(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월12일
(11) 등록번호 10-1428958
(24) 등록일자 2014년08월04일

(51) 국제특허분류(Int. Cl.)
G06F 21/10 (2013.01) *G06F 21/30* (2013.01)
(21) 출원번호 10-2013-7022371(분할)
(22) 출원일자(국제) 2006년10월02일
심사청구일자 2013년08월23일
(85) 번역문제출일자 2013년08월23일
(65) 공개번호 10-2013-0103810
(43) 공개일자 2013년09월24일
(62) 원출원 특허 10-2008-7010636
원출원일자(국제) 2006년10월02일
심사청구일자 2011년09월30일
(86) 국제출원번호 PCT/US2006/038596
(87) 국제공개번호 WO 2007/041567
국제공개일자 2007년04월12일
(30) 우선권주장
11/242,223 2005년10월03일 미국(US)
(56) 선행기술조사문헌
US20050010531 A1
US20050203959 A1
전체 청구항 수 : 총 35 항

(73) 특허권자
인텔 코포레이션
미국 캘리포니아주 95054 산타클라라 미션 칼리지 불바드 2200
(72) 발명자
허그, 조슈아, 디.
미국, 워싱턴 98119, 시애틀, 530 더블유. 올림픽 #301
(74) 대리인
제일특허법인

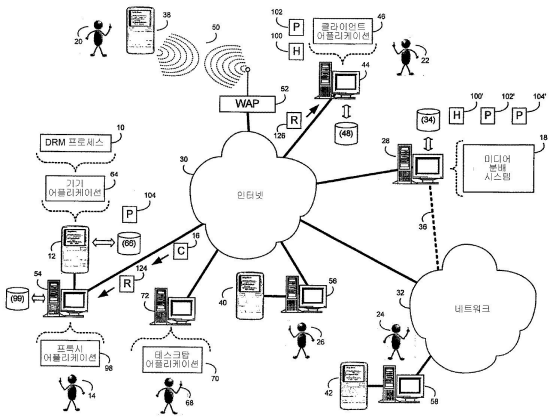
심사관 : 문남두

(54) 발명의 명칭 **미디어 콘텐츠를 획득하여 공유하기 위한 시스템 및 방법**

(57) 요 약

기기 초기화 방법은 개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계를 포함한다. 타임아웃 표시기는 상기 개인용 미디어 기기와 연관된 가입에 대해 획득될 수 있다. 상기 라이센스 요청 및 상기 타임아웃 표시기는 상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 결합될 수 있다. 상기 기기 라이센스는 서명된 기기 라이센스를 형성하기 위해 디지털적으로 서명될 수 있다.

대 표 도



특허청구의 범위

청구항 1

개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계;

상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 획득하는 단계;

상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계;

서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및

상기 서명된 기기 라이센스의 무결성을 검증하는 단계를 포함하되,

상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것인 개인용 미디어 기기 초기화 방법.

청구항 2

제 1 항에 있어서,

미디어 분배 시스템에 상기 라이센스 요청을 제공하는 단계; 및

상기 개인용 미디어 기기에 상기 기기 라이센스를 제공하는 단계를 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 3

제 1 항에 있어서, 상기 라이센스 요청은 상기 가입을 식별하는 사용자 ID; 챌린지; 및 상기 개인용 미디어 기기에 대한 기기 디지털 인증서 중 적어도 하나를 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 4

제 1 항에 있어서, 서명된 라이센스 요청을 형성하기 위해 상기 라이센스 요청에 디지털적으로 서명하는 단계를 더 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 5

제 4 항에 있어서, 상기 서명된 라이센스 요청의 무결성(integrity)을 검증하는 단계를 더 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 6

제 1 항에 있어서, 상기 기기 라이센스는 라이센싱 서비스 디지털 인증서; 시스템 타임 표시기; 및 사용자 암호화 키 중 적어도 하나를 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 7

개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계;

상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 판단하는 단계;

상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계;

서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및

상기 서명된 기기 라이센스의 무결성을 검증하는 단계를 포함하는 동작들을 수행하는 프로그램을 기록하되,

상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것인, 컴퓨터로 읽을 수 있는 기록 매체.

청구항 8

개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계;

상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 획득하는 단계;

상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계;

서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및

서명된 라이센스 요청을 형성하기 위해 상기 라이센스 요청에 디지털적으로 서명하는 단계를 포함하되,

상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것인 개인용 미디어 기기 초기화 방법.

청구항 9

제 8 항에 있어서,

미디어 분배 시스템에 상기 라이센스 요청을 제공하는 단계; 및

상기 개인용 미디어 기기에 상기 기기 라이센스를 제공하는 단계를 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 10

제 8 항에 있어서,

상기 라이센스 요청은 상기 가입을 식별하는 사용자 ID; 챌린지; 및 상기 개인용 미디어 기기에 대한 기기 디지털 인증서 중 적어도 하나를 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 11

제 8 항에 있어서,

상기 서명된 라이센스 요청의 무결성(integrity)을 검증하는 단계를 더 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 12

제 8 항에 있어서,

상기 기기 라이센스는 라이센싱 서비스 디지털 인증서; 시스템 타임 표시기; 및 사용자 암호화 키 중 적어도 하나를 포함하는, 개인용 미디어 기기 초기화 방법.

청구항 13

개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계;

상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 판단하는 단계;

상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계;

서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및

서명된 라이센스 요청을 형성하기 위해 상기 라이센스 요청에 디지털적으로 서명하는 단계를 포함하는 동작들을 수행하는 프로그램을 기록하되,

상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것인, 컴퓨터로 읽을 수 있는 기록 매체.

청구항 14

라이센싱 서비스에 의해 디지털적으로 서명되어 있는, 타겟 기기로부터 타겟 기기 라이센스를 수신하는 단계;

상기 타겟 기기 라이센스의 무결성을 검증하는 단계;

상기 타겟 기기로부터 타겟 기기 디지털 인증서를 수신하는 단계;

상기 타겟 기기 디지털 인증서의 무결성을 검증하는 단계;

소스 기기와 상기 타겟 기기 간 보안 통신 채널을 수립하는 단계; 및

상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 적어도 하나의 미디어 데이터 파일을 전송하는 단계를 포함하되,

상기 타겟 기기 라이센스는, 상기 타겟 기기에 고유한 것이고, 암호화된 상기 미디어 데이터 파일에 대한, 소스 기기 라이센스와 상이한 것인 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 15

제 14 항에 있어서,

상기 타겟 기기와 연관된 가입에 대한 타임아웃 표시기를, 상기 타겟 기기 라이센스로부터, 획득하는 단계를 더 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 16

제 15 항에 있어서,

상기 가입이 현재 유효한지를 판단하기 위해 시스템 클록과 상기 타임아웃 표시기를 비교하는 단계; 및

상기 가입이 현재 유효하지 않다고 판단되는 경우 적어도 하나의 미디어 데이터 파일의 전송을 금지하는 단계를 더 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 17

제 14 항에 있어서,

상기 소스 기기로부터 소스 디지털 인증서를 수신하는 단계; 및

상기 소스 기기 디지털 인증서의 무결성을 검증하는 단계를 더 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 18

제 14 항에 있어서,

상기 타겟 기기 라이센스는,

상기 타겟 기기와 연관된 가입을 확인하는 사용자 ID; 챌린지; 타겟 기기 디지털 인증서; 라이센싱 서비스 디지털 인증서; 시스템 타임 표시기; 사용자 암호화 키; 및 상기 가입에 대한 타임아웃 표시기 중 적어도 하나를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 19

제 18 항에 있어서,

적어도 하나의 미디어 데이터 파일을 전송하는 단계는,

적어도 하나의 바인딩 해제된 미디어 데이터 파일을 생성하기 위해 상기 소스 기기의 사용자로부터 상기 적어도 하나의 미디어 데이터 파일을 바인딩 해제하는 단계;

상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일을 전송하는 단계; 및

상기 사용자 암호화 키를 사용하여 상기 타겟 기기의 사용자에 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일을 바인딩하는 단계를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 20

제 19 항에 있어서,

상기 타겟 기기의 사용자에 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일을 바인딩하는 단계는,

상기 사용자 암호화 키를 사용하여 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일에 대한 콘텐츠 암호화 키를 암호화하는 단계를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 21

제 14 항에 있어서,

상기 보안 통신 채널은 무선 통신 채널인, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 22

제 14 항에 있어서,

상기 보안 통신 채널은 유선 통신 채널인, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 23

제 14 항에 있어서,

보안 통신 채널을 수립하는 단계는,

제1 소스 기기 및 상기 타겟 기기상에 랜덤 세션 키를 생성하는 단계; 및

다른 소스 기기 및 상기 타겟 기기에 상기 랜덤 세션 키를 제공하는 단계를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 24

라이센싱 서비스에 의해 디지털적으로 서명되어 있는, 타겟 기기로부터 타겟 기기 라이센스를 수신하는 단계;

상기 타겟 기기 라이센스의 무결성을 검증하는 단계;

소스 기기로부터 소스 디지털 인증서를 수신하는 단계;

상기 소스 기기 디지털 인증서의 무결성을 검증하는 단계;

상기 소스 기기와 상기 타겟 기기 간 보안 통신 채널을 수립하는 단계; 및

상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 적어도 하나의 미디어 데이터 파일을 전송하는 단계를 포함하되,

상기 타겟 기기 라이센스는, 상기 타겟 기기에 고유한 것이고, 암호화된 상기 미디어 데이터 파일에 대한, 소스 기기 라이센스와 상이한 것인 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 25

제 24 항에 있어서,

상기 타겟 기기와 연관된 가입에 대한 타임아웃 표시기를, 상기 타겟 기기 라이센스로부터, 획득하는 단계를 더 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 26

제 25 항에 있어서,

상기 가입이 현재 유효한지를 판단하기 위해 시스템 클록과 상기 타임아웃 표시기를 비교하는 단계; 및

상기 가입이 현재 유효하지 않다고 판단되는 경우 적어도 하나의 미디어 데이터 파일의 전송을 금지하는 단계를 더 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 27

제 24 항에 있어서,

상기 타겟 기기로부터 타겟 기기 디지털 인증서를 수신하는 단계; 및

상기 타겟 기기 디지털 인증서의 무결성을 검증하는 단계를 더 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 28

제 24 항에 있어서,

상기 타겟 기기 라이센스는,

상기 타겟 기기와 연관된 가입을 확인하는 사용자 ID; 챌린지; 타겟 기기 디지털 인증서; 라이센싱 서비스 디지털 인증서; 시스템 타임 표시기; 사용자 암호화 키; 및 상기 가입에 대한 타임아웃 표시기 중 적어도 하나를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 29

제 28 항에 있어서,

적어도 하나의 미디어 데이터 파일을 전송하는 단계는,

적어도 하나의 바인딩 해제된 미디어 데이터 파일을 생성하기 위해 상기 소스 기기의 사용자로부터 상기 적어도 하나의 미디어 데이터 파일을 바인딩 해제하는 단계;

상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일을 전송하는 단계; 및

상기 사용자 암호화 키를 사용하여 상기 타겟 기기의 사용자에 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일을 바인딩하는 단계를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 30

제 29 항에 있어서,

상기 타겟 기기의 사용자에 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일을 바인딩하는 단계는,

상기 사용자 암호화 키를 사용하여 상기 적어도 하나의 바인딩 해제된 미디어 데이터 파일에 대한 콘텐츠 암호화 키를 암호화하는 단계를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 31

제 24 항에 있어서,

상기 보안 통신 채널은 무선 통신 채널인, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 32

제 24 항에 있어서,

상기 보안 통신 채널을 유선 통신 채널인, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 33

제 24 항에 있어서,

보안 통신 채널을 수립하는 단계는,

제1 소스 기기 및 상기 타겟 기기상에 랜덤 세션 키를 생성하는 단계; 및

다른 소스 기기 및 상기 타겟 기기에 상기 랜덤 세션 키를 제공하는 단계를 포함하는, 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법.

청구항 34

라이센싱 서비스에 의해 디지털적으로 서명되어 있는, 타겟 기기로부터 타겟 기기 라이센스를 수신하는 단계;

상기 타겟 기기 라이센스의 무결성을 검증하는 단계;

상기 타겟 기기로부터 타겟 기기 디지털 인증서를 수신하는 단계;

상기 타겟 기기 디지털 인증서의 무결성을 검증하는 단계;

소스 기기와 상기 타겟 기기 간 보안 통신 채널을 수립하는 단계; 및

상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 적어도 하나의 미디어 데이터 파일을 전송하는 단계를 포함하는 동작들을 수행하는 프로그램을 기록하되,

상기 타겟 기기 라이센스는, 상기 타겟 기기에 고유한 것이고, 암호화된 상기 미디어 데이터 파일에 대한, 소스 기기 라이센스와 상이한 것인, 컴퓨터로 읽을 수 있는 기록 매체.

청구항 35

라이센싱 서비스에 의해 디지털적으로 서명되어 있는, 타겟 기기로부터 타겟 기기 라이센스를 수신하는 단계;

상기 타겟 기기 라이센스의 무결성을 검증하는 단계;

소스 기기로부터 소스 디지털 인증서를 수신하는 단계;

상기 소스 기기 디지털 인증서의 무결성을 검증하는 단계;

상기 소스 기기와 상기 타겟 기기 간 보안 통신 채널을 수립하는 단계; 및

상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 적어도 하나의 미디어 데이터 파일을 전송하는 단계를 포함하는 동작들을 수행하는 프로그램을 기록하되,

상기 타겟 기기 라이센스는, 상기 타겟 기기에 고유한 것이고, 암호화된 상기 미디어 데이터 파일에 대한, 소스 기기 라이센스와 상이한 것인, 컴퓨터로 읽을 수 있는 기록 매체.

명 세 서

기 술 분 야

[0001] 이 출원서는 아래 출원서들의 우선권을 주장하는 것으로서, 본원에 참조로서 병합된다: SYSTEM AND METHOD FOR OBTAINING AND SHARING MEDIA CONTENT로 명칭된, 2005년 10월 3일에 출원된, 미국일련번호 제11/242,223호; DIGITAL RIGHTS MANAGEMENT FOR CONTENT RENDERING ON PLAYBACK DEVICES로 명칭된, 2003년 11월 21일에 출원된, 미국일련번호 제10/719,981호.

[0002] 본 발명은 미디어 콘텐츠를 공유하는 것에 관한 것이며, 보다 자세하게는, 다수의 개인용 미디어 기기들 간에 콘텐츠를 공유하는 것에 관한 것이다.

배 경 기 술

[0003] 미디어 분배 시스템(예를 들면, 워싱턴주, 시애틀의 리얼네트웍스™에 의해 제공된 랩소디™ 및 랩소디-투-고우™ 서비스들)은 미디어 서버로부터 클라이언트 전자 기기(예, MP3 플레이어)로 미디어 콘텐츠를 분배한다. 미디어 분배 시스템은 사용자가 미디어 데이터 파일들을 다운로드 하도록 하고/하거나 수신하도록 하여 미디어 데이터 스트림들을 프로세스 하도록 함으로써 미디어 콘텐츠를 분배할 수 있다.

[0004] 미디어 데이터 파일들은 종래에는 사용자의 클라이언트 전자 기기로 다운로드 되며, 다운로드 된 각 미디어 데이터 파일은 상기 사용자의 클라이언트 전자 기기에 대한 독점적인 사용이 허용되며, (상기 다운로드 된 미디어 데이터 파일과 관련된) 상기 사용권은 상기 미디어 데이터 파일이 다운로드 됨과 동시에 상기 클라이언트 기기로 넘겨진다.

[0005] 종종, 제1 클라이언트 전자기기의 사용자는 제1 클라이언트 전자 기기의 사용자와 미디어 데이터 파일(예, 노래)을 공유하기를 원할 수 있다. 불행하게도, 상기 미디어 데이터 파일들은 특정 클라이언트 전자 기기에 대

한 독점적 사용이 허용되며, 상기 미디어 데이터 파일은 상기 제1 클라이언트 전자 기기에서 상기 제2 클라이언트 전자 기기로 직접 전송되지 않을 수도 있다. 따라서, 상기 제2 클라이언트 전자 기기의 사용은 일반적으로 상기 미디어 분배 시스템으로부터 상기 미디어 데이터 파일을 획득하는 것이 요구될 것이다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 과제는 다수의 개인용 미디어 기기들 간에 콘텐츠를 공유하는 개인용 미디어 기기 초기화 방법을 제공하는 것이다.

[0007] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해 될 수 있을 것이다.

과제의 해결 수단

[0008] 상기 기술적 과제를 달성하기 위한 본 발명의 제1 실시예에 따른 개인용 미디어 기기 초기화 방법은, 개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계; 상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 획득하는 단계; 상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계; 서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및 상기 서명된 기기 라이센스의 무결성을 검증하는 단계를 포함하되, 상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것일 수 있다.

[0009] 상기 기술적 과제를 달성하기 위한 본 발명의 제2 실시예에 따른 컴퓨터 프로그램 제품은, 저장된 다수의 인스트럭션들을 가지는 컴퓨터 판독가능한 매체 상에 존재하는 컴퓨터 프로그램 제품에 있어서, 프로세서에 의해 수행될 때, 상기 프로세서가, 개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계; 상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 판단하는 단계; 상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계; 서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및 상기 서명된 기기 라이센스의 무결성을 검증하는 단계를 포함하는 동작들을 수행하되, 상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것일 수 있다.

[0010] 상기 기술적 과제를 달성하기 위한 본 발명의 제3 실시예에 따른 개인용 미디어 기기초기화 방법은, 개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계; 상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 획득하는 단계; 상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계; 서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및 서명된 라이센스 요청을 형성하기 위해 상기 라이센스 요청에 디지털적으로 서명하는 단계를 포함하되, 상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것일 수 있다.

