 스크램블된다. 또한, "체커" 필드는 도시된 각종의 데이터에 대하여 무결성을 검사하기 위한 것으로서, 예를 들어 CRC 코드 또는 Even/Odd 비트일 수 있다.

또한, "난수" 필드는 랜덤하게 발생한 값을 기록하는 필드로서, 호스트 플레이어(210)는 인증서파일의 신규발행을 요청할 때 난수를 생성하여 인증요청서 파일에 삽입하고, 이후에 접속된 플래시디스크(230) 내에 필드포맷 (c)의 신규 인증서파일을 발견하였을 때 상기 신규 인증서파일이 자신이 요청한 인증서파일에 해당하는지 여부, 즉 매칭성을 판단한다. 이를 위해, 호스트 플레이어(210)는 인증요청서 파일을 플래시디스크(230) 내에 기록한 후에는 상기 인증요청서 파일에 삽입한 난수를 필드포맷 (e)의 형태로 비휘발성 메모리 공간, 예컨대 보안메모리(215) 내에 저장해 둔다.

본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터로 판독가능한 정보기록매체를 포함할 수 있다. 상기 컴퓨터로 판독가능한 정보기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 정보기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 혹은 컴퓨터 소프트웨어 당업자에게 공지되어 사용가능한 것일 수도 있다. 컴퓨터로 판독가능한 정보기록매체의 예에는 하드디스크, 플로피디스크, CD-ROM, DVD-ROM, 및 플래시메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 정보기록매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어 지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급언어 코드를 포함한다.

발명의 효과

본 발명의 호스트 플레이어의 콘텐츠 보안처리 시스템에 따르면 플래시메모리를 내장하지 않는 형태의 디지털 오디오 재생장치인 호스트 플레이어를 사용함에 있어서 표준 UMS 규격의 플래시디스크 상에 저장된 디지털 콘텐츠 파일의 불법복제를 효과적으로 방지함으로써 디지털 콘텐츠 파일에 일체된 저작권을 보호할 수 있다는 장점이 있다.

또한, 본 발명의 호스트 플레이어의 콘텐츠 보안처리 시스템에 따르면 인증데이터의 버전관리와 무결성 검사를 수행함으로써 보안장치가 해킹되더라도 조속하게 이에 대응하는 새로운 버전의 인증데이터를 유포시킴으로써 상기 해킹의 피해확산을 방지할 수 있다는 장점이 있다.

(57) 청구의 범위

청구항 1.

(1) 내장인증서를 저장하기 위한 보안메모리; 외장장치와 결합되기 위한 디지털 접속부; 상기 보안메모리 내에 유효한 내장인증서가 존재하는지 여부를 검사하여 ① 존재한다면 상기 내장인증서에 기초하여 인증서파일 - 제1 인증서파일 -을 생성하여 상기 외장장치 내에 기록하고 ② 존재하지 않는다면 상기 외장장치 내에 특정 포맷의 인증요청서 파일을 기록하며 ③ 상기 내장인증서에 기초하여 복호화-키를 획득하기 위한 보안모듈; 상기 외장장치로부터 판독한 디지털 콘텐츠 파일의 데이터를 재생하기 위한 디코딩모듈; 및 상기 디지털 콘텐츠 파일이 암호화된 경우 상기 복호화-키를 이용하여 상기 디지털 콘텐츠 파일의 데이터를 복호화 처리하기 위한 복호화모듈을 구비하는 호스트 플레이어; 및

(2) 디지털 접속을 통해 외장장치가 접속되는 것을 자동검출하기 위한 UMS 자동검출모듈; 상기 외장장치 내에 유효한 인증서파일 - 제3 인증서파일 -이 존재하는지 여부를 검사하여 ① 존재한다면 상기 제3 인증서파일에 기초하여 암호화 키를 획득하고 ② 존재하지 않는다면 상기 외장장치에 저장된 특정 포맷의 인증요청서 파일에 기초하여 인증서파일 - 제4 인증서파일 -을 생성하여 상기 외장장치 내에 기록하고 상기 제4 인증서파일에 기초하여 암호화-키를 획득하는 인증데이터 관리모듈; 및 상기 암호화 키를 사용하여 상기 디지털 콘텐츠 파일의 데이터를 암호화 처리하기 위한 암호화모듈을 구비하는 관리자 프로그램

을 포함하여 구성되는 것을 특징으로 하는 콘텐츠 보안처리 시스템.