[0011] 상기 기술적 과제를 달성하기 위한 본 발명의 제4 실시예에 따른 컴퓨터 프로그램 제품은, 저장된 다수의 인스트럭션들을 가지는 컴퓨터 판독가능한 매체 상에 존재하는 컴퓨터 프로그램 제품에 있어서, 프로세서에 의해 수행될 때, 상기 프로세서가, 개인용 미디어 기기에 대한 라이센스 요청을 생성하는 단계; 상기 개인용 미디어 기기와 연관된 가입에 대한 타임아웃 표시기를 판단하는 단계; 상기 개인용 미디어 기기에 대한 기기 라이센스를 형성하기 위해 상기 라이센스 요청과 상기 타임아웃 표시기를 결합하는 단계; 서명된 기기 라이센스를 형성하기 위해 상기 기기 라이센스에 디지털적으로 서명하는 단계; 및 서명된 라이센스 요청을 형성하기 위해 상기 라이센스 요청에 디지털적으로 서명하는 단계를 포함하는 동작들을 수행하되, 상기 개인용 미디어 기기에 대한 상기 기기 라이센스는, 상기 개인용 미디어 기기에 고유(unique)한 것일 수 있다.

[0012] 상기 기술적 과제를 달성하기 위한 본 발명의 제5 실시예에 따른 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법은, 라이센싱 서비스에 의해 디지털적으로 서명되어 있는, 타겟 기기로부터 타겟 기기 라이센스를 수신하는 단계; 상기 타겟 기기 라이센스의 무결성을 검증하는 단계; 상기 타겟 기기로부터 타겟 기기 디지털 인증서를 수신하는 단계; 상기 타겟 기기 디지털 인증서의 무결성을 검증하는 단계; 소스 기기와 상기 타겟 기기 간 보안 통신 채널을 수립하는 단계; 및 상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 적어도 하나의 미디어 데이터 파일을 전송하는 단계를 포함하되, 상기 타겟 기기 라이센스는, 상기 타겟 기기에 고유한

것이고, 암호화된 상기 미디어 데이터 파일에 대한, 소스 기기 라이센스와 상이한 것일 수 있다.

[0013] 상기 기술적 과제를 달성하기 위한 본 발명의 제6 실시예에 따른 소스 기기에서 타겟 기기로 콘텐츠를 전송하는 방법은, 라이센싱 서비스에 의해 디지털적으로 서명되어 있는, 타겟 기기로부터 타겟 기기 라이센스를 수신하는 단계; 상기 타겟 기기 라이센스의 무결성을 검증하는 단계; 상기 소스 기기로부터 소스 디지털 인증서를 수신하는 단계; 상기 소스 기기 디지털 인증서의 무결성을 검증하는 단계; 소스 기기와 상기 타겟 기기 간 보안 통신 채널을 수립하는 단계; 및 상기 보안 통신 채널을 사용하여 상기 소스 기기에서 상기 타겟 기기로 적어도 하나의 미디어 데이터 파일을 전송하는 단계를 포함하되, 상기 타겟 기기 라이센스는, 상기 타겟 기기에 고유한 것이고, 암호화된 상기 미디어 데이터 파일에 대한, 소스 기기 라이센스와 상이한 것일 수 있다.

발명의 효과

[0014] 본 발명은 다수의 개인용 미디어 기기들 간에 콘텐츠를 공유하는 개인용 미디어 기기 초기화 방법을 제공할 수 있다.

[0015] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0016] 도 1은 DRM 프로세스, 미디어 분배 시스템, 클라이언트 어플리케이션, 프록시 어플리케이션, 기기 어플리케이션, 및 분배형 컴퓨팅 네트워크에 커플된 개인용 미디어 기기의 개략도.

도 2는 도 1의 개인용 미디어 기기의 등각투상도.

도 3은 도 1의 개인용 미디어 기기의 개략도.

도 4는 도 1의 클라이언트 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 5는 도 1의 클라이언트 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 6은 도 1의 클라이언트 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 7은 도 1의 클라이언트 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 8은 도 1의 클라이언트 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 9는 도 1의 프록시 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 10은 도 1의 프록시 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 11은 도 1의 프로시 어플리케이션에 의해 렌더링된 디스플레이 스크린.

도 12a는 도 1의 미디어 분배 시스템, 개인용 미디어 기기, 분배형 컴퓨팅 네트워크의 개략도.

도 12b는 도 1의 DRM 프로세스에 의해 수행된 프로세스의 흐름도.

도 13a는 도 1의 미디어 분배 시스템, 개인용 미디어 기기, 분배형 컴퓨팅 네트워크의 개략도.

도 13b는 도 1의 DRM 프로세서에 의해 수행된 프로세스의 흐름도.

도 14a는 보안 통신 채널을 통해 서로 커플된 두 개의 개인용 미디어 기기들의 개략도.

도 14b는 도 1의 DRM 프로세스에 의해 수행된 프로세스의 흐름도.

도 15는 비대칭 키 블록의 개략도.

발명을 실시하기 위한 구체적인 내용

[0017] **시스템 개요:**

[0018] 도 1을 참조하면, 개인용 미디어 기기(12)에 존재하여 수행될 수 있는 DRM(이를 테면, 디지털 저작권 관리(digital rights management)) 프로세스(10)가 도시된다. 하기에 논의될 것처럼, DRM 프로세스(10)는 개인용 미디어 기기(12)의 사용자(예, 사용자(14))가 개인용 미디어 기기(12)에 존재하는 미디어 콘텐츠(16)를 관리하도록 한다. 개인용 미디어 기기(12)의 예들로, 예를 들면, 랩톱/노트북 컴퓨터, PDA(이를 테면, 개인 휴대용 정

보 단말기(personal digital assistant)), 셀룰러폰, 휴대용 미디어 플레이어(예, MP3 플레이어), 페이저, 무선 이메일 기기(예, 블랙베리™ 기기), 및/또는 휴대용 게임 기기(예, 휴대용 플레이스테이션™)를 포함한다.

[0019] 하기에 논의될 것처럼, 상기 미디어 분배 시스템(18)으로부터 수신된 상기 미디어 콘텐츠(16)의 포맷의 예들로 다음을 포함할 수 있다: 예를 들면, 미디어 분배 시스템(18)(이를 테면, 미디어 분배 시스템(18)사용을 위해 예를 들면, 사용자(14)에게 허락된 미디어 콘텐츠); 및 미디어 분배 시스템(18)으로부터 스트리밍된 미디어 콘텐츠. 일반적으로, 미디어 콘텐츠(16)가 예를 들어, 컴퓨터(28)(이를 테면, 예를 들어, 서버 컴퓨터, 데스크톱 컴퓨터, 랩톱 컴퓨터, 개인 휴대용 정보 단말기, 또는 일련의 서버들을 포함할 수 있으나, 이에 국한하지 않음)로부터 개인용 미디어 기기(12)로 스트리밍될 때, 상기 미디어 콘텐츠(16)의 사본이 개인용 미디어 기기(12) 상에 영구히 보존되지 않는다. 미디어 분배 시스템(18)에 추가로, 미디어 콘텐츠(16)는 다른 소스들로부터 획득될 수 있으며, 그 예들로 뮤직 컴팩트 디스크들로부터 리핑된(ripped) 파일들을 포함할 수 있으나, 이에 국한되지 않는다.

[0020] 미디어 분배 시스템(18)에 의해 분배된 미디어 콘텐츠(16) 유형의 예들로 다음을 포함한다: 오디오 파일들(그 예들로 예를 들면, 음악 파일들, 오디오 뉴스 방송, 오디오 스포츠 방송, 및 서적의 오디오 레코딩들을 포함할 수 있으나, 이에 국한되지 않음); 비디오 파일들(그 예들로 예를 들면, 음향을 포함하지 않는 비디오 피트길이(video footage)를 포함할 수 있으나, 이에 국한되지 않음); 오디오/비디오 파일들(그 예들로 예를 들면, a/v 뉴스 방송, a/v 스포츠 방송, 극영화, 뮤직 비디오, 및 텔레비전 쇼의 에피소드들을 포함할 수 있으나, 이에 국한되지 않음); 및 멀티미디어 콘텐츠(그 예들로 예를 들면, 쌍방향 프레젠테이션 및 곁들이 프로들을 포함할 수 있으나, 이에 국한되지 않음).

[0021] 미디어 분배 시스템(18)은 일반적으로 다수의 사용자들(예, 사용자들(14,20,22,24,26))에게 미디어 데이터 스트림들 및/또는 미디어 데이터 파일들을 제공한다. 그러한 미디어 분배 시스템(18)의 예들로 워싱턴주, 시애틀의 리얼네트웍스™서비스에 의해 제공된 랩소디™ 서비스와 랩소디-투-고우™ 서비스를 포함한다. 전송 전에, 미디어 분배 시스템(18)은 예들 들면, MP3(이를 테면, MPEG 오디오 레이어 3(Motion Picture Experts Group Audio Layer 3)) 형식, AAC(이를 테면, Advanced Audio Coding) 형식, 리얼오디오™ 형식, 퀵타임™ 형식, 및 AVI(이를 테면, Audio Video Interleave) 형식으로 상기 미디어 데이터 스트림들 및/또는 미디어 데이터 파일들을 인코딩할 수 있다. 수신시, 상기 스트림들/파일들은 (적절한 디코더를 사용하여) 디코딩되고 렌더링 될 수 있다.

[0022] 미디어 분배 시스템(18)은 일반적으로 네트워크(30)(예, 인터넷)에 접속되는 컴퓨터(28)상에 상주하고 그에 의해 실행되는 서버 어플리케이션이다. 컴퓨터(28)는 네트워크 운용 시스템을 실행하는 웹서버(또는 일련의 많은 접속된 서버들)일 수 있으며, 그 예들로 마이크로소프트 윈도우즈 2000 서버™, 노벨 네트웨어™, 또는 레드햇 리눅스™를 포함할 수 있으나, 이에 국한되지 않는다.

[0023] 일반적으로, 컴퓨터(28)는 또한 웹서버 어플리케이션을 수행하며, 그 예로 네트워크(30)를 통해 컴퓨터(28)로의 HTTP(이를 테면, HyperText Transfer Protocol) 접근을 허용하는, 마이크로소프트 IIS™, 노벨 웹서버™, 아파치 웹서버™를 포함할 수 있으나, 이에 국한되지 않는다. 네트워크(30)는 예를 들면, 지역(local area) 네트워크; 광역(wide area) 네트워크; 또는 인트라넷과 같은, 하나 이상의 2차 네트워크들(예, 네트워크(32))에 접속될 수 있다.

[0024] 미디어 분배 시스템(18)의 인스트럭션 세트와 서브루틴은, 일반적으로 컴퓨터(28)에 커플된 저장장치(34)상에 저장되는 것으로서, 컴퓨터(28)에 병합된 하나 이상의 프로세서(도시하지 않음)와 하나 이상의 메모리 아키텍처(도시하지 않음)에 의해 수행된다. 저장장치(34)는 하드 디스크 드라이브, 테이프 드라이브, 광학 드라이브, RAID 어레이, 램(RAM: random access memory), 또는 롬(ROM: read-only memory)을 포함할 수 있으나, 이에 국한되지 않는다.

[0025] 사용자들(14,20,22,24,26)은 네트워크(30)를 통해 또는 2차 네트워크(32)를 통해 직접 미디어 분배 시스템(18)에 접근할 수 있다. 또한, 컴퓨터(28)(이를 테면, 미디어 분배 시스템(18)을 수행하는 컴퓨터)는 팬텀 링크 회선(36)으로 도시된 바와 같은, 2차 네트워크(32)를 통해 네트워크(30)에 접속될 수 있다.

[0026] 사용자들(14,20,22,24,26)은 다양한 클라이언트 미디어 기기들(12,38,40,42)를 통해 미디어 분배 시스템(18)에 접근할 수 있으며, 클라이언크 미디어 기기의 예들로 예를 들면, 개인용 미디어 기기들(12,38,40,42), 클라이언트 컴퓨터(44), 랩톱 컴퓨터(도시하지 않음), 개인 휴대용 정보 단말기(도시하지 않음), 셀룰러 폰(도시하지 않

음), 텔레비전(도시하지 않음), 케이블 박스(도시하지 않음), 인터넷 라디오(도시하지 않음), 또는 네트워크 전용 기기(도시하지 않음)를 포함할 수 있으나 이에 국한되지 않는다.

[0027] 상기 다양한 클라이언트 전자 기기들은 직접 또는 간접적으로 네트워크(30)(또는 네트워크(32))에 커플될 수 있다. 예를 들면, 클라이언트 컴퓨터(44)는 배선형 네트워크 접속(hardwired network connection)을 통해 네트워크(30)에 직접 커플되어 도시된다. 또한, 클라이언트 컴퓨터(44)는 예를 들면, 사용자(22)가 네트워크(30)(또는 네트워크(32))를 통해 미디어 분배 시스템(18)에 접근하여 구성하도록 하는 클라이언트 어플리케이션(26)(그 예로 마이크로소프트 인터넷 익스플로어™, 넷스케이프 네비게이터™, 리얼랩소디™ 클라이언트, 리얼플레이어™ 클라이언트 또는 특화된 인터페이스를 포함할 수 있으나 이에 국한되지 않음)을 수행한다. 클라이언트 컴퓨터(44)는 운용 시스템을 실행할 수 있으며, 그 운용 시스템의 예들로 마이크로소프트 윈도우즈™, 또는 레드햇 리눅스™를 포함할 수 있으나 이에 국한되지 않는다.

[0028] 클라이언트 어플리케이션(46)의 인스트럭션 세트와 서브루틴은, 일반적으로 클라이언트 컴퓨터(44)에 커플된 저장장치(48)에 저장되는 것으로, 클라이언트 컴퓨터(44)로 병합된 하나 이상의 프로세서(도시하지 않음)와 하나 이상의 아키텍처(도시하지 않음)에 의해 실행된다. 저장장치(48)는 하드 디스크 드라이브, 테이프 드라이브, 광학 드라이브, RAID 어레이, 램(RAM), 또는 롬(ROM)을 포함할 수 있으나 이에 국한되지 않는다.

[0029] 상기에 논의된 바와 같이, 다양한 클라이언트 전자 기기들은 네트워크(30)(또는 네트워크(32))에 직접 또는 간접적으로 커플될 수 있다. 예를 들면, 개인용 미디어 장치(38)는 개인용 미디어 기기(38)와 무선 접근점(이를 테면, WAP)(52) 간에 수립된 무선 통신 채널(50)을 통하여 네트워크(30)에 직접 커플되어 도시된다. WAP(52)은, 예를 들면, 개인용 미디어 장치(38)와 WAP(52) 간에 보안 통신 채널(50)을 수립할 수 있는 IEEE 802.11a, 502.11b, 802.11g, Wi-Fi, 및/또는 블루투스 장치일 수 있다.

[0030] 당해 기술분야에서 공지되는 것처럼, 모든 IEEE 802.11x 사양은 경로를 공유하기 위해 이더넷 프로토콜 및 반송파 감지 다중 접근/충돌 예방(carrier sense multiple access with collision avoidance)(이를 테면, CSMA/CA)을 사용한다. 다양한 802.11x 사양은, 예를 들면, 위상편이변조(phase-shift keying)(이를 테면, PSK) 또는 보수 코드 키잉(complementary code keying)(이를 테면, CCK)을 사용할 수 있다. 당해 기술분야에서 공지된 것처럼, 블루투스란, 예를 들면, 모바일 폰, 컴퓨터, 및 개인 휴대용 정보 단말기가 단거리 무선 접속을 사용하여 상호연결되도록 하는 텔레통신 산업 사양을 말한다.

[0031] 네트워크(30)(또는 네트워크(32))에 무선으로 커플되는 것에 추가로, 개인용 미디어 기기들은 프록시 컴퓨터(예를 들면, 개인용 미디어 기기(12)용 프록시 컴퓨터(54), 개인용 미디어 기기(40)용 프록시 컴퓨터(56), 및 개인용 미디어 기기(42)용 프록시 컴퓨터(58))에 커플될 수 있다.

[0032] [실시예]

[0033] **개인용 미디어 기기:**

[0034] 예를 들면 그리고 또한 도 2를 참조하면, 개인용 미디어 기기(12)는 도킹 크레이들(docking cradle)(60)을 통해 프록시 컴퓨터(54)로 연결될 수 있다. 일반적으로, 개인용 미디어 장치(12)는 도킹 크레이들(60)에 개인용 미디어 기기(12)를 커플하는 (하기에 보다 자세히 논의될) 버스 인터페이스를 포함한다. 도킹 크레이들(60)은 프록시 컴퓨터(54) 내에 포함된, 예를 들면, 범용 직렬 버스(universal serial bus)(이를 테면, USB) 포트, 직렬 포트, 또는 IEEE 1394(이를 테면, 방화벽) 포트에 (케이블(62)로) 커플될 수 있다.

[0035] 개인용 미디어 기기(12) 내에 포함된 버스 인터페이스는 USB 인터페이스일 수 있으며, 도킹 크레이들(60)은 USB 허브(이를 테면, 개인용 미디어 기기(12)와 도킹 크레이들(60)의 "핫(hot)" 커플링 및 언커플링을 허용하는 플러그-앤드-플레이 인터페이스)의 역할을 할 수 있다.

[0036] 프록시 컴퓨터(54)는 개인용 미디어 기기(12)를 위한 인터넷 게이트웨이의 역할을 할 수 있다. 따라서, 개인용 미디어 기기(12)는 네트워크(30)(및 네트워크(32))를 통해 미디어 분배 시스템(18)에 접근하고 미디어 콘텐츠(16)를 획득하는 프록시 컴퓨터(54)를 사용할 수 있다. 특히, 개인용 미디어 기기(12)로부터 미디어 분배 시스템(18)에 대한 요청을 수신시, (개인용 미디어 기기(12)를 대신해 인터넷 클라이언트의 역할을 하는) 프록시 컴퓨터(54)는 컴퓨터(28)(이를 테면, 미디어 분배 시스템(18)을 수행하는 컴퓨터)로부터 적절한 웹 페이지/서비스를 요청할 수 있다. 상기 요청된 웹 페이지/서비스가 프록시 컴퓨터(54)로 리턴되면, 프록시 컴퓨터(54)는 리턴된 웹 페이지/서비스와 (개인용 미디어 기기(12)에 의해 배치된) 원시 요청과 관련시켜 개인용 미디어 기기(12)로 상기 웹 페이지/서비스를 보낸다. 따라서, 프록시 컴퓨터(54)는 컴퓨터(28)로, 그리고, 그에 의해 미디어

분배 시스템(18)으로 개인용 미디어 기기(12)를 커플링하는 도관(conduit)의 역할을 할 수 있다.

[0037] 또한, 개인용 미디어 기기(12)는 기기 어플리케이션(64)(그 예들로 리얼랩소디™ 클라이언트, 리얼플레이어™ 클라이언트, 또는 특성화된 인터페이스를 포함할 수 있으나 이에 국한되지 않음)을 수행할 수 있다. 개인용 미디어 기기(12)는 운용 시스템을 실행할 수 있으며, 그 운용 시스템의 예들로 마이크로소프트 윈도우즈 CE™, 레드햇 리눅스™, 팜 OS™, 또는 장치-스퀵(이를 테면, 커스텀) 운용 시스템을 포함할 수 있으나 이에 국한되지 않는다.

[0038] DRM 프로세스(10)는 일반적으로 기기 어플리케이션(64)(그 예들로 기기 어플리케이션(64)의 임베디드된 특징, 기기 어플리케이션(64)을 위한 소프트웨어 플러그-인, 또는 기기 어플리케이션(64)에 제어되고 그로부터 명칭된 스탠드-얼론형(stand-alone) 어플리케이션을 포함할 수 있으나 이에 국한되지 않음)의 컴포넌트이다. 기기 어플리케이션(64) 및 DRM 프로세스(10)의 인스트럭션 세트 및 서브루틴은, 일반적으로 개인용 미디어 기기(12)에 커플된 저장 기기(66)상에 저장되는 것으로서, 개인용 미디어 기기(12)로 병합된 하나 이상의 프로세서(도시하지 않음)와 하나 이상의 메모리 아키텍처(도시하지 않음)에 의해 수행된다. 저장 기기(66)는, 예를 들면, 하드 디스크 드라이브, 광 드라이브, 램(RAM), 롬(ROM, CF(이를 테면, 컴팩트 플래시) 카드, SD(이를 테면, 보안 디지털) 카드, 스마트카드, 메모리 스틱, 및 멀티미디어 카드일 수 있다.

[0039] 관리자(administrator)(68)는 일반적으로 네트워크(30)(또는 네트워크(32))에 또한 연결되는 관리자 컴퓨터(72)상에서 실행하는 데스크톱 어플리케이션(70)(그 예들로 마이크로소프트 인터넷 익스플로어™, 넷스케이프 네비게이터™, 또는 특화된 인터페이스를 포함할 수 있으나 이에 국한되지 않음)을 통해 미디어 분배 시스템(18)에 접근하여 관리한다.

[0040] 데스크톱 어플리케이션(70)의 상기 인스트럭션 세트 및 서브루틴은, 일반적으로 관리자 컴퓨터(72)에 커플된 저장 기기(도시하지 않음) 상에 저장되는 것으로서, 관리자 컴퓨터(72)로 병합된 하나 이상의 프로세서(도시하지 않음) 및 하나 이상의 메모리 아키텍처(도시하지 않음)에 의해 수행된다. 관리자 컴퓨터(72)에 커플된 상기 저장 기기(도시하지 않음)는 하드 디스크 드라이브, 테이프 드라이브, 광 드라이브, RAID 어레이, 램(RAM), 또는 롬(ROM)을 포함할 수 있으나 이에 국한되지 않는다.

[0041] 도 3을 또한 참조하면, 개인용 미디어 기기(12)의 개략도가 도시된다. 개인용 미디어 기기(12)는 일반적으로 마아크로프로세서(150)(예, 캘리포니아주, 산타클라라의 인텔™에 의해 생산된 ARM™ 마이크로프로세서), 비휘발성 메모리(예,롬(152)), 및 휘발성 메모리(예, 램(154))를 포함하며; 각각은 하나 이상의 데이터/시스템 버스들(156, 158)을 통해 상호연결될 수 있다. 개인용 미디어 기기(12)는 또한 제거가능한 결속을 위한ㄴ 오디오 잭(162), 예를 들면, 헤드폰 어셈블리(164), 원격 스피커 어셈블리(166), 또는 이어 버드(ear bud) 어셈블리(168)에 아날로그 오디오 신호를 제공하는 오디오 서브시스템(160)을 포함할 수 있다. 대안적으로, 개인용 미디어 기기(12)는 하나 이상의 내부 오디오 스피커들(도시하지 않음)을 포함하도록 구성될 수 있다.

[0042] 개인용 미디어 기기(12)는 또한 사용자 인터페이스(170) 및 디스플레이 서브시스템(172)를 포함할 수 있다. 사용자 인터페이스(170)는 개인용 미디어 기기(12) 내에 포함된 다양한 입력 기기들로부터 데이터 신호들을 수신할 수 있다. 다양한 입력 기기들의 예들로, 예를 들면, 레이팅 스위치들(rating switches)(74,76); 뒤로 건너뛰기 스위치(78); 앞으로 건너뛰기 스위치(80); 재생/정지 스위치(82); 메뉴 스위치(84); 라디오 스위치(86); 및 슬라이더 어셈블리(88)를 포함할 수 있다(그러나 이에 국한되지 않음). 디스플레이 서브시스템(172)은 개인용 미디어 기기(12) 내에 포함된 디스플레이 패널(90)에 디스플레이 신호들을 제공할 수 있다. 디스플레이 패널(90)은 예를 들면, 능동형 매트릭스 액정 디스플레이 패널, 수동형 매트릭스 액정 디스플레이 패널, 또는 발광 다이오드 디스플레이 패널일 수 있다.

[0043] 오디오 서브시스템(150), 사용자 인터페이스(170), 및 디스플레이 서브시스템(172)은 하나 이상의 데이터/시스템 버스들(174, 176, 178) (각각)을 통해 마이크로프로세서(150)와 각각 커플될 수 있다.

[0044] 개인용 미디어 기기(12)의 사용 동안, 디스플레이 패널(90)은 예를 들면, 개인용 미디어 기기(12) 내에 저장된 미디어 콘텐츠(92, 94, 96)의 다양한 단편(piece)들의 제목 및 아티스트를 디스플레이하도록 구성될 수 있다. 슬라이더 어셈블리(88)는 개인용 미디어 기기(12) 내에 저장된 미디어 콘텐츠의 목록을 통해 위로 또는 아래로 스크롤링하는데 사용될 수 있다. 미디어 콘텐츠의 소정의 단편이 하이라이팅되면(예, "Taj Mahal"의 "Phantom Blues"), 사용자(14)는 재생/정지 스위치(82)를 사용하여 렌더링하기 위해 상기 미디어 콘텐츠를 선택할 수 있

다. 사용자(14)는 앞으로 건너뛰기 스위치(80)를 사용하여 다음 단편(예, "Robert Johnson"의 "Happy To Be Just...")의 미디어 콘텐츠를 앞으로 넘길 수 있거나; 또는 뒤로 건너뛰기 스위치(78)을 사용하여 이전 단편(예, "Leroy Brownstone"의 "Big New Orleans...")의 미디어 콘텐츠를 뒤로 넘길 수 있다. 추가로, 사용자(14)는 레이팅 스위치들(74, 76)을 사용함으로써 그들이 그것을 들음에 따라 미디어 콘텐츠의 사용률을 매길 수 있다.

[0045] 상기에 논의된 바와 같이, 개인용 미디어 기기(12)는 예를 들면, 도킹 크레이들(60)을 통해 프록시 컴퓨터(54)와 인터페이싱하기 위한 버스 인터페이스를 포함할 수 있다. 추가로 그리고 상기에 논의된 바와 같이, 개인용 미디어 기기(12)는 예를 들면, 개인용 미디어 기기(12)와 예를 들면, WAP(52) 간에 수립된 예를 들면, 무선 통신 채널(50)을 통해 네트워크(30)(및/또는 기타 개인용 미디어 기기들)에 무선으로 커플될 수 있다. 따라서, 개인용 미디어 기기(12)는 네트워크(30)(또는 네트워크(32)) 및/또는 기타 개인용 미디어 기기들에 개인용 미디어 기기(12)를 무선으로 커플링하기 위한 무선 인터페이스(182)를 포함할 수 있다. 무선 인터페이스(182)는 예를 들면, WAP(52)과의 RF 통신을 위한 안테나 어셈블리(184), 및/또는 예를 들면, (개인용 미디어 기기(40)와 같은) 제2 개인용 미디어 기기와의 적외선 통신을 위한 IR(이를 테면, 적외선) 통신 어셈블리(186)에 커플될 수 있다.

[0046] 상기에 논의된 바와 같이, 개인용 미디어 기기(12)는 기기 어플리케이션(64) 및 DRM 프로세스(10)의 인스트럭션 세트 및 서브루틴을 저장하기 위한 저장 기기(66)를 포함할 수 있다. 추가로, 저장 기기(66)는 미디어 분배 시스템(18)으로부터 다운로드된 미디어 데이터 파일들을 저장하고 미디어 분배 시스템(18)으로부터 스트리밍된 미디어 데이터 스트림(또는 그 일부)을 일시적으로 저장하는데 사용될 수 있다.

[0047] 저장 기기(66), 버스 인터페이스(180), 및 무선 인터페이스(182)는 하나 이상의 데이터/시스템 버스들(188, 190, 192) (각각)을 통해 마이크로프로세서(150)와 각각 커플될 수 있다.

[0048] 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 사용자들(14, 20, 22, 24, 26)에게 미디어 콘텐츠를 분배하며, 상기 분배된 미디어 콘텐츠는 미디어 데이터 스트림들 및/또는 미디어 데이터 파일들의 형태로 존재할 수 있다.

[0049] 따라서, 미디어 분배 시스템(18)은 단지 사용자들이 미디어 데이터 파일들을 다운로드하도록 구성될 수 있다. 예를 들면, 사용자(14)는, 미디어 분배 시스템(18)으로부터, 미디어 데이터 파일들(이를 테면, 그 예들로 MP3 파일들 또는 AAC 파일들을 포함할 수 있으나 이에 국한되지 않음)을 다운로드 하도록 할 수 있어, 상기 미디어 데이터 파일의 사본들이 컴퓨터(28)에서 (저장 기기(66) 상에 저장되어 있는) 개인용 미디어 기기(12)로 전송된다.

[0050] 대안적으로, 미디어 분배 시스템(18)은 단지 사용자들이 미디어 데이터 파일들의 미디어 데이터 스트림들을 수신 및 프로세스 하도록 구성될 수 있다. 예를 들면, 사용자(22)는 미디어 분배 시스템(18)으로부터 수신된 미디어 데이터 스트림들을 (클라이언트 컴퓨터(44) 상에서) 수신 및 프로세스 하도록 허용될 수 있다. 상기에 논의된 바와 같이, 미디어 콘텐츠가 예를 들어, 컴퓨터(28)에서 클라이언트 컴퓨터(44)로 스트리밍되면, 상기 미디어 데이터 파일의 사본은 클라이언트 컴퓨터(44) 상에 영구히 보존되지 않는다.

[0051] 또한, 미디어 분배 시스템(18)은 사용자들이 미디어 데이터 스트림들을 수신 및 프로세스 하도록 하고 미디어 데이터 파일들을 다운로드 하도록 구성될 수 있다. 그러한 미디어 분배 시스템의 예들로 워싱턴주, 시애틀의 리얼네트웍스™에 의해 제공된 랩소디™ 및 랩소디-투-고우™ 서비스들을 포함한다. 따라서, 사용자(14)는 미디어 분배 시스템(18)으로부터 미디어 데이터 파일들을 다운로드 하도록 하고 미디어 데이터 스트림들을 수신하도록 할 수 있다. 그러므로, 미디어 데이터 파일들의 사본들은 컴퓨터(28)에서 개인용 미디어 기기(12)(이를 테면, 저장 기기(66) 상에 저장되어 있는 상기 수신된 미디어 데이터 파일들)로 전송될 수 있다; 그리고 미디어 데이터 파일들의 스트림들은 개인용 미디어 기기(12)(이를 테면, 저장 기기(66) 상에 일시적으로 저장되어 있는 상기 수신된 미디어 데이터 파일들의 일부와 함께)에 의해 컴퓨터(28)로부터 수신될 수 있다. 추가로, 사용자(22)는 미디어 분배 시스템(18)으로부터 미디어 데이터 파일들을 다운로드 하도록 하고 미디어 데이터 스트림들을 수신 및 프로세스 하도록 할 수 있다. 그러므로, 미디어 데이터 파일들의 사본들은 컴퓨터(18)에서 클라이언트 컴퓨터(44)(이를 테면, 저장 기기(48) 상에 저장되어 있는 상기 수신된 미디어 데이터 파일들)로 전송될 수 있다; 그리고 미디어 데이터 파일들의 스트림들은 (저장 기기(48) 상에 일시적으로 저장되어 있는 상기 수신된 스트림들의 일부와 함께) 클라이언트 컴퓨터(44)에 의해 컴퓨터(28)로부터 수신될 수 있다.

[0052] 일반적으로, 예를 들면, 컴퓨터(28)로부터 미디어 데이터 스트림을 수신 및 프로세스 하기 위한 장치를 위해,

상기 장치는 컴퓨터(28), 그리고, 이에 따른 미디어 분배 시스템(18)에 능동형 접속부를 가져야 한다. 따라서, (이를 테면, 무선 채널(50)을 통해 컴퓨터(28)에 능동적으로 접속된) 개인용 미디어 기기(38), 및 (이를 테면, 배선에 의해 접속된 네트워크 접속부를 통해 컴퓨터(28)에 능동적으로 접속된) 클라이언트 컴퓨터(44)는 예를 들면, 컴퓨터(28)로부터 미디어 데이터 스트림들을 수신 및 프로세스 할 수 있다.

[0053] 상기에 논의된 바와 같이, 프록시 컴퓨터들(54, 56, 58)은 컴퓨터(28) 그리고, 그에 따른, 미디어 분배 시스템(18)에 개인용 미디어 기기들(12, 40, 42)을 (각각) 커플링 하기 위한 도관의 역할을 할 수 있다. 따라서, 개인용 미디어 기기들(12,40,42)이 예를 들면, 도킹 클레이들(60)을 통해 프록시 컴퓨터들(54, 56, 58)로 (각각) 커플링 되면, 개인용 미디어 기기들(12, 40, 42)은 컴퓨터(28)로 능동적으로 접속되며, 이에 따라, 컴퓨터(28)에 의해 제공된 미디어 데이터 스트림들을 수신 및 프로세스 할 수 있다.

[0054] **사용자 인터페이스들:**

[0055] 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 다양한 유형의 클라이언트 전자 기기들을 사용하여 접근될 수 있는 것으로서, 예를 들면, 개인용 미디어 기기들(12, 38, 40, 42), 클라이언트 컴퓨터(44), 개인 휴대용 정보 단말기들(도시하지 않음), 셀룰러 폰들(도시하지 않음), 텔레비전들(도시하지 않음), 케이블 박스들(도시하지 않음), 인터넷 라디오들(도시하지 않음), 또는 전용 네트워크 기기들(도시하지 않음)을 포함하나 이에 국한되지 않는다. 일반적으로 (특정 클라이언트 전자 기기를 위한 미디어 분배 시스템(18)을 구성할 때) 상기 사용자에 의해 사용된 인터페이스의 유형은 상기 미디어 콘텐츠가 스트리밍/다운로딩 되고 있는 클라이언트 전자 기기의 유형에 따라 달라질 것이다.

[0056] 예를 들면, 개인용 미디어 기기(12)의 (도 2에) 도시된 실시예와 같이 키보드를 포함하지 않으며 개인용 미디어 기기(12)의 디스플레이 패널(90)은 초소형이고, 미디어 분배 시스템(18)은 프록시 컴퓨터(54)상에 수행된 프록시 어플리케이션(98)을 통해 개인용 미디어 기기(12)를 위해 구성될 수 있다.

[0057] 프록시 어플리케이션(98)의 인스트럭션 세트들 및 서브 루틴들은, 일반적으로 프록시 컴퓨터(54)에 커플된 저장 기기(99)(도시하지 않음) 상에 저장되는 것으로서, 프록시 컴퓨터(54)로 병합된 하나 이상의 프로세서들(도시하지 않음) 및 하나 이상의 메모리 아키텍쳐들(도시하지 않음)에 의해 수행된다. 프록시 컴퓨터(54)에 커플된 저장 기기(99)(도시하지 않음)는 하드디스크 드라이브, 테이프 드라이브, 광 드라이브, RAID 어레이, 램(RAM), 또는 롬(ROM)을 포함할 수 있으나 이에 국한되지 않는다.

[0058] 추가로 그리고 유사한 이유들로, 개인 휴대용 정보 단말기들(도시하지 않음), 셀룰러 폰들(도시하지 않음), 텔레비전들(도시하지 않음), 케이블 박스들(도시하지 않음), 인터넷 라디오들(도시하지 않음), 및 전용 네트워크 기기들(도시하지 않음)은 미디어 분배 시스템(18)에 프록시 컴퓨터(54) 상에 수행된 프록시 어플리케이션(98)을 사용할 수 있다.