청구항 2.

제1항에 있어서, 상기 호스트 플레이어의 상기 보안모듈은 상기 보안메모리 내에 유효한 내장인증서가 존재하지 않는 경우에는 상기 외장장치 내에 상기 호스트 플레이어와 매칭되고 유효한 인증서파일 - 제2 인증서파일 -이 존재하는지 여부를 검사하여 ① 존재한다면 상기 제2 인증서파일에 기초하여 상기 내장인증서를 생성하여 저장하고 ② 존재하지 않는다면 상기 외장장치 내에 상기 특정 포맷의 인증요청서 파일을 기록하는 것을 특징으로 하는 콘텐츠 보안처리 시스템.

청구항 3.

제1항에 있어서, 상기 관리자 프로그램의 상기 인증데이터 관리모듈은 상기 외장장치 내에 상기 제3 인증서파일이 존재하지 않는 경우에는 상기 외장장치 내에 상기 특정 포맷의 인증요청서 파일이 존재하는지 여부를 검사하여 ① 존재한다면 상기 인증요청서 파일에 기초하여 상기 제4 인증서파일을 생성하여 상기 외장장치에 기록하고 ② 존재하지 않는다면 에러를 표시하고 보안처리 동작을 중단하는 것을 특징으로 하는 콘텐츠 보안처리 시스템.

청구항 4.

호스트 플레이어가 유효한 내장인증서를 보유하는지 여부를 검사하는 단계; 상기 호스트 플레이어의 검사결과, 보유하는 경우에는 상기 내장인증서에 기초하여 인증서파일 - 제1 인증서파일 -을 생성하여 외장장치 내에 기록하는 단계; 상기 호스트 플레이어의 검사결과, 보유하지 않는 경우에는 상기 외장장치 내에 특정 포맷의 인증요청서 파일을 기록하는 단계; 호스트 플레이어가 상기 내장인증서에 기초하여 복호화-키를 획득하는 단계; 상기 외장장치로부터 디지털 콘텐츠 파일을 판독하여, 암호화 처리된 경우에는 상기 복호화-키를 사용하여 상기 디지털 콘텐츠 파일의 데이터를 복호화 처리하는 단계; 관리자 프로그램이 외장장치 내에 유효한 인증서파일 - 제3 인증서파일 -이 존재하는지 여부를 검사하는 단계; 상기 관리자 프로그램의 검사결과, 존재하는 경우에는 상기 제3 인증서파일에 기초하여 암호화-키를 획득하는 단계; 상기 관리자 프로그램의 검사결과, 존재하지 않는 경우에는 상기 외장장치에 저장된 특정 포맷의 인증요청서 파일에 기초하여 인증서파일 - 제4 인증서파일 -을 생성하여 상기 외장장치 내에 기록하고 상기 제4 인증서파일에 기초하여 암호화-키를 획득하는 단계; 및 관리자 프로그램이 상기 암호화 키를 사용하여 콘텐츠 파일을 암호화 처리하여 상기 외장장치로 복사하는 단계를 포함하여 구성되는 것을 특징으로 하는 콘텐츠 보안처리 방법.

청구항 5.

제4항에 있어서, 상기 호스트 플레이어는 내부의 보안메모리에 상기 내장인증서가 존재하는지 여부를 검사하고 그 결과 존재하는 경우에는 상기 내장인증서 내의 특정 체커필드에 대해서 무결성 검사를 수행함으로써 상기 호스트 플레이어가 유효한 내장인증서를 보유하는지 여부를 검사하는 것을 특징으로 하는 콘텐츠 보안처리 방법.

청구항 6.