[0059] 또한, 상기 클라이언트 전자 기기는 프록시 어플리케이션(98)을 통해 구성될 미디어 분배 시스템(18)용 프록시 컴퓨터(54)에 직접 접속될 필요가 없다. 예를 들면, 미디어 분배 시스템(18)으로의 접근을 위해 사용된 상기 클라이언트 전자 기기는 셀룰러 폰인 것으로 가정하자. 셀룰러 폰들이 일반적으로 예를 들면, 프록시 컴퓨터(54)에 물리적으로 접속가능하지 않는 반면, 프록시 컴퓨터(54)는 여전히 상기 셀룰러 폰으로의 사용을 위해 미디어 분배 시스템(18)을 원격으로 구성하도록 사용될 수 있다. 따라서, 예를 들면, 프록시 컴퓨터(54)를 통해 진입하는 (상기 셀룰러 폰에 관한) 구성 정보는 사용자가 상기 셀룰러 폰으로 미디어 분배 시스템(18)에 접근하는 다음 시간까지 (컴퓨터(28)상의) 미디어 분배 시스템(18) 내에서 계속 간직될 수 있다. 동시에, 미디어 분배 시스템(18) 상에 저장된 상기 구성 정보는 상기 셀룰러 폰으로 다운로드 될 수 있다.

[0060] *키보드 및 보다 큰 디스플레이들(예, 클라이언트 컴퓨터(44))을 포함하는 시스템들을 위해, 클라이언트 어플리케이션(46)은 클라이언트 컴퓨터(44)로의 사용을 위해 미디어 분배 시스템(18)을 구성하도록 사용될 수 있다.

[0061] 또한 도 4를 참조하면, 미디어 분배 시스템(18)에 접근하기 위해 클라이언트 어플리케이션(46)을 사용할 때, 사용자(22)는 클라이언트 어플리케이션(46)에 의해 나타낸 정보 디스플레이 스크린(200)에 나타낼 수 있다. 클라이언트 어플리케이션(46)은 일반적으로 미디어 분배 시스템(18)과 인터페이싱하고 정보 디스플레이 스크린(200)을 보기 위한 사용자 인터페이스(202)(예, 웹 브라우저)를 포함한다.

[0062] 예들 들어, 사용자(22)가 예를 들어, 컴퓨터(28)로부터 미디어 콘텐츠를 스트림/다운로드할 때, 미디어 분배 시스템(18)은 상기 사용자의 클라이언트 전자 기기(예를 들면, 클라이언트 컴퓨터(44))로 스트리밍된/다운로드된

상기 미디어 콘텐츠를 모니터할 수 있으며, 그 결과 그 사용자를 위한 미디어 히스토리 파일(100)(도 1)의 생성을 야기한다. 미디어 히스토리 파일(100)이 일반적으로 국부적으로 보존되는 반면(예를 들면, 클라이언트 컴퓨터(44)상에 보존됨), 미디어 히스토리 파일(100)은 대안적으로/추가적으로 원격 미디어 히스토리 파일(100')로서 원격으로 보존될 수 있다(예를 들면, 컴퓨터(28) 상에 보존됨).

[0063] 상기 사용자(예, 사용자(22))는 이러한 미디어 히스토리 파일(또는 그 일부)을 저장할 수 있다. 재생목록은 일반적으로 미디어 분배 시스템(18)이 차례로 나타나게 될 트랙 그룹(그 예들로 노래, 비디오, 뉴스 방송, 스포츠 방송 등을 포함할 수 있으나 이에 국한되지 않음)이다. 이는, 차례로, 상기 사용자가 (다수의 재생목록의 형태로) 커스텀 음악 편집을 편집하도록 할 수 있다.

[0064] 히스토리 창(204)은 미디어 히스토리 파일(100) 내에 포함된 정보를 항목화하는 클라이언트 어플리케이션(46)에 의해 나타낼 수 있다. 이 예에서, 히스토리 창(204)은 10개의 미디어 데이터 스트림들(예, "Jailhouse Rock"; "Surf City"; "Runaround Sue"; "The Wanderer"; "The Great Pretender"; "Blueberry Hill"; "i'm Walkin'"; "Blue Christmas"; "Yakety Yak"; 및 "Peggy Sue")을 항목화하고, 이렇게 나타내어 사용자(22)가 이러한 10개의 미디어 데이터 스트림들을 미리 청취하게 된다.

[0065] 미디어 데이터 스트림들(이를 테면, 원격 기기, 예를 들어 컴퓨터(28)로부터 수신된 미디어 데이터 스트림들)에 추가로, 클라이언트 어플리케이션(46)은 사용자(12)가 로컬 미디어 데이터 파일들을 나타내도록 한다. 상기에 논의된 바와 같이, 로컬 미디어 데이터 파일은 미디어 분배 시스템(18)(이를 테면, 영구한 사용을 위한 사용자(14)에게 허락된 미디어 콘텐츠)로부터 수신된 구매형 다운로드; 미디어 분배 시스템(18)(이를 테면, 예를 들어, 유효한 가입이 미디어 분배 시스템(18)에 존재하는 동안 사용을 위한 사용자(14)에게 허락된 미디어 콘텐츠)로부터 수신된 가입형 다운로드; 및/또는 예를 들어, 음악 컴팩트 디스크로부터 추출된(이를 테면, 리핑된) 미디어 데이터 파일일 수 있다. 이러한 로컬 미디어 데이터 파일들은 일반적으로 국부적으로, 예를 들면 클라이언트 컴퓨터(44)에 커플된 저장 기기(48)에 국부적으로 저장된다.

[0066] 사용자(22)가 로컬 미디어 데이터 파일(이를 테면, 클라이언트 컴퓨터(44)에 저장된 파일)을 나타내기를 원한다면, 사용자(22)는 예를 들어, 클라이언트 어플리케이션(46)을 사용하여 나타내게 될 파일(들)을 선택할 수 있다. 따라서, 사용자(22)는 스크린 포인터(208)를 사용하여 드롭다운 "파일" 메뉴(206)를 선택할 수 있으며, 이는 포인팅 기기(예, 컴퓨터 마우스, 도시하지 않음)에 의해 제어가능할 수 있다. "열기(Open)" 커맨드를 선택하는 것은 파일 관리 창(210)을 나타내는 클라이언트 어플리케이션(46)을 초래할 수 있는 것으로, 사용자(22)가 재생을 위해 로컬 미디어 데이터 파일들을 선택하게 한다.

[0067] 이 예에서, 파일 관리 창(210)은 세 개의 로컬 미디어 데이터 파일들, 즉: "Chantilly Lace"(212); "Great Balls of Fire"(214); 및 "Tutti Frutti"(216)을 규정하는 것으로, 그 모두는 폴더 "내 음악(My Music)" 내에 저장된다. 사용자(22)는 클라이언트 어플리케이션(46) 상의 재생을 위해 이러한 파일들 중 임의의 것(또는 모두)를 선택할 수 있다.

[0068] 검색 창(218)은 사용자(예, 사용자(22))가 미디어 콘텐츠를 검색하도록 한다. 예를 들어, 사용자(22)는 검색어들(예, "앨비스 프레슬리(Elvis Presley)")을 입력하고, 적절한 용어 유형(예, 아티스트(artist))을 선택하며, 질의(query)을 수행할 수 있다. 다수의 아티스트들이 상기 질의를 만족할 경우에, 그 결과 세트는 사용자(22)가 선택할 수 있는, 예를 들면, 적절한 아티스트에 비롯하여 생성될 수 있다. 일단 적절한 아티스트가 선택되면, 사용자(22)는 선택된 아티스트(또는 상기 선택된 아티스트에 의한 트랙들을 포함하는 것)에 의해 발매된 다양한 앨범들을 리뷰할수 있다. 사용자(22)는 그 후 상기 앨범들 중 어느 하나 안에 포함된 하나 이상의 다양한 트랙들을 스트리밍하거나 다운로드할 수 있다. 일단 트랙이 렌더링되면, 상기 렌더링된 트랙에 관한 식별 정보는 로컬 미디어 히스토리 파일(100) 및/또는 원격 미디어 히스토리 파일(100')에 추가될 수 있으며 히스토리 창(204)에 포함될 수 있다. 아티스트에 의해 미디어 콘텐츠를 검색할 수 있는 것에 추가로, 사용자(14)는 또한 예를 들어, 키보드, 트랙, 앨범 및/또는 작곡가에 의해 미디어 콘텐츠를 검색할 수 있게 된다.

[0069] 또한 도 5를 참조하여 사용자(22)가 재생을 위해 세 개의 로컬 미디어 데이터 파일들 모두를 선택한다고 가정하면, 미디어 히스토리 파일(100)은 세 개의 추가 등록들, 즉 하나는 "Chantilly Lace"; 하나는 "Great Balls of Fire"; 및 하나는 "Tutti Frutti"를 포함하도록 수정될 수 있다. 따라서, 히스토리 창(204)은 미디어 히스토리 파일(100) 내에 포함된 정보를 항목화하므로, 히스토리 창(204)은 로컬 미디어 데이터 파일 "Chantilly Lace"(212); 로컬 미디어 데이터 파일 "Great Balls of Fire"(214); 및 로컬 미디어 데이터 파일 "Tutti Frutti"(216)에 상응하는, 세 개의 추가 등록들(이를 테면, 등록들(220, 222, 224))을 포함할 것이다.

[0070] 사용자(22)가 앞으로의 재생을 위해 이러한 음악 모음집을 저장하길 원한다고 가정하면, 사용자(22)는 재생목록(102)(도 1)으로 현재 미디어 히스토리 파일(100)(또는 그 일부)을 저장할 수 있다. 재생목록(102)은 일반적으로 국부적으로 보존되는 (예를 들면, 클라이언트 컴퓨터(44) 상에 보존됨) 반면에, 재생목록(102)은 대안적으로/추가적으로 원격 재생목록(102')으로서 원격으로 보존될 수 있다(예를 들면 컴퓨터(28) 상에 보존됨).

[0071] 또한 도 6을 참조하면, 사용자(22)는 (스크린 포인터(208)를 사용하여) "저장(save)" 버튼(240)을 선택할 수 있다. 일단 상기 "저장" 버튼(240)이 선택되면, 재생목록 이름 창(242)은 사용자(22)가 재생목록 이름 창(242)의 이름 필드(244) 내에 재생목록(102)에 대한 유일한 이름을 상술하게 하는 것으로 (클라이언트 어플리케이션(46)에 의해) 나타낼 수 있다.

[0072] 사용자(22)가 재생목록 이름으로 "50's Hits"를 선택한다고 가정하면, 재생목록(102)은 (이를 테면, "50's Hits"로) 저장되며 히스토리 창(204) 내에 항목화된 미디어 콘텐츠의 모든 단편의 위치를 규정한다.

[0073] 또한 도 7을 참조하면, 일단 재생목록(102)이 저장되면, 재생목록(102)(예, "50's Hits")에 대한 링크(260)가 디렉토리 창(262)에 나타난다. 사용자(22)는 그 후 스크린 포인터(208)를 사용하여 링크를 선택할 수 있다. 일단 선택되면, 재생목록(102)(예, "50's Hits") 내에 포함된 트랙들은 사용자 인터페이스(202)를 통해 볼 수 있는 재생목록 창(264)(예, 웹페이지) 내에 항목화 된다. 상기에 논의된 바와 같이, 10개의 이러한 등록들(즉, "Jailhouse Rock"; "Surf City"; "Runaround Sue"; "The Wanderer"; "The Great Pretender"; "Blueberry Hill"; "I'm Walkin'"; "Blue Christmas"; "Yakety Yak"; 및 "Peggy Sue")은 미디어 데이터 스트림들의 위치를 규정하고 세 개의 이러한 등록들(즉, "Tutti Frutti"; "Chantilly Lace"; 및 "Great Balls of Fire")은 미디어 데이터 파일들의 위치를 규정한다.

[0074] 일반적으로, 재생목록 창(264)은 재생목록(102) 내에 항목화된 개별 등록들과 연관된 상기 스트림들/파일들이 위치하는 하이퍼링크들을 포함한다(이를 테면, 상기 스트림들/파일들의 주소들을 제공함). 이러한 위치 정보는 재생목록(102) 내에 저장될 수 있다. 예를 들면, 하기 표는 그 트랙 이름과 연관된 상기 스트림/파일의 주소를 갖는 재생목록(102) 내 등록의 트랙 이름과 관련된다:

[0075]

트랙 이름	주소
Jailhouse Rock	www.musicshop.com\songs\jailhouse_rock.ram
Surf City	www.musicshop.com\songs\surf_city.ram
Runaround Sue	www.musicshop.com\songs\runaround_sue.ram
The Wanderer	www.musicshop.com\songs\the_wanderer.ram
The Great Pretender	www.musicshop.com\songs\the_great_pretender.ram
Blueberry Hill	www.musicshop.com\songs\blueberry_hill.ram
I'm Walkin'	www.musicshop.com\songs\im_walkin.ram
Blue Christmas	www.musicshop.com\songs\blue_christmas.ram
Yakety Yak	www.musicshop.com\songs\yakety_yak.ram
Peggy Sue	www.musicshop.com\songs\peggy_sue.ram
Tutti Frutti	c:\my music\tutti_frutti.mp3
Chantilly Lace	c:\my music\chantilly_lace.mp3
Great Balls of Fire	c:\my music\great_balls_of_fire.mp3

[0076] 처음 10개의 등록들(즉, "Jailhouse Rock"; "Surf City"; "Runaround Sue"; "The Wanderer"; "The Great Pretender"; "Blueberry Hill"; "I'm Walkin'"; "Blue Christmas"; "Yakety Yak"; 및 "Peggy Sue")은 미디어 데이터 스트림들을 식별하므로, 각 등록에 제공된 주소는 예를 들면, 미디어 분배 시스템(18)으로부터 이용가능한 미디어 스트림으로 나타낸다. 또한, 마지막 세 개의 등록들(즉, "Tutti Frutti"; "Chantilly Lace"; 및 "Great Balls of Fire")은 미디어 데이터 파일들을 식별하므로, 각 등록에 제공된 주소는 예를 들면, 클라이언트 컴퓨터(44)로부터 이용가능한 미디어 데이터 파일로 나타낸다.

[0077] 재생목록 창(264)은 일반적으로 표로 되어 있으며 재생목록 창(264) 내의 각 등록에 대한 미디어 유형(이를 테면, 예를 들어 미디어 데이터 스트림 또는 미디어 데이터 파일)을 식별하는 컬럼(266)을 포함할 수 있다. 일반적으로, 컬럼(266)은 상기 미디어 유형을 식별하는 아이콘들을 포함한다(예, 아이콘(268)은 미디어 데이터 파일을 규정하고 아이콘(270)은 미디어 데이터 스트림을 규정함). 사용자(22)는 재생목록(102)을 나타내기 위해 "재생(play)" 버튼(272)를 선택할 수 있다.

[0078] 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 일반적으로 사용자들(예, 사용자(22))에게 미디어 데이터 스트림들 및/또는 미디어 데이터 파일들을 제공한다. 일반적으로, 메타데이터(metadata)는 미디어 분배 시스템(18)에 의해 제공된 각 미디어 데이터 스트림과 연관된다. 이러한 메타데이터는 예들 들어, 아티스트 식별자, 앨범 식별자, 트랙 식별자, 앨범 커버 이미지, 및 음악 장르 식별자를 포함할 수 있다(그러나 이에 국한되지 않음).

[0079] 따라서, 예를 들어, 사용자(12)가 원격 미디어 데이터 스트림을 렌더링할 때는 언제나, 미디어 분배 시스템(18)은 트랙에 대한, 예를 들면, 개별 사용자들의 청취 취향 및 음악 선호도에 대한 (사용자별로) 이러한 메타데이터를 편집 및 저장할 수 있다.

[0080] 상기에 논의된 바와 같이, 로컬 디지털 미디어 데이터 파일은 미디어 분배 시스템(18)(이를 테면, 예를 들어, 영구적 사용을 위한 사용자(14)에게 허락된 미디어 콘텐츠)으로부터 수신된 구매형 다운로드; 미디어 분배 시스템(이를 테면, 유효한 가입이 미디어 분배 시스템(18)에 존재하는 동안 예를 들어, 사용을 위한 사용자(14)에게 허락된 미디어 콘텐츠)로부터 수신된 가입형 다운로드; 및/또는 예를 들어, 음악 컴팩트 디스크로부터 추출된 (이를 테면, 리핑된) 미디어 데이터 파일일 수 있다.

[0081] 상기 구매형 다운로드 및/또는 가입형 다운로드가 미디어 분배 시스템(18)에 의해 제공된다면, 이러한 로컬 미디어 데이터 파일들은 일반적으로 상기 설명된 메타데이터를 또한 포함할 것이다. 따라서, 이러한 구매형/가입형 다운로드들이 예를 들어, 사용자(22)에 의해 렌더링 때, 이러한 구매형/가입형 다운로드들에 관한 메타데이터는 트랙에 예를 들어, 청취 취향과 음악 선호도들이 (사용자별로) 편집되어 저장되도록, 컴퓨터(44)에서 컴퓨터(28)로 전송될 수 있다.

[0082] 하지만, 예를 들어, 음악 컴팩트 디스크들로부터 추출되는 미디어 데이터 파일들에 대하여, 이러한 데이터 파일들은 상기 설명된 메타데이터를 포함하지 않을 수 있다. 상기에 논의된 바와 같이, 메타데이터 파일들(이를 테면, 클라이언트 컴퓨터(44) 상에 저장된 파일들)은 클라이언트 어플리케이션(46)을 사용하여 렌더링되거나 재생목록들(예, 재생목록(102))에 추가될 수 있다. 따라서, 사용자(22)가 재생목록(예, 재생목록(102))에 미디어 데이터 파일을 추가하도록 시도할 때는 언제나, 사용자(22)는 그 미디어 데이터 파일에 관한 메타데이터를 제공하도록 촉구될 수 있다.

[0083] 또한 도 8을 참조하고 상기 설명된 예에 계속이어, 사용자(22)는 세 개의 로컬 미디어 데이터 파일들(즉, "Tutti Frutti"; "Chantilly Lace"; 및 "Great Balls of Fire")을 포함하는 재생목록(예, 재생목록(102))을 저장하도록 시도하는 경우, 세 개의 로컬 미디어 데이터 파일들은 메타데이터를 포함하지 않는 것으로 가정하면, 클라이언트 어플리케이션(46)은 사용자(22)가 각각의 상기 세 개의 메타데이터 파일들에 관한 메타데이터를 등록하도록 하는 메타데이터 등록 폼(280)을 렌더링할 수 있다.

[0084] 이 예에서, 메타데이터 등록 폼(280)은 5개의 사용자-편집가능 필드들, 즉 아티스트 필드(282), 앨범 필드(284), 트랙 필드(286), 앨범 커버 이미지 필드(288), 및 음악 장르 필드(290)를 포함한다. 앨범 커버 이미지 필드(288)는 사용자(22)가 앨범 커버 이미지에 대한 드라이브, 경로, 및 파일명을 규정하도록 할 수 있다. 음악 장르 필드(290)는 사용자(22)가 미리 규정된 음악 장르의 수로부터 음악 장르를 선택하게 하는 (스크린 포인터(208)를 통해 동작가능한) 드롭-다운 메뉴일 수 있다(도시하지 않음).

[0085] 일반적으로, 상기 미디어 데이터 파일의 제목이 상기 트랙 이름을 설명인 경우, 상기 트랙 필드(286)는 클라이언트 어플리케이션(46)의 추측이 트랙 제목으로 자동으로 채워질 수 있다. 상기 제1 로컬 미디어 데이터 파일이 "tutti frutti"로 지징됨에 따라, 트랙 필드(286)는 일반적으로 추측된 이름 "tutti frutti"로 채워질 것이다. 사용자(22)는 남은 필드들을 채울 수 있으며 (스크린 포인터(208)를 사용하여) 저장 버튼(292)을 선택하거나 대안적으로 취소 버튼(294)을 선택할 수 있다.

[0086] 상기 메타데이터 생성 프로세스를 보다 자동화하기 위해, 클라이언트 어플리케이션(44)은 예를 들면, 미디어 분배 시스템(18) 또는 제3자(도시하지 않음)에 의해 서비스된 원격 메타데이터 데이터베이스(도시하지 않음)와 인터페이싱할 수 있다. 이러한 메타데이터 데이터베이스는 다양한 트랙들 및 앨범들에 대한 메타데이터를 규정할 수 있다. 그러한 데이터베이스의 예로 캘리포니아주, 에버리빌의 Gracenote™(www.gracenote.com)에 의해 보존된 CDDB™ 데이터베이스가 있다. 예를 들어, 사용자(22)가 전체 컴팩트 디스크로부터 각 트랙을 리핑했다면, 상기 메타데이터 데이터베이스는 클라이언트 어플리케이션(44)에 의해 접근될 수 있으며 질의(query)는 예를 들면, 상기 컴팩트 디스크 상에 포함된 트랙의 총수, 상기 컴팩트 디스크 상에 포함된 각 트랙의 길이, 및 상기 컴팩트 디스크의 총 길이를 규정하는 것으로 구성될 수 있다. 최종 결과가 이러한 질의에 의해 생성되는 것으로

가정하면, 상기 컴팩트 디스크로부터 리핑된 각 트랙에 대한 메타데이터가 생산될 것이다. 최종 결과 세트(이를테면, 다수의 가능한 컴팩트 디스크들을 규정하는 세트)가 생성되는 경우에, 사용자(22)는 가능한 매치들의 목록(도시하지 않음)으로부터 적절한 컴팩트 디스크를 선택하도록 촉구될 수 있다.

[0087] 상기에 논의된 바와 같이, (클라이언트 기기에 대한 미디어 분배 시스템(18)을 구성할 때) 상기 사용자에 의해 사용된 인터페이스의 유형은 상기 미디어 콘텐츠가 스트리밍/다운로드 되고 있는 상기 클라이언트 전자 기기의 유형과 성능에 따라 변할 수 있다. 따라서 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 프록시 컴퓨터(54) 상에 수행된 프록시 어플리케이션(98)을 통해 개인용 미디어 기기(12)가 구성될 수 있다.

[0088] 프록시 어플리케이션(98)은 개인용 미디어 기기(12)가 도킹 크레이들(60)로 예를 들어 사용자(14)에 의해 배치될 때 자동으로 수행될 수 있다. 대안적으로, 프록시 어플리케이션(98)은 프록시 컴퓨터(54)의 부팅시 완전히 또는 부분적으로 로드될 수 있다. 프록시 어플리케이션(98)은 그 후 개인용 미디어 기기(12)가 도킹 크레이들(60)로 배치될 때까지 백그라운드로 동작할 수 있으며, 그 시점에서 프록시 어플리케이션(98)이 수행을 위해 포그라운드로 완전히 로드 및/또는 이동될 수 있다. 또한, 프록시 어플리케이션(98)은 사용자(14)에 의해 수동으로 수행될 수 있다. 하기에 보다 자세히 논의될 것처럼, (일단 수행된) 프록시 어플리케이션(98)은 예를 들어 개인용 미디어 기기(12)를 구성하고 예를 들어, 미디어 데이터 파일들을 개인용 미디어 기기(12)로 전송하며 개인용 미디어 기기(12)로부터 미디어 데이터 파일들을 제거하는데 사용될 수 있다.

[0089] 또한 도 9를 참조하면, 미디어 분배 시스템(18)으로의 접근을 위해 프록시 어플리케이션(98)을 사용할 때, 사용자(14)는 프록시 어플리케이션(98)에 의해 렌더링된 정보 디스플레이 스크린(300)으로 나타낼 수 있다. 프록시 어플리케이션(98)은 일반적으로 미디어 분배 시스템(18)과 인터페이싱하여 정보 디스플레이 스크린(300)을 보기 위한 사용자 인터페이스(302)(예, 웹 브라우저)를 포함한다.

[0090] 검색 창(304)은 사용자(예, 사용자(14))가 미디어 콘텐츠를 검색하도록 한다. 예를 들어, 사용자(14)는 검색 필드(306)에 검색 용어들(예, "Elvis Presley")를 입력할 수 있다. 다수의 아티스트들이 그 질의를 만족하는 경우에, 그 결과 세트는 사용자(22)가 선택할 수 있는, 예를 들면, 적절한 아티스트에 비롯하여 생성될 수 있다. 일단 적절한 아티스트가 선택되면, 사용자(14)는 상기 선택된 아티스트(또는 상기 선택된 아티스트의 트랙들을 포함하는 것)에 의해 발매된 다양한 앨범들을 리뷰할 수 있다. 사용자(14)는 그 후 (개인용 미디어 기기(12)상에서의 사용을 위해) 상기 앨범들 중 어느 하나에 포함된 하나 이상의 다양한 트랙들을 다운로드 할 수 있다. 아티스트들의 미디어 콘텐츠에 대한 검색을 할 수 있는 것에 추가로, 사용자(14)는 또한 예를 들어, 키보드, 트랙, 앨범 및/또는 작곡가로 미디어 콘텐츠를 검색할 수도 있다.

[0091] 추가로, 클라이언트 어플리케이션(46)의 방식과 유사한 방식으로, 프록시 어플리케이션(98)은 사용자(12)가 상기 선택된 아티스트의 앨범들 중 어느 하나 안에 포함된 하나 이상의 다양한 트랙들을 (프록시 컴퓨터(54)를 통해) 렌더링하도록 구성될 수 있다.

[0092] 콘텐츠 창(308)은 사용자(14)가 개인용 미디어 기기(12)의 콘텐츠를 리뷰하도록 하는 프록시 어플리케이션(98)에 의해 렌더링 될 수 있다. 상기에 논의된 바와 같이, 개인용 미디어 기기(12)는 예를 들면 USB 포트, 직렬 포트, 또는 방화벽 포트를 통해 프록시 컴퓨터(54)로 커플될 수 있다. 프록시 어플리케이션(98)의 수행시 또는 수행 동안, 프록시 어플리케이션(98)은 기기(12) 상의 현재 미디어 콘텐츠에 관한 정보를 회수하기 위해 개인용 미디어 기기(12)를 폴링할 수 있다. 이러한 폴링(polling)은 USB 하드 드라이브의 콘텐츠가 결정되는 것과 유사한 방식으로 발생할 수 있다. 상기 특정 실시예에서, 콘텐츠 창(308)은 10개의 등록, 즉: "Jailhouse Rock"; "Surf Fity"; "Runaround Sue"; "The Wanderer"; "The Great Pretender"; "Blueberry Hill"; "I'm Walkin'"; "Blue Christmas"; "Yakety Yak"; 및 "Peggy Sue"를 포함하며, 이에 따라 10개의 미디어 데이터 파일들이 개인용 미디어 기기(12)로 미리 다운로드 되어 온 것을 나타내는 것으로, 일반적으로 개인용 미디어 기기(12)의 저장 기기(66)상에 저장된다.

[0093] 콘텐츠 창(308)은 표의 형태이며 트랙(310), 아티스트(312), 트랙 길이(314) 및 트랙 크기(316)를 포함하는, 다운로드된 파일들에 관한 다양한 단편의 정보를 항목화 할 수 있다. 추가로, 프록시 어플리케이션(98)은 기기 식별 정보를 회수하기 위한 내 폴 개인용 미디어 기기(14)로서, 콘텐츠 창(308) 내에 포함된 기기 유형 필드(320) 및 기기 일련 번호 필드(322) 내에 렌더링 될 수 있다. 또한, 콘텐츠 창(308)은 예를 들어, 기가바이트의 "비사용 공간"; 기가바이트의 "사용 공간"; 총 용량 중 "비사용 공간"의 비율; 및 총 수용량의 "사용 공간" 비율 중 하나 이상을 포함하는, 기기(12)의 현재 용량에 관한 요약 정보 필드(324)를 포함할 수 있다.

[0094] 또한 도 10을 참조하고 상기 설명된 실시예에 계속하여, 사용자(14)는 검색 창(304)의 검색 필드(306)에 용어

"Elvis Presley"를 입력하고, 드롭다운 메뉴(340)를 통해 용어 유형 "아티스트"를 선택하며, 스크린 포인터(208)로 "검색(Go)" 버튼(324)을 선택함으로써 질의를 수행하는 것으로 가정하자.

[0095] 그 질의를 충족시키는 다른 아티스트가 없다고 가정하면, 정보 스크린(300)은 사용자에게 앨비스 프레슬리에 관한 정보를 보여줄 수 있는 것으로서, 예를 들어, 아티스트 정보 스크린(344), 상위 트랙 목록(346), 앨범 목록(348), 및 유사한 아티스트 목록(350)을 포함할 수 있다.

[0096] 사용자(14)는 다운로드될 트랙에 해당하는 다운로드 버튼(352)을 선택함으로써 개인용 미디어 기기(12) 상의 사용을 위해 미디어 분배 시스템(18)으로부터 미디어 데이터 파일들을 다운로드 할 수 있다. 추가로, 사용자(14)는 다운로드될 트랙들로부터 다운로드 모두 버튼(354)을 선택함으로써 트랙 그룹들(예, 상위 트랙 목록(346) 내에 포함된 각 트랙, 또는 싱글 앨범 내에 포함된 모든 트랙들)을 다운로드 할 수 있다.

[0097] 일단 사용자(14)가 다운로딩을 하기 위해 트랙을 선택하면, 프록시 어플리케이션(98)은 예를 들어, 다운로드 되고 있는 트랙의 제목을 식별하는 트랙 제목 필드(358) 및 다운로드 되고 있는 트랙의 아티스트를 식별하는 아티스트 필드(360)를 포함하는, 다운로드 창(356)을 렌더링할 수 있다.

[0098] 상기에 논의된 바와 같이, 파일들은 구매형 다운로드들(이를 테면, 영구적 사용을 위한 예를 들면, 사용자(14)에게 허락된 미디어 콘텐츠), 또는 가입형 다운로드들(이를 테면, 유효한 가입이 미디어 분배 시스템(18)에 존재하는 동안 사용을 위한 예를 들면, 사용자(14)에게 허락된 미디어 콘텐츠)로서 미디어 분배 시스템(18)으로부터 다운로드 될 수 있다. 사용자(14)가 미디어 분배 시스템(28)에 현재 가입을 갖도록 제공되면, 일반적으로 상기 다운로드된 미디어 콘텐츠는 사용자가 유효한 가입을 가질 동안에는 렌더링될 수 있으므로, 각 가입형 다운로드에 대해 청구된 추가 비용은 없다. 사용자는 일반적으로 상기 미디어 콘텐츠가 사용자의 가입의 상태에 상관없이 렌더링 가능하므로, 각 구매형 다운로드에 대한 비용(예를 들면, 9¢, 89¢, 또는 99¢)을 지불해야 한다.

[0099] 따라서, 다운로드 창(356)은 구매 버튼(362) 및 다운로드 버튼(364)을 포함할 수 있는 것으로서, 그 둘 모두는 스크린 포인터(208)를 통해 선택가능하다. 이 실시예에서, 사용자(14)가 스크린 포인터(208)로 구매 버튼(362)을 선택한다면, "Elvis Presley"의 Hound Dog"에 대한 미디어 데이터 파일은 컴퓨터(28)에서 개인용 미디어 기기(12)로 전송될 것이다. 일반적으로, 사용자(14)는 예를 들면, 이 미디어 콘텐츠 파일을 다운로딩 하기 위해 한 번의 다운로드 비용이 청구될 것이다. 하지만, 이것은 구매형 다운로드이므로, 수신된 상기 미디어 데이터 파일은 미디어 분배 시스템(18)에 상기 사용자의 가입 상태에 상관없이 렌더링 가능하다.

[0100] 대안적으로, 사용자(14)가 스크린 포인터(208)로 다운로드 버튼(364)을 선택한다면, "Elvis Presley"의 "Hound Dog"에 대한 미디어 데이터 파일은 컴퓨터(28)에서 개인용 미디어 기기(12)로 전송될 것이다. 일반적으로, 사용자(14)는 이 미디어 데이터 파일을 다운로딩 하기 위한 비용이 청구되지 않을 것이다. 하지만, 이것은 가입형 다운로드이므로, 수신된 미디어 데이터 파일은 사용자(14)가 미디어 분배 시스템(18)에 유효한 가입을 가지는 동안만 렌더링 가능하다.

[0101] 다운로드 창(114)은 일반적으로 사용자(14)가 다운로드를 취소하고 다운로드 창(356)을 닫도록 하는 취소 버튼(366)을 또한 포함한다.

[0102] 사용자(14)가 구매 버튼(362)이든 또는 다운로드 버튼(364)이든 선택한다면, 선택된 미디어 데이터 파일의 다운로드는 초기화될 것이다. 다운로드 창(356)은 다운로드 과정, 예를 들면, "Elvis Presley"의 "Hound Dog"를 표시하기 위한 다운로드 상태 표시기(368)를 포함할 수 있다.

[0103] 또한 도 11을 참조하면, 일단 "Elvis Presley"의 "Hound Dog"에 대한 상기 미디어 데이터 파일의 다운로드가 완료되면, 콘텐츠 창(308)은 "Elvis Presley"의 "Hound Dog"가 미디어 분배 시스템(18)에서 개인용 미디어 기기(12)로 성공적으로 다운로드 되었음을 표시하는, "Elvis Presley"의 "Hound Dog"에 대한 등록(380)을 포함하도록 업데이트 될 것이다.

[0104] 클라이언트 어플리케이션(46)에 관한 상기에 설명된 방식과 유사한 방식으로, 사용자(14)는 개인용 미디어 기기(12)상에 저장된 다양한 미디어 데이터 파일들에 관한 재생목록들을 규정하기 위해 프록시 어플리케이션(98)을 사용할 수 있다. 예를 들어, 사용자(14)가 재생목록으로서 먼저 13개의 트랙(즉 "Jailhous Rock"; "Surf City"; "Runaround Sue"; "The Wanderer"; "The Great Pretender"; "Blueberry Hill"; "I'm Walkin'"; "Blue Christmas"; "Yakety Yak"; "Peggy Sue"; "Tutti Frutti"; "Chantilly Lace"; 및 "Great Balls of Fire")을 저장하기를 원한다고 가정하면, 사용자(14)는 (스크린 포인터(208)을 사용하여) 트랙들의 원하는 선택을 강조하고 스크린 포인터(208)을 사용하여 저장 버튼(382)을 선택할 것이다. 재생목록 이름 창(384)은 사용자(14)가 재

생목록 이름 창(384) 내의 재생목록에 대해 유일한 이름을 설명하게 한다는 것을 (프록시 어플리케이션(98)에 의해) 렌더링될 수 있다.

[0105] 사용자(14)가 재생목록 이름으로 "50's Hits"를 선택한다고 가정하면, "50's Hits"로 지칭된 재생목록(104)(도 1)은 재생목록(104) 내에 항목화된 미디어 콘텐츠의 모든 단편들이 (개인용 미디어 기기(12) 내에) 위치한다고 규정될 수 있다.

[0106] 일단 선택되면, 재생목록(104) 내에 포함된 트랙들(예, "50's Hits")은 일반적으로 사용자 인터페이스(302)를 통해 볼 수 있는 재생목록 창(392)(예, 웹 페이지) 내에 항목화된다.