제4항에 있어서, 상기 관리자 프로그램은 상기 외장장치 내에 인증서파일이 존재하는지 여부를 검사하고 그 결과 존재하는 경우에는 상기 인증서파일 내의 특정 체커필드에 대해서 무결성 검사를 수행함으로써 상기 외장장치 내에 유효한 제3 인증서파일이 존재하는지 여부를 검사하는 것을 특징으로 하는 콘텐츠 보안처리 방법.

청구항 7.

제4항에 있어서, 상기 호스트 플레이어는 상기 유효한 내장인증서를 보유하지 않는 경우에는 상기 외장장치 내에 상기 호스트 플레이어와 매칭되고 유효한 인증서파일 - 제2 인증서파일 -이 존재하는지 여부를 검사하여 ① 존재한다면 상기 제2 인증서파일에 기초하여 상기 내장인증서를 생성하여 저장하고 ② 존재하지 않는다면 상기 외장장치 내에 상기 특정 포맷의 인증요청서 파일을 기록하는 것을 특징으로 하는 콘텐츠 보안처리 방법.

청구항 8.

제7항에 있어서, 상기 호스트 플레이어는 상기 외장장치 내에 인증서파일이 존재하는 경우에 ① 상기 인증서파일 내의 특정 난수 필드와 상기 호스트 플레이어가 상기 인증요청서 파일에 기록한 특정 난수 필드를 비교함으로써 상기 인증서파일이 매칭되는지 여부를 판단하고 ② 상기 인증서파일 내의 특정 체커필드에 대해서 무결성 검사를 수행함으로써 상기 인증서파일이 유효한지 여부를 판단하는 것을 특징으로 하는 콘텐츠 보안처리 방법.

청구항 9.

제4항에 있어서, 상기 호스트 플레이어는 상기 디지털 콘텐츠 파일 내의 특정 헤더포맷을 파싱함으로써 상기 디지털 콘텐츠 파일이 암호화 처리된 파일인지 여부를 판단하는 것을 특징으로 하는 콘텐츠 보안처리 방법.

청구항 10.

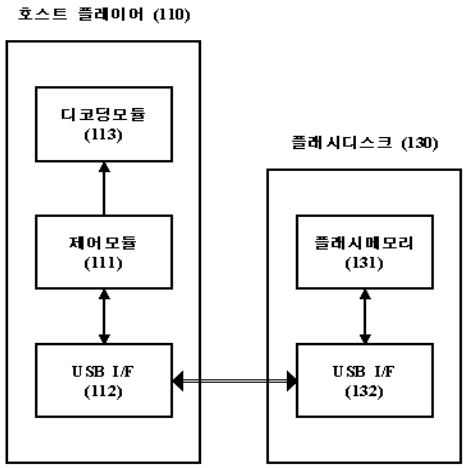
제4항에 있어서, 상기 관리자 프로그램은 상기 외장장치 내에 상기 제3 인증서파일이 존재하지 않는 경우에는 상기 외장장치 내에 상기 특정 포맷의 인증요청서 파일이 존재하는지 여부를 검사하여 ① 존재한다면 상기 인증요청서 파일에 기초하여 상기 제4 인증서파일을 생성하여 상기 외장장치에 기록하고 ② 존재하지 않는다면 에러를 표시하고 보안처리 동작을 중단하는 것을 특징으로 하는 콘텐츠 보안처리 시스템.

청구항 11.