[0107] 클라이언트 어플리케이션(44)을 사용하여 생성됨으로써 상기에 설명된 재생목록들로서, 프록시 어플리케이션(98)을 사용하여 생성된 재생목록들은 일반적으로 국부적으로 유지된다(예를 들면, 개인용 미디어 기기(12) 상에 유지됨). 하지만 상기에 논의된 바와 같이, 재생목록들은 원격 재생목록(104')으로서 원격으로 대안적으로/추가적으로 보존될 수 있다(예를 들어, 컴퓨터(28) 상에 보존됨).

[0108] **기기 초기화:**

[0109] 미디어 분배 시스템(18)은 일반적으로 사용자(14)가 미디어 분배 시스템(18)에 가입하고 미디어 분배 시스템(18)으로의 접근이 허용되도록 예를 들면 매달 가입비를 지불하는, 가입 기반 서비스이다. 일단 사용자(14)가 미디어 분배 시스템(18)에 가입하면, 사용자(14)는 예를 들면, 다음과 같은 형태로 (개인용 미디어 기기(12)로 사용하기 위한) 미디어 콘텐츠를 획득할 수 있다: 미디어 분배 시스템(18)으로부터 수신된 구매형 다운로드(이를 테면, 예를 들어 영구적 사용을 위한 사용자(14)에게 허락된 미디어 콘텐츠); 미디어 분배 시스템(18)으로부터 수신된 가입형 다운로드(유효한 가입이 미디어 분배 시스템(18)에 있을 동안, 예를 들어, 사용을 위한 사용자(14)에게 허락된 미디어 콘텐츠); 및 미디어 분배 시스템(18)으로부터 스트리밍된 미디어 콘텐츠. 일반적으로, 미디어 분배 시스템(18)에 접근할 때, 사용자(14)는 미디어 분배 시스템(18)게 상기 사용자(예, 사용자(14)) 및/또는 기기(예, 기기(12))를 식별하는 사용자 "인증서들(credentials)"를 제공해야한다. 이러한 인증서 수신시, 미디어 분배 시스템(18)은 상기 인증서를 검증하도록 그리고, 검증되면, 승인된 사용자(14) 및 기기(12)가 미디어 분배 시스템(18)에 접근하도록 시도할 수 있다. 미디어 분배 시스템(18)에 의해 수신 및 검증된 인증서는 사용자 이름, 사용자 비밀번호, 사용자 키, 기기 이름, 기기 비밀번호, 기기 키, 및/또는 하나 이상의 디지털 인증서들을 포함할 수 있으나, 이에 국한되지 않는다.

[0110] 일반적으로, 개인용 미디어 기기(12)가 도킹 크레이들(60)로 배치될 때, 개인용 미디어 기기(12)는 프록시 컴퓨터(54)를 통해 미디어 분배 시스템(18)과의 접속부를 수립한다. 상기에 논의된 바와 같이, 프록시 컴퓨터(54)는 개인용 미디어 기기(12)를 위한 인터넷 게이트웨이의 역할을 하고, 이에 따라, 개인용 미디어 기기(12)가 컴퓨터(28)와 미디어 분배 시스템(18)에 접근하도록 한다.

[0111] 일단 접속부가 미디어 분배 시스템(18)에 수립되면, DRM 프로세스(10)는 초기화될 수 있다. DRM 프로세스(10)는 일반적으로 개인용 미디어 기기(12)가 처음에 구성됨(이를 테면, 처음 개인용 미디어 기기(12)가 미디어 분배 시스템(18)과의 접속부를 수립했을 때)과 동시에 수행된다. 하기에 보다 자세히 기술되는 것처럼, DRM 프로세스(10)는 시스템적으로 그리고 반복적으로 기기(12)(및/또는 사용자(14))가 미디어 분배 시스템(18)의 가입자들이 실제 가입자임을 증명하기 위해 수행될 수 있다.

[0112] 또한 도 12a와 12b를 참조하면, 제조시, 개인용 미디어 기기(12)는 비휘발성 메모리(예, 롬(152) 및/또는 저장 기기(66))에 저장된 개인 암호키(예, 기기 암호키(400)) 및 공개 암호키(예, 기기 공개키(402))를 포함할 수 있다. 키들(400, 402)은 1024 비트의 비대칭 암호키들일 수 있으며 DRM(이를 테면, 디지털 저작권 관리) 키들로 불릴 수 있다.

[0113] 당해 기술에 공지된 바와 같이, 개인키/공개키 암호화 방식은 불안전한 네트워크(예, 인터넷)의 사용자들이 한 쌍의 암호화 키들, 즉 개인 암호키(예, 기기 암호키(400)) 및 공개 암호키(예, 기기 암호키(402))의 사용을 통해 데이터를 안전하게 교환하도록 한다. 개인키/공개키 암호화 방식은 일반적으로, 메세지를 암화화하기 위해 사용된 키가 상기 메시지를 판독하기 위해 사용된 키와 다른, 비대칭 암호화 방식으로 지칭된다.

[0114] 개인키/공개키 암호화에 있어서, 상기 개인 암호키(예, 기기 개인키(400)) 및 공개 암호키(예, 기기 공개키(402))는 일반적으로 동일한 알고리즘(예, Ron Rivest, Adi Shamir, 및 Adlemana에 의해 창조된 RSA 알고르즘)을 사용하여 동시에 생성된다. 기기 개인키(400)는 일반적으로 요구 당사자(requesting party)에게만 주어지며 기기 공개키(402)는 (디지털 인증서(404)의 일부로서) 공개적으로 이용가능하게 만들어진다. 일반적으로, 기

기 공개키(400)는 공유하지 않으며 예를 들면, 개인용 미디어 기기(12) 내에 안전하게 보존된다.

[0115] 따라서, 안전 메세지가 전송자에서 수신자에게로 전송될 때, (상기 전송자에게 반복적으로 접근가능한) 상기 수신자의 공개키(예, 기기 공개키(402))는 상기 메세지를 암호화하는데 사용된다. 일단 암호화되면, 상기 메세지는 상기 수신자에게 전송될 수 있으며 상기 수신자의 개인키(예, 기기 개인키(400))만을 사용하여 판독될 수 있다. 개인키(400)는 상기 수신자에 의해 안전하게 보존되므로, 상기 수신자만이 암호화된 메세지를 판독할 수 있다.

[0116] 메세지 암호화 및 판독하는 것에 추가로, 전송자는 디지털 인증서를 암호화하기 위해 그들의 개인키(예, 기기 개인키(400))를 사용하여 그들의 신원을 인증할 수 있으며, 그 후 수신자(이를 테면, 수신자가 그들의 신원을 인증하고 있는 사람)에게 전송된다. 따라서, 상기 디저털 인증서가 상기 수신자에 의해 수신될 때, 상기 수신자는 상기 전송자의 공개키(예, 기기 공개키(402))를 사용하여 암호화된 디지털 인증서를 판독할 수 있으며, 상기 디지털 인증서가 상기 전송자의 개인키(예, 기기 개인키(400))를 사용하여 암호화되는 것을 증명하고, 이에 따라, 상기 전송자의 신원을 증명하게 된다.

[0117] DRM 프로세스(10)는 챌린지(challenge)(406)를 생성할 수 있는 것으로서, 일반적으로 개인용 미디어 기기(12) 내에 포함된 랜덤 번호 생성 프로세스(도시하지 않음)에 의해 생성된 램덤 번호이다. 일단 생성되면, 챌린지(406)는 라이센스 요청(408)을 생성하기 위해 (일반적으로 기기 공개키(402)를 포함하는) 기기 디지털 인증서(404)와 쌍(pair)이 될 수 있다. DRM 디지털 인증서로서 불릴 수 있는, 기기 디지털 인증서(404)는 예를 들면, 기기 일련번호(예, 도 9의 기기 일련번호 필드(322)로부터의 137660523-1)와 같은 그러한 추가 정보를 포함할 수 있다.

[0118] 상기에 논의된 바와 같이, 프록시 어플리케이션(98)은 기기(12)의 소유자(예, 사용자(14))가 미디어 분배 시스템(18)과의 사용을 위해 기기(12)를 구성하고 기기(12)와의 사용을 위해 미디어 분배 시스템(18)을 구성하도록 한다. 일반적으로, 프록시 어플리케이션(98)이 프록시 컴퓨터(54)상에 구성될 때, 사용자(14)는 사용자(예, 사용자(14))의 신원을 밝히고 사용자(14), 기기(12), 및 프록시 어플리케이션(98)이 미디어 분배 시스템(18)에 접근하도록 하는 유효한 가입을 규정하는 사용자 인증서들을 제공하도록 요구될 수 있다. 대안적으로 또는 추가로, 개인용 미디어 기기(12)는 상기 사용자(예, 사용자(14))가 기기(12)가 처음에 구성될 때 (기기(12)를 통해) 상기 사용자 인증서들을 직접 등록하도록 구성될 수 있다.

[0119] DRM 프로세스(10)는 미디어 분배 시스템(18)에 (네트워크(30) 및/또는 네트워크(32)를 통해) 라이센스 요청(408)을 제공할 수 있다(452). 추가로, 개인용 미디어 기기(12) 내에 규정되면, (예, 상기에 설명된 사용자 인증서들을 열거하는) 사용자 ID(410)는 또한 라이센스 요청(408) 내에 포함될 수 있다. 상기에 논의된 바와 같이, (이를 테면, 사용자 ID(410) 내에 포함된) 상기 사용자 인증서들은 사용자 이름, 사용자 비밀번호, 사용자 키, 기기 이름, 기기 비밀번호, 기기 키, 및/또는 하나 이상의 디지털 인증서들을 포함할 수 있으나, 이에 국한되지 않는다. 미디어 분배 시스템(18)에 분배되기(452) 전에, DRM 프로세스(10)는 기기 개인키(400)를 사용하여 라이센스 요청(408)에 디지털적으로 서명(454)할 수 있다.

[0120] 디지털 서명은 (상기에 설명한) 개인키/공개키 암호화 방법을 사용하여 메세지의 전송자가 그들의 신원과 전송된 메세지의 무결성(integrity)을 인증하도록 하는 전자 서명이다. 디지털 서명은 암호화 및 비암호화 메세지 모두에 사용될 수 있으며 상기 메시지를 판독하기 위해 상기 메세지의 수신자의 성능에 장애가 되지 않는다.

[0121] 예를 들어, DRM 프로세스(10) 미디어 분배 시스템(18)에 라이센스 요청(408)을 제공(452)하기 전에 라이센스 요청(408)에 디지털적으로 서명되었다(454)고 가정하자. 라이센스 요청(408)에 디지털적으로 서명(454)할 때, 수학적 기능은 일반적으로 라이센스 요청(408)의 콘텐츠 상에 수행된다. 예를 들어, 라인센스 요청(408)의 메시지 해시(hash)는 개인용 미디어 기기(12)에 의해 계산될 수 있으며, 그러한 메세지 해시는 문자열(예, 라이센스 요청(408))을 원시 문자열을 나타내는 대개 더 짧은 고정-길이 값으로 변형하는 공지된 한 방법의 해시 기능의 수학적 산출물이다. 해싱 기능이 수학적 기능의 한 방법이므로, 일단 메세지 해시가 생성되면, 원시 메시지는 상기 메세지 해시를 프로세싱함으로써 회수될 수 없다. DRM 프로세스(10)는 그 후 상기 디지털 서명(도지되지 않음)을 생성하기 위해 (기기 개인키(400)를 사용하여) 상기 메세지 해시를 암호화할 수 있다. 이러한 디지털 서명은 그 후 라이센스 요청(408)에 첨부될 수 있다. 따라서, 상기 디지털 서명이 암호화되는 동안, 상기 원시 메세지(이를 테면, 라이센스 요청(408))는 필요 없다. 그러므로, 라이센스 요청(408)은 상기 디지털 서명이 프로세스되지 않는 경우에도 미디어 분배 시스템(18)에 의해 프로세스될 수 있다.

[0122] 상기에 설명된 예에 계속이어, 라이센스 요청(408) 및 디지털 서명은 미디어 분배 시스템(18)에 의해 수신될 수

있으며, 미디어 분배 시스템(18)은 라이센스 요청(408)의 메세지 해시를 생성하기 위해 동일한 해시 기능을 사용할 수 있다. 미디어 분배 시스템(18)은 또한 개인용 미디어 기기(12)에 의해 계산된 메세지 해시를 재생성하기 위해 (기기 디지털 인증서(404) 내에 포함된) 기기 공개키(402)를 사용하여 개인용 미디어 기기(12)로부터 수신된 디지털 서명을 판독할 것이다. 미디어 분배 시스템(18)은 그 후 상기 미디어 분배 시스템(408)에 의해 계산된 메세지 해시와 판독된 디지털 서명을 비교할 수 있다. 상기 메세지 해시들이 일치한다면, 라이센스 요청(408)의 무결성 및 개인용 미디어 기기(12)의 무결성은 모두 검증된다(456).

[0123] 추가로, 기기 디지털 인증서(404)의 무결성(및 이에 따른, 기기 공개키(402))는 라이센스 요청(408)이 개인용 미디어 기기(12)로부터 수신될 때 검증될 수 있다. 디지털 인증서들은 일반적으로 발행되고 CA 개인키(414)를 사용하여 예를 들면, 인증 기관(412)에 의해 디지털적으로 서명된다. 따라서, 기기 디지털 인증서(404)는 기기 디지털 인증서(404)의 디지털 서명을 검증하기 위해 상기 CA 공개키(416)을 획득함으로써 검증될 수 있다.

[0124] 일단 챌린지(406), 기기 디지털 인증서(404), 및 사용자 ID(410)(이를 테면, 라이센스 요청(408))가 미디어 분배 시스템(18)에 의해 수신될 때, 미디어 분배 시스템(18)은 사용자(14)(이를 테면, 사용자 ID(410) 내에 규정된 사용자)에 관한 가입 정보를 획득하기 위해(458) 데이터 기억장치(418)에 접근할 수 있으며 예를 들면, 현재 사용자(14)의 가입이 만료될 시점의 날짜를 결정할 수 있다. 데이터 기억장치(418)는 컴퓨터(28)에 커플된 저장 기기(34) 상에 보존될 수 있다.

[0125] 예시를 위해, 미디어 분배 시스템(18)이 다가오는 달에 대한 가입비에 대해 각 달의 첫째 날에 각 가입자에게 자동으로 청구되도록 구성된다고 가정하자. 따라서, 2005년 3월 1일, 사용자(14)는 그 2005년 3월 가입비가 청구될 것이다. 그러므로, 미디어 분배 시스템(18)이 2005년 3월 6일 사용자(14)에 관한 가입 정보를 획득한다면(458), 획득된 상기 가입 정보(458)는 사용자(14)가 2005년 3월 31일까지 유효한 가입을 갖는다는 것을 나타낼 것이다.

[0126] 따라서 상기 설명된 예에 계속하여, 라이센스 요청(408)이 수신될 때, 미디어 분배 시스템(18)은 사용자(14)에 관한 가입 정보를 획득할 것이다(458). 이 예에서, 상기 가입 정보는 사용자(14)가 2005년 31일 내내 (미디어 분배 시스템(18)에 대한) 유효한 가입자임을 나타낼 것이다.

[0127] 미디어 분배 시스템(18)은 타임아웃 표시기(420)를 생성할 수 있으며, 이는 예를 들어, 사용자의 가입 정보 및 상기 사용자의 현재 가입의 만료일을 나타낸다. 이 예에서, 타임아웃 표시기(420)는 예를 들면, 사용자(14)의 가입이 2005년 3월 31일에 만료할 것임을 나타낼 것이다. 미디어 분배 시스템(18)은 데이터 기억장치(418)로부터 사용자 암호키(422)(이를 테면, 사용자(14)에 대한 암호키)를 획득할 수 있다. 미디어 분배 시스템(18)은 그 후 암호화된 사용자 암호키(422')(해시 충전으로 도시됨)를 생성하기 위해, 기기 공개키(402)를 사용하여, 사용자 암호키(422)를 암호화할 수 있다. 타임아웃 표시기(420), 챌린지(406), (기기 공개키(402)를 포함하는) 기기 디지털 인증서(404), 사용자 ID(410), 및 암호화된 사용자 암호키(422')는 기기 라이센스(424)를 형성하기 위해 (미디어 분배 시스템(18)에 의해) 결합될 수 있다(462).

[0128] 기기 라이센스(424)는 미디어 분배 시스템(18)에 의해 규정된 것과 같은 시스템 타임을 표시하는, 시스템 타임 표시기(426)를 더 포함할 수 있다. 시스템 타임 표시기(426)는 개인용 미디어 기기(12) 내에 포함된 시스템 클록(194)(도 3)과 미디어 분배 시스템(18) 내에 포함된 시스템 클록(428)을 동조시키는데 사용될 수 있다.

[0129] 기기 라이센스(424)는 일반적으로 라이센싱 서비스(이를 테면, LS) 공개키(432)를 포함하는, 라이센싱 서비스(이를 테면, LS) 디지털 인증서(430)를 더 포함할 수 있다.

[0130] 미디어 분배 시스템(18)은 (미디어 분배 시스템(18)의) 라이센싱 서비스(이를 테면, LS) 개인키(434)를 사용하여 기기 라이센스(424)에 디지털적으로 서명할 수 있으며(464) 개인용 미디어 기기(12)에 기기 라이센스(424)를 제공할 수 있다(466). 라이센싱 시스템 개인키(434)는 데이터 기억장치(418)상에 저장될 수 있다.

[0131] 기기 라이센스(424)가 미디어 분배 시스템(18)으로부터 수신될 때, DRM 프로세스(10)는 LS 디지털 인증서(430)(및, 이에 따른 LS 공개키(432))의 무결성을 검증할 수 있다. 상기에 논의된 바와 같이, 디지털 인증서들은 CA 개인키(414)를 사용하여 예를 들면, 인증 기관(412)에 의해 일반적으로 발행되어 디지털적으로 서명된다.

[0132] DRM 프로세스(10)는 (LS 개인키(434)를 사용하여 디지털적으로 서명되는) 기기 라이센스(424)를 검증하기 위해 (LS 디지털 인증서(430)에 포함된) LS 공개키(432)를 사용할 수 있다. DRM 프로세스(10)는 기기 라이센스(424)가 개인용 미디어 기기(12)용으로 되는 것을 보장하기 위해 (기기 디지털 인증서(404) 내에 포함된) 챌린지 값(406), 기기 공개키(402), 및 기기 일련번호를 추가로 검증할 수 있다. DRM 프로세스(10)는 그 후 기기 개인키(400), (기기 공개키(402)를 사용하여 암호화되는) 암호화된 사용자 암호키(422')를 판독할 수 있는 것으로, 비

휘발성 메모리에 저장될 수 있으며, 비휘발성 메모리의 예들로 롬(152)(도 3) 및/또는 저장 기기(66)(도 3)를 포함할 수 있다. 사용자 ID(410), 사용자 암호화 키(422), 및 타임아웃 표시기(420)는 개인용 미디어 기기(12)가 미디어 분배 시스템(18)으로부터 다운로드된 미디어 콘텐츠를 렌더링할 때 사용을 위해, 예를 들면, 비휘발성 메모리 상에 저장될 수 있으며, 그 예들로 롬(152)(도 3) 및/또는 저장 기기(66)(도 3)를 포함할 수 있다. 추가로, 하기에 더 자세히 논의될 것처럼, DRM 프로세스(10)는 개인용 미디어 기기(12)와 예를 들면 개인용 미디어 기기(40) 사이에 미디어 콘텐츠를 전송할 때 사용을 위해 기기 라이센스(424)의 사본을 보유할 수 있다.

[0133] **가입형 미디어 콘텐츠 획득:**

[0134] 상기에 논의된 바와 같이, 일단 사용자(14)가 미디어 분배 시스템(18)에 가입하면, 사용자(14)는 다음의 형태로 (개인용 미디어 기기(12)에 사용을 위해) 미디어 분배 시스템(18)으로부터 미디어 콘텐츠를 획득할 수 있다: 미디어 분배 시스템(18)으로부터 수신된 구매형 다운로드들(이를 테면 영구적 사용을 위한, 예를 들면, 사용자(14)에게 허락된 미디어 콘텐츠); 미디어 분배 시스템(18)으로부터 수신된 가입형 다운로드들(이를 테면, 유효한 가입이 미디어 분배 시스템(18)에 존재하는 동안 사용을 위해, 예를 들면, 사용자(14)에게 허락된 미디어 콘텐츠); 및 미디어 분배 시스템(18)으로부터 스트리밍된 미디어 콘텐츠.

[0135] 또한 도 13a 및 13b를 참조하면, 미디어 분배 시스템(18)으로부터 다운로드 가능한 각 미디어 데이터 파일(500, 502, 504, 506, 508)은 유일한 CEK(이를 테면, 콘텐츠 암호화 키)(510, 512, 514, 516, 518)를 각각 사용하여 암호화될 수 있다(550). 예를 들면, 미디어 분배 시스템(18)이 예를 들어, 개인용 미디어 기기(12)로의 다운로딩을 위해 이용가능한 1,000,000개의 미디어 데이터 파일들을 포함할 수 있다면, 미디어 분배 시스템(18)은 유일한 암호화 키를 사용하여 각 미디어 데이터 파일을 암호화할 것이다(550). 따라서, 1,000,000개의 미디어 데이터 파일들을 위해, 1,000,000개의 유일한 CEK가 요구될 것이며, 그 각각은 상기 CEK가 관련되는 상기 미디어 데이터 파일로 바인딩된다(is bound). 따라서, CEK(510)는 예를 들면, 미디어 데이터 파일(500)로 바인딩 될 수 있으며(552), CEK(512)는 미디어 데이터 파일(502)로 바인딩 될 수 있다(552).

[0136] 각 CEK(예, 키들(510, 512, 514, 516, 518)는 대칭 암호화 키일 수 있으며, 즉 미디어 데이터 파일을 암호화하는데 사용된 상기 키는 동일한 미디어 데이터 파일을 판독하는데 또한 사용될 수 있다. 일반적으로, 각 미디어 데이터 파일은 예를 들면, 컴퓨터(28)에 부착된 저장 기기(34)상에 저장될 수 있다.

[0137] 상기에 논의된 바와 같이, 프록시 어플리케이션(98)의 검색창(304)(도 10)은 사용자(14)가 미디어 데이터 파일들에 대해 검색하도록 할 수 있다. 추가로, 사용자(14)는 다운로드 될 상기 미디어 데이터 파일에 해당하는 다운로드 버튼(3 52)(도 10)을 선택함으로써 개인용 미디어 기기(12) 상에 사용을 위해 미디어 분배 시스템(18)으로부터 미디어 데이터 일들을 다운로드 할 수 있다.

[0138] 일단 미디어 데이터 파일의 다운로드가 초기화되면, 개인용 미디어 기기(12)는 미디어 분배 시스템(18)에 적절한 다운로드 요청(들)을 제출할 수 있다. 예를 들면, 사용자(14)가 세 개의 미디어 데이터 파일들, 즉 미디어 데이터 파일들(520, 522, 524)을 다운로드하고자 한다고 가정하자. DRM 프로세스(10)는 다운로드 요청들(520, 522, 524)을 각각 제출할 것이며, 그 각각은 바람직한 파일을 요청한다. 안전하고 인증을 위해, 다운로드 요청들(520, 522, 524)은 (예를 들면, LS 공개키(432)를 사용하여) 개인용 미디어 기기(12)에 의해 예를 들면, 암호화 될 수 있으며 및/또는 (기기 개인키(400)를 사용하여) 개인용 미디어 기기(12)에 의해 디지털적으로 서명될 수 있다. 따라서, (예를 들어, LS 공개키(432)를 사용하여) 다운로드 요청이 암호화되면, 상기 암호화된 다운로드 요청은 이어 LS 개인키(434)를 사용하여 미디어 분배 시스템(18)에 의해 판독될 수 있다(554). 또한, (기기 개인키(400)을 사용하여) 다운로드 요청이 디지털적으로 서명되면, 상기 서명된 다운로드 요청은 이어 기기 공개키(402)를 사용하여 미디어 분배 시스템(18)에 의해 검증될 수 있다(556).

[0139] 일단 예를 들어, 미디어 분배 시스템(18)에 의해 다운로드 요청들(520, 522, 524)이 수신되고(558) 프로세스되며(554, 556), 미디어 분배 시스템(18)은 예를 들어, 저장 기기(34)로부터 요청된 미디어 데이터 파일들(500, 504, 506)을 회수할 수 있다. 상기에 논의된 바와 같이, 각 미디어 데이터 파일은 유일한 CEK를 사용하여 쉽게 암호화되어, 상기 CEK는 상기 미디어 데이터 파일로 바인딩 된다.

[0140] 개인용 미디어 기기(12)로 다운로드 되기 전에, 다운로드 될 각 미디어 데이터 파일은 상기 다운로드를 요청한 사용자(예, 사용자(14))에게 바인딩 될 수 있다(560). 상기에 논의된 바와 같이, 기기 초기화 동안, 개인용 미디어 기기(12)는 미디어 분배 시스템(18)에 라이센스 요청(408)을 제공한다. 미디어 분배 시스템(18)은 차례로 라이센스 요청(408)을 프로세스하고 상기 라이센스 요청(408)(예, 사용자(14))와 연관된 사용자에 관한 현재 가입 정보를 획득한다. 상기에 논의된 바와 같이, 이러한 초기화 과정은 주기적으로 일어날 수 있으며, 그에

따라, 개인용 미디어 기기(12)가 도킹 크레이들(60)(도 2)로 배치됨과 동시에 일어날 수 있다. 따라서 예를 들면, 개인용 미디어 기기(12)가 미디어 분배 시스템(18)에 적절히 접근하기 위해 요구된 사용자 인증들을 제공했다고 가정하자. 상기에 논의된 바와 같이, 미디어 분배 시스템(18)에 제공된 사용자 인증들은 사용자 이름, 사용자 비밀번호, 사용자 키, 기기 이름, 기기 비밀번호, 기기 키, 및/또는 하나 이상의 디지털 인증서들을 포함할 수 있으나, 이에 국한되지 않는다.

[0141] 일단 미디어 분배 시스템(18)이 예를 들면, 저장 기기(34)로부터 요청된 미디어 데이터 파일들(500, 504, 506)을 회수하면, 미디어 분배 시스템(18)은 예를 들면 상기 미디어 데이터 파일들을 요청하는 사용자(14)에게 상기 회수된 미디어 분배 파일들(500, 504, 506)을 바인딩 하며(560), 이로써 바인딩 된 미디어 파일들(526, 528, 530)을 생성한다. 따라서, 각 미디어 데이터 파일(예, 미디어 데이터 파일(500))과 관련된 콘텐츠 암호화 키(예, CEK(510))는 상기 미디어 데이터 파일들을 요청하는 사용자(예, 사용자(14))의 상기 암호화 키(예, 사용자 암호화 키(422))를 사용하여 암호화될 수 있다(562). 따라서, CEK(510)는 CEK(510')를 생성하기 위해 암호화될 수 있으며(562), CEK(514)는 CEK(514')를 생성하기 위해 암호화될 수 있다(562). 일단 암호화되면(562), (암호화된 CEK들(510', 514', 516') 각각 포함하는) 바인딩 된 미디어 데이터 파일들(526, 528, 530)은 개인용 미디어 기기(12)로 제공될 수 있다(564).

[0142] 각 바인딩 된 미디어 데이터 파일(526, 528, 530)의 CEK가 예를 들면 사용자 암호화 키(422)를 사용하여 암호화될 수 있기 때문에, 바인딩 된 미디어 데이터 파일들(526, 528, 530)은 단지 사용자 암호화 키(422)를 소유하는 개인용 미디어 기기에 의해 프로세스 될(예를 들면, 렌더링 될) 수 있다. 상기에 논의된 바와 같이, 사용자 암호화 키(422)의 사본은 개인용 미디어 기기(12) 내 비휘발성 메모리 상에 저장될 수 있다. 일단 바인딩 된 미디어 데이터 파일들(526, 528, 530)이 개인용 미디어 기기(12)에 의해 수신되면, 파일들(526, 528, 530)은 개인용 미디어 기기(12) 내에, 예를 들면 저장 기기(66) 상에 저장될 수 있다.

[0143] **가입형 미디어 콘텐츠 재생:**

[0144] 상기에 논의된 바와 같이, 사용자 ID(410), 사용자 암호화 키(422), 및 타임아웃 표시기(420)는 개인용 미디어 기기(12)가 미디어 분배 시스템(18)으로부터 다운로드 된 미디어 콘텐츠를 렌더링할 때 사용을 위해 저장될 수 있다.

[0145] 상기 설명된 예들에 계속하여, 사용자(14)가 바인딩 된 미디어 데이터 파일들(526, 528, 530) 중 하나를 렌더링하기 원한다면, 사용자(14)는 개인용 미디어 기기(12)의 제어들(예를 들면, 뒤로 건너뛰기 스위치(78)(도 3); 앞으로 건너뛰기 스위치(86)(도 3); 재생/정지 스위치(82)(도 3); 메뉴 스위치(84)(도 3); 라디오 스위치(86)(도 3); 및 슬라이더 어셈블리(88)(도 3)) 및 재생 패널(90)(도 3)을 통해 적절한 미디어 데이터 파일을 선택할 수 있다. 일단 하나 이상의 미디어 데이터 파일들이 재생을 위해 선택되면, 적절한 파일(들)은 예를 들면, 저장 기기(66)로부터 회수된다. 상기에 논의된 바와 같이, 개인용 미디어 기기(12)에 제공되어 있는 각 미디어 파일은 사용자 암호화 키(422)를 사용하여 (미디어 분배 시스템(18)에 의해) 암호화될 수 있다. 상기에 논의된 바와 같이, 사용자 암호화 키(422)는 대칭 암호화 키일 수 있으며, 그에 따라, CEK(510)를 암호화하는데 사용된 키는 또한 암호화된 CEK(510')을 판독하는데 사용될 수도 있다.

[0146] 일단 적절한 바인딩 된 미디어 데이터 파일들이 예를 들면, 저장 기기(66)로부터 회수된다면, DRM 프로세스(10)는 상기 미디어 데이터 파일이 개인용 미디어 기기(12) 상에 프로세스 되고 렌더링 될 수 있도록 (사용자 암호화 키(422)를 사용하여) 적절한 CEK를 판독할 수 있다. 예를 들면, 사용자(14)가 바인딩 된 미디어 데이터 파일들(526, 528)을 렌더링하기 원한다면, 개인용 미디어 기기(12)는 CEK(510)를 생성하기 위해 암호화된 CEK(510')를 판독할 것이다. CEK(510)은 그 후 개인용 미디어 기기(12)에 의한 재생을 위해 미디어 데이터 파일(500)을 판독하는 DRM 프로세스(10)에 의해 사용될 수 있다. 또한, DRM 프로세스(10)는 CEK(514)를 생성하기 위해 암호화된 CEK(514')를 판독할 것이다. CEK(514)는 그 후 개인용 미디어 기기(12)에 의한 재생을 위해 미디어 데이터 파일(504)을 판독하기 위한 DRM 프로세스(10)에 의해 사용될 수 있다.

[0147] 일반적으로, 예를 들어, 바인딩 된 미디어 데이터 파일들(526, 528)을 프로세싱하고 렌더링하기 전에, DRM 프로세스(10)는 예를 들어, 사용자(14)가 상기 바인딩 된 미디어 데이터 파일들을 프로세스하고 렌더링하기에 충분한 권한을 갖는다는 점을 검증할 것이다.

[0148] 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 일반적으로 가입-기반 서비스로서, 즉 예를 들면, 사용자(14)가 미디어 분배 시스템(18)에 가입하고 미디어 분배 시스템(18)으로의 접근이 인가되도록 예를 들면, 매달 가입비를 지불한다. 또한, 사용자(14)가 미디어 분배 시스템(18)으로부터 사용자(14)가 유효한 가입이 미디어

분배 시스템(18)에 존재하는 동안만 가입형 다운로드들을 프로세스하고 재생하도록 하는 다운로드들을 획득할 수 있다.

[0149] 바인딩 된 미디어 데이터 파일들(526, 528, 530)을 렌더링 및/또는 프로세싱하기 전에, 바인딩 된 미디어 데이터 파일들(526, 528, 530)이 (사용자(14)에 의한 사용을 위해 영구히 허락되는 구매형 다운로드들에 상반되는 것으로서) 가입형 다운로드인 것으로 가정하면, DRM 프로세스(10)는 상기에 논의된 바와 같은, 예를 들어, 비휘발성 메모리 상에 저장될 수 있는, 타임아웃 표시기(420)를 획득할 수 있으며, 비휘발성 메모리의 예들로 롬(152)(도 3) 및/또는 저장 기기(66)(도 3)를 포함할 수 있다. DRM 프로세스(10)는 그 후 예를 들어, 사용자(14)가 여전히 바인딩 된 미디어 데이터 파일들(526, 528, 530)을 렌더링하도록 허용되는지를 결정하기 위해 시스템 클록(194) 내에 규정된 날짜 및/또는 시간에 대한 타임아웃 표시기(420) 내의 규정된 만료일(예, 2005년 3월 31일)을 비교할 수 있다. 이 실시예에서, 사용자(14)가 2005년 3월 31일 내내 유효한 가입을 갖고 (시스템 클록(194)에 의해 규정된 바와 같은) 현재 날짜 및 시간이 2006년 3월 6일 17시 53분 GMT이므로, (미디어 분배 시스템(18)에 관한) 사용자(14)의 가입은 현재 유효하다. 따라서, 바인딩 된 미디어 데이터 파일들(526, 528, 530)은 재생을 위해 프로세스 될 수 있다.

[0150] 상기에 논의된 바와 같이, DRM 프로세스(10)는 기기(12)(및/또는 사용자(14))가 미디어 분배 시스템(18)의 실제 가입자들임을 검증하기 위해 시스템적으로 그리고 반복적으로 수행될 수 있다. 예를 들어, DRM 프로세스(10)는 개인용 미디어 기기(12)가 도킹 크레이들(60)로 배치되는 각 시간에 수행될 수 있다. DRM 프로세스(10)는 미디어 분배 시스템(18)에 (네트워크(30) 및/또는 네트워크(32)를 통해) 라이센스 요청(408)을 제공할 수 있다(452). 라이센스 요청(408) 수신시, 미디어 분배 시스템(18)은 타임아웃 표시기(420)를 포함하여, 사용자(14)에 관한 가입 정보를 획득할 수 있다(458).

[0151] 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 다가오는 달에 대한 가입비에 대한 각 달의 첫째 날에 각 가입자에게 자동으로 청구되도록 구성될 수 있다. 따라서, 개인용 미디어 기기(12)가 도킹 크레이들(60)로 배치되는 각 시간, 업데이트된 가입 정보(예, 타임아웃 표시기)는 미디어 분배 시스템(18)으로부터 획득될 수 있다. 따라서, 사용자(14)가 예를 들어, 그들의 매달 가입비들을 계속 지불하도록 제공되면, 개인용 미디어 기기(12)는 현재 타임아웃 표시기를 포함하기 위해 계속 시스템적으로 업데이트 되도록 할 것이다.