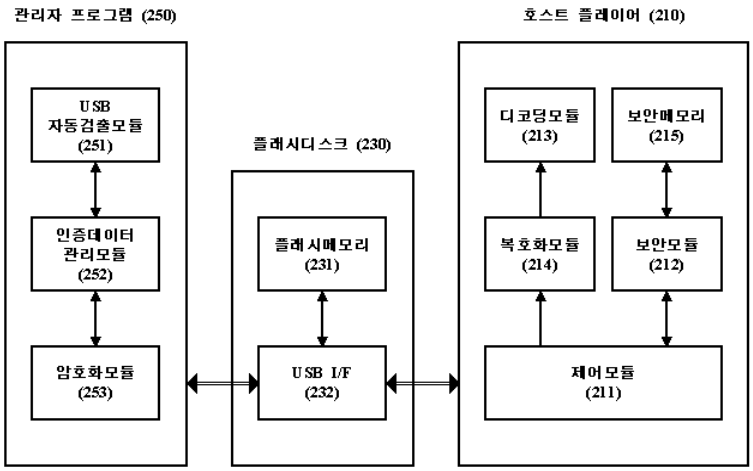
제4항 내지 제10항 중 어느 하나의 항에 따른 콘텐츠 보안처리 방법을 실행하기 위한 프로그램이 기록되어 있는 컴퓨터로 판독가능한 정보기록매체.

도면

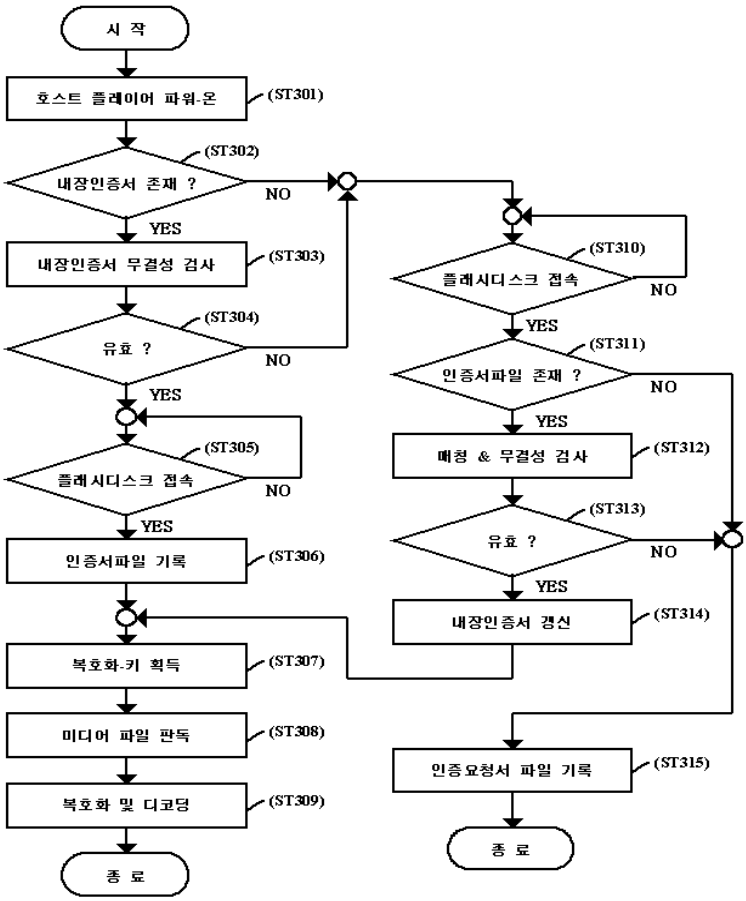
도면1



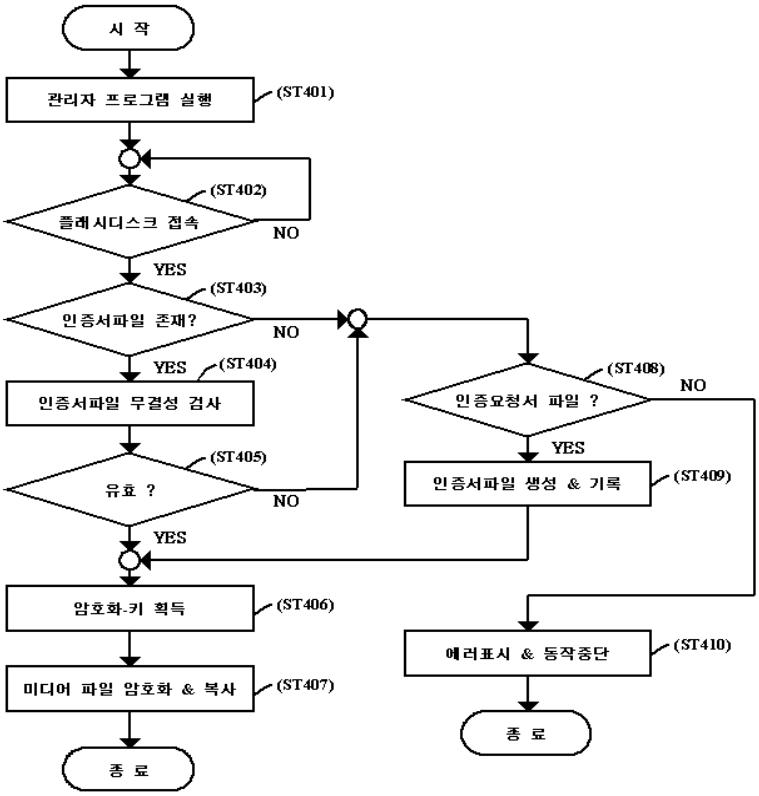
도면2


관리자 프로그램 (250)
USB
자동검출모듈
(251)
인증데이터
관리모듈
(252)
암호화모듈
(253)
플레시디스크 (230)
플레시메모리
(231)
USB I/F
(232)
호스트 플레이어 (210)
디코딩모듈
(213)
보안메모리
(215)
복호화모듈
(214)
보안모듈
(212)
제어모듈
(211)

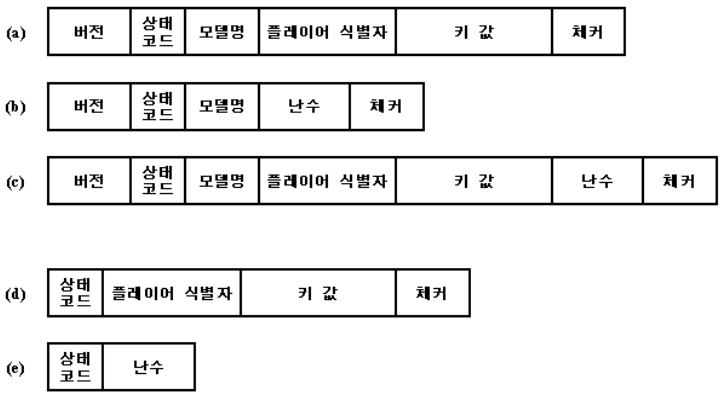
도면3


시 작
호스트 플레이어 파워-온
(ST301)
내장인증서 존재 ?
(ST302)
NO
YES
내장인증서 무결성 검사
(ST303)
유효 ?
(ST304)
NO
YES
플레시디스크 접속
(ST305)
NO
YES
인증서파일 기록
(ST306)
복호화-키 획득
(ST307)
미디어 파일 판독
(ST308)
복호화 및 디코딩
(ST309)
종 료
플레시디스크 접속
(ST310)
NO
YES
인증서파일 존재 ?
(ST311)
NO
YES
매칭 & 무결성 검사
(ST312)
유효 ?
(ST313)
NO
YES
내장인증서 갱신
(ST314)
인증요청서 파일 기록
(ST315)
종 료

도면4


시 작
관리자 프로그램 실행
(ST401)
(ST402)
플레시디스크 접속
NO
YES
(ST403)
인증서파일 존재?
NO
YES
(ST404)
인증서파일 무결성 검사
(ST405)
유효 ?
NO
YES
(ST408)
인증요청서 파일 ?
NO
YES
인증서파일 생성 & 기록
(ST409)
암호화-키 획득
(ST406)
미디어 파일 암호화 & 복사
(ST407)
종 료
에러표시 & 동작중단
(ST410)
종 료

도면5


(a)
버전
상태 코드
모델명
플레이어 식별자
키 값
체커
(b)
버전
상태 코드
모델명
난수
체커
(c)
버전
상태 코드
모델명
플레이어 식별자
키 값
난수
체커
(d)
상태 코드
플레이어 식별자
키 값
체커
(e)
상태 코드
난수