[0152] 하지만, 이러한 실시예에서, 가입 정보(예, 타임아웃 표시기)는 단지 개인용 미디어 기기(12)가 크레이들(60)로 배치될 때만 업데이트 된다. 따라서, 사용자(14)가 그들의 예를 들어, 매달 가입비들을 계속 지불하도록 하더라도, 예를 들어, 2005년 3월 31일(이를 테면, 현재 타임아웃 표시기의 날짜) 전에 개인용 미디어 기기(12)가 크레이들(60)로 배치되지 않는다면, 개인용 미디어 기기(12)는 (개인용 미디어 기기(12)가 기한이 없는 타임아웃 표시기를 획득될 수 없으므로) 유효한 현재 가입을 가질지라도 2005년 3월 31일 이후 미디어 데이터 파일들을 렌더링하는 것이 금지될 수 있다.

[0153] **기기-대-기기 미디어 콘텐츠 전송:**

[0154] 상기에 논의된 바와 같이, 미디어 분배 시스템(18)은 일반적으로 가입-기반 서비스, 즉, 예를 들어, 사용자(14)가 미디어 분배 시스템(18)에 가입하여 미디어 분배 시스템(18)으로의 접근을 인가되도록 예를 들면, 매달 가입비를 지불하는, 서비스이다. 또한, 사용자(14)는 미디어 분배 시스템(18)으로부터 사용자(14)가 유효한 가입이 미디어 분배 시스템(18)에 존재하는 동안만 가입형 다운로드들을 프로세스 하고 재생하도록 하는 가입형 다운로드들을 획득할 수 있다. 따라서, 가입형 다운로드에 연관된 권한들은 미디어 분배 시스템(18)에 유효한 가입의 존재에 기초되며, 가입형 다운로드들은 제2 개인용 미디어 기기에 관한 유효 가입이 존재하는 한, 제1 개인용 미디어 기기에서 제2 미디어 기기로 전송될 수 있다.

[0155] 또한 도 14a 및 14b를 참조하고 상기 설명된 예에 계속하여, 사용자(14)가 개인용 미디어 기기(12) 내에 예를 들면, 저장 기기(66)에 저장되는 바인딩 된 미디어 데이터 파일들(526, 528, 530)을 다운로드했다고 가정하자. 또한, 사용자(26)(이를 테면, 개인용 미디어 기기(40)의 소유자)가 개인용 미디어 기기(40)상에 재생을 위해 바인딩 된 미디어 데이터 파일(526)의 사본을 획득하기를 원한다고 가정하자. 상기에 논의된 바와 같이, 기기가 초기화되면, 기기 라이센스의 사본은 개인용 미디어 기기들 간에 미디어 콘텐츠 전송시 사용을 위한 상기 개인용 미디어 기기상에 전송되고 보유될 수 있다. 따라서, 개인용 미디어 기기(12)는 소스(source) 기기 라이센스(424)를 포함하며 개인용 미디어 기기(40)는 타겟(target) 기기 라이센스(600)를 포함한다.

[0156] 일반적으로, 기기-대-기기 콘텐츠 전송은 상기 소스 기기의 사용자에 의해 초기화된다. 상기-설명된 실시예에서, 개인용 미디어 기기(12)는 소스 기기이며 개인용 미디어 기기(40)는 타겟 기기이다. 따라서, 사용

자(14)(이를 테면, 개인용 미디어 기기(12)의 소유자)는 개인용 미디어 기기(12)에서 개인용 미디어 기기(40)로의 바인딩 된 미디어 데이터 파일(526)의 전송을 초기화할 수 있다.

[0157] 다시 도 2를 참조하면, 예를 들어, 사용자(14)가 또 다른 개인용 미디어 기기로 미디어 데이터 파일을 전송하기를 원한다면, 사용자(14)는 예를 들어, 메뉴 스위치(84)를 누룰 수 있어, 그 결과 예를 들면, 팝-업 메뉴(106)의 생성을 초래한다. 슬라이더 어셈블리(88)를 사용하여, 사용자(14)는 팝-업 메뉴(106)로부터 "공유 콘텐츠" 커맨드를 선택할 수 있어, 그 결과 콘텐츠 창(110)의 생성을 초래한다. 콘텐츠 창(11)으로부터, 사용자(14)는 전송을 위한 적절한 파일을 선택할 수 있다. 사용자(14)가 바인딩 된 미디어 데이터 파일(526)에 해당하는 "Peggy Sue"를 선택한다고 가정하자. 일단 사용자(14)가 전송을 위해 트랙을 선택하면, 기기 어플리케이션(64)은 예를 들면, 전송되고 있는 트랙의 제목을 식별하는 트랙 제목 필드(114) 및 전송되고 있는 트랙의 아티스트를 식별하는 아티스트 필드(116)을 포함하는, 전송창(112)을 렌더링할 수 있다.

[0158] 전송창(112)은 예를 들어, 개인용 미디어 기기(40)에 바인딩 된 미디어 데이터 파일(526)의 전송을 초기화하기 위한 (슬라이더 어셈블리(88)를 통해 선택가능한) 전송 버튼(118)을 포함할 수 있다. 이 실시예에서, 사용자(14)가 슬라이더 어셈블리(88)로 된 전송 버튼(118)을 선택한다면, 개인용 미디어 기기(12)에서 (이 실시예에서) 개인용 미디어 기기(40)로 바인딩 된 미디어 데이터 파일(526)(이를 테면, "Buddy Holly"의 "Peggy Sue")의 전송이 초기화된다. 전송창(112)은 예를 들면, "Buddy Holly"의 "Peggy Sue"의 전송 과정을 표시하기 위한 전송 상태 표시기(120)를 포함할 수 있다. 전송창(112)은 사용자(14)가 상기 파일 전송을 취소하고 다운로드 창(112)을 닫도록 하는 취소 버튼(122)을 더 포함할 수 있다.

[0159] 다시 도 14a 및 14b를 참조하면, 일단 바인딩 된 미디어 데이터 파일(526)의 전송이 초기화되면, 상기 기기들은 인증을 위해 기기 디지털 인증서들을 교환할 수 있다. 예를 들면, DRM 프로세스(10)는 인증을 위해 개인용 미디어 기기(40)에 (소스 기기 공개키(402)를 포함하는) 소스 기기 디지털 인증서(404)를 제공할 수 있다. 일단 수신되면(650) 상기에 논의된 바와 같이, 소스 기기 디지털 인증서(404)(및, 그에 따른, 소스 기기 공개키(402))의 무결성은 소스 기기 디지털 인증서(404)가 발행되고 CA 개인키(414)(도 12a)를 사용하여 인증 기관(412)(도 12a)에 의해 디지털적으로 서명되므로, CA 공개키(416)(그 사본은 일반적으로 개인용 미디어 기기(40)의 비휘발성 메모리(602)에 저장됨)를 통해 (개인용 미디어 기기(40)에 의해) 검증될 수 있다(652).

[0160] 또한, 개인용 미디어 기기(40)는 인증을 위해 개인용 미디어 기기(12)에 (타겟 기기 공개키(606)를 포함하는) 타켓 기기 디지털 인증서(604)를 제공할 수 있다. 일단 수신되면(654), 타켓 기기 디지털 인증서(604)(및, 그에 따른, 타겟 기기 공개키(606))의 무결성은 타겟 기기 디지털 인증서(604)가 일반적으로 발행되었을 것이고 CA 개인키(414)(도 12 A)를 사용하여 예를 들면, 인증 기관(412)(도 12a)에 의해 디지털적으로 서명되었을 것이므로, CA 공개키(416)(그 사본은 일반적으로 개인용 미디어 기기(12)의 비휘발성 메모리(66/152)에 저장됨)를 통해 DRM 프로세스(10)에 의해 검증될 수 있다(656).

[0161] 상기에 논의된 바와 같이 도 3에 도시된 것처럼, 개인용 미디어 기기들(예, 개인용 미디어 기기(12))은 네트워크(30) (또는 네트워크(32)) 및/또는 개인용 미디어 기기들을 무선으로 커플링하기 위한 무선 인터페이스(182)를 포함할 수 있다. 무선 인터페이스(182)는 예를 들어, WAP(52)과의 RF 통신을 위한 안테나 어셈블리(184), 및/또는 (개인용 미디어 기기(40)와 같은) 제2 미디어 기기와의 적외선 통신을 위한 IR(이를 테면, 적외선) 통신 어셈블리(186)에 커플될 수 있다. 따라서, 개인용 미디어 기기들(12, 40) 사이의 통신은 RF 통신 및/또는 적외선 통신을 통해 무선으로 발생할 수 있다. 추가로, 외부 접속부(도시하지 않음)는 다수의 개인용 미디어 기기들의 하드웨어에 내장된 상호접속부를 허용하는 각 개인용 미디어 기기 내에 포함될 수 있다.

[0162] 일단 인증서들(404 및 604)이 검증되면(652, 656), 개인용 미디어 기기(40)는 개인용 미디어 기기(12)로 타켓 기기 라이센스(600)를 제공한다. 기기 라이센스(424)(도 12a)로서, 타켓 기기 라이센스(600)는 다음을 포함할 수 있다: (LS 공개키(432)를 포함하는) LS 디지털 인증서(608), 시스템 타임 표시기(612), (이를 테면, 사용자(26)의 가입에 대한) 타임아웃 표시기(614), (이를 테면, 사용자(26)를 위한) 암호화된 사용자 암호화 키(616), (이를 테면, 사용자(26)를 위한) 사용자 ID(618), 챌린지(620), 및 (타겟 기기 공개키(606)의 사본을 포함하는) 타겟 기기 디지털 인증서(604). 기기 라이센스(424)(도 12a)로서, 타켓 기기 라이센스(600)는 개인용 미디어 기기(40)로 제공되기 전에 (LS 개인키(434)를 사용하여 미디어 분배 시스템(18)에 의해) 디지털적으로 서명되었을 수 있다.

[0163] 개인용 미디어 기기(40)로부터 타겟 기기 라이센스(600) 수신시, DRM 프로세스(10)는 타겟 기기 라이센스(600)의 무결성을 검증할 수 있다(660). 따라서, DRM 프로세스(10)는 LS 디지털 인증서(608)(및, 그에 따른, LS 공개키(432))의 무결성을 검증할 수 있다. 상기에 논의된 바와 같이, 디지털 인증서들은 CA 개인키(414)(도 12a)를

사용하여 예를 들면, 인증 기관(412)(도 12a)에 의해 일반적으로 발행되고 디지털적으로 서명된다. 따라서, LS 디지털 인증서(608)는 CA 공개키(416)를 사용하여 DRM 프로세스(10)에 의해 검증될 수 있다.

[0164] DRM 프로세스(10)는 (LS 개인키(434)(도 12a)를 사용하여 디지털적으로 서명되는) 타켓 기기 라이센스(600)를 검증하기 위해 (LS 디지털 인증서(608) 내에 포함된) LS 공개키(432)를 사용할 수 있다. DRM 프로세스(10)는 추가로 사용자(26)가 신호를 획득하고(662) 시스템 클록(194)과 타임아웃 표시기(614)를 비교함으로써 미디어 분배 시스템(18)에 유효한 가입을 가지는 것을 검증할 수 있다(665). 예를 들면, 사용자(26)는 (타임아웃 표시기(614)에 규정된 바와 같은) 2005년 3월 22일 내내 유효한 가입을 가지고 (시스템 클록(194)에 의해 규정된 바와 같은) 현재 날짜 및 시간이 2005년 3월 13일 22시 06분 GMT이므로, (미디어 분배 시스템(18)에 대한) 사용자(26)의 가입은 현재 유효하다.

[0165] 타겟 기기 라이센스(600)의 무결성이 검증된다고 가정하면, 바인딩 된 미디어 데이터 파일(526)의 전송이 시작될 것이다. DRM 시스템(10)이 구성되는 방식에 따라, 사용자(26)는 개인용 미디어 기기(40)로 임의의 미디어 데이터 파일들의 전송, 또는 금지될 수 있는 그 밖의 전송을 초기화하기 전에 (미디어 분배 시스템(18)에) 현재 유효한 가입을 가지도록 요구될 수 있다. 하지만 상기에 논의된 바와 같이, 개인용 미디어 기기들은 미디어 데이터 파일들을 렌더링하기 전에 현재 유효한 가입의 존재를 확인하므로, 사용자(26)가 미디어 분배 시스템(18)에 현재 유효한 가입을 갖지 않을 동안 전송이 실시되더라도, 사용자(26)는 상기 전송된 미디어 데이터 파일들을 렌더링하는 것이 금지될 수 있을 것이다. 따라서, DRM 시스템(10)은, (상기에 논의된 바와 같은) 타겟 기기(40)가 사용자(26)가 현재 유효한 가입을 가질 때까지 상기 전송된 미디어 데이터 파일(들)을 렌더링하도록 허용되지 않을 것이므로, 사용자(26)가 현재 유효한 가입을 갖지 않더라도, 소스 기기(12)에서 타겟 기기(40)로 하나 이상의 미디어 데이터 파일들의 전송이 허용되도록 구성될 수 있다.

[0166] 추가로, 소스 기기(12)(및/또는 사용자(14))는 미디어 데이터 파일을 타겟 기기(40)로 전송하도록 허용되기 전에 현재 유효한 가입을 갖도록 요구될 수 있다. 따라서, 미디어 데이터 파일을 전송하기 전에, 소스 기기(12)는 사용자(14)가 현재 유효한 가입을 갖는다는 것을 검증하기 위해 그들 자체의 타임아웃 표시기(이를 테면, 도 12a의 타임아웃 표시기(420))를 검사할 수 있다. 대안적으로/추가로, 타켓 기기(40)는 소스 기기(12)의 타임아웃 표시기(420)가 상기 미디어 데이터 파일이 전송되기 전에 검증될 수 있도록 기기 라이센스(424)를 (소스 기기(12)로부터) 수신하고 프로세스 할 수 있다.

[0167] 상기 미디어 데이터 파일 전송을 실시하기 위해, DRM 프로세스(10)는 랜덤 세션 키(이를 테면, (random session key:RSK)(622)를 생성하며(668), 암호화된 RSK(622')를 생성하기 위해 (타켓 기기 디지털 인증서(604) 내에 포함된) 타겟 기기 공개키(606)를 사용하여 암호화될 수 있다. DRM 프로세스(10)는 개인용 미디어 기기(40)로 암호화된 RSK(622')를 제공하고(670), RSK(622)를 회수하기 위해 (타겟 기기 개인키(도시하지 않음)를 사용하여) 판독될 수 있다. RSK(622)는 1024-비트의 대칭 암호화 키일 수 있다.

[0168] 개인용 미디어 기기(12) 및 개인용 미디어 기기(40) 각각은 RSK(622)의 사본을 보유하므로, 보안 통신 채널(624)이 기기들(12, 14) 간에 수립될 수 있으며(672), 보안 통신 채널(624)을 거쳐 그 안에 전송된 모든 데이터는 전송 전에 (RSK(622)를 사용하여) 암호화될 수 있으며(674) 수신시 (RSK(622)를 사용하여) 판독될 수 있다. 보안 통신 채널(624)은 (예를 들면, RF 통신 및/또는 적외선 통신을 사용하는) 무선 통신 채널, 또는 (기기들(12, 40) 상의 외부 접속기(도시하지 않음)를 사용하는) 유선 통신 채널일 수 있다.

[0169] DRM 프로세스(10)는 개인 미디어 기기(40)로 전송을 위해 바인딩 된 미디어 데이터 파일(526)을 (예를 들면, 저장 기기(66)로부터) 회수할 수 있다. 하지만 상기에 논의된 바와 같이, 바인딩 된 미디어 데이터 파일(526)의 CEK(510')이 사용자(12)의 암호화 키(예, 사용자 암호화 키(422))를 사용하여 암호화되기 때문에, 바인딩 된 미디어 데이터 파일(526)은 사용자(26)에 의해 (그 현재 형태로) 접근가능하지 않을 것이다. 그러므로, 바인딩 된 미디어 데이터 파일(526)은 사용자(12)로부터 바인딩 해제하여(676) 사용자(26)에 바인딩 되어야 한다. 따라서, DRM 프로세스(10)는 예를 들면, 저장 기기(66)로부터 바인딩 된 미디어 데이터 파일(526)을 획득하고 CEK(510)를 획득하기 위해 (사용자 암호화 키(422)를 사용하여) CEK(510')를 판독한다. 바인딩 해제된 미디어 데이터 파일(626)은 (보안 통신 채널(624)을 통해) 개인용 미디어 기기(12)에서 개인용 미디어(40)로 전송될 수 있다(678). 수신시, 개인용 미디어 기기(40)는 암호화된 CEK(510'')를 포함하는, 바인딩 된 미디어 데이터 파일(630)을 생성하기 위해 사용자(26)의 암호화 키(이를 테면, 사용자 암호화 키(628))를 사용하여, 바인딩 해제된 미디어 데이터 파일(626)의 CEK(510)를 암호화할 수 있다(680). 개인용 미디어 기기(40)는 비휘발성 메모리(602)에 연이은 렌더링을 위해 바인딩 된 미디어 데이터 파일(630)을 저장할 수 있다.

[0170] 사용자 암호화 키(422)는 일반적으로 대칭 암호화 키로 존재하는 것으로서, 즉 CEK를 암호화하는데 사용될 수

있는 동일한 키가 상기 CEK의 암호화된 버전을 판독하는데 또한 사용될 수도 있음이 상기에 설명된다. 또한 상기에 설명된 바와 같이, 동일한 사용자 암호화 키(422)는 모든 CEK들을 암호화하는데 사용될 수 있다. 그러므로, 100개의 바인딩 된 미디어 데이터 파일들이 개인용 미디어 기기(12)에 다운로드 되어 저정된다면, 동일한 사용자 암호화 키(422)는 각각의 상기 100개의 암호화된 CEK들 판독하는데 사용될 수 있다. 하지만, 사용자 암호화 키(422)의 다른 구성들이 가능하다.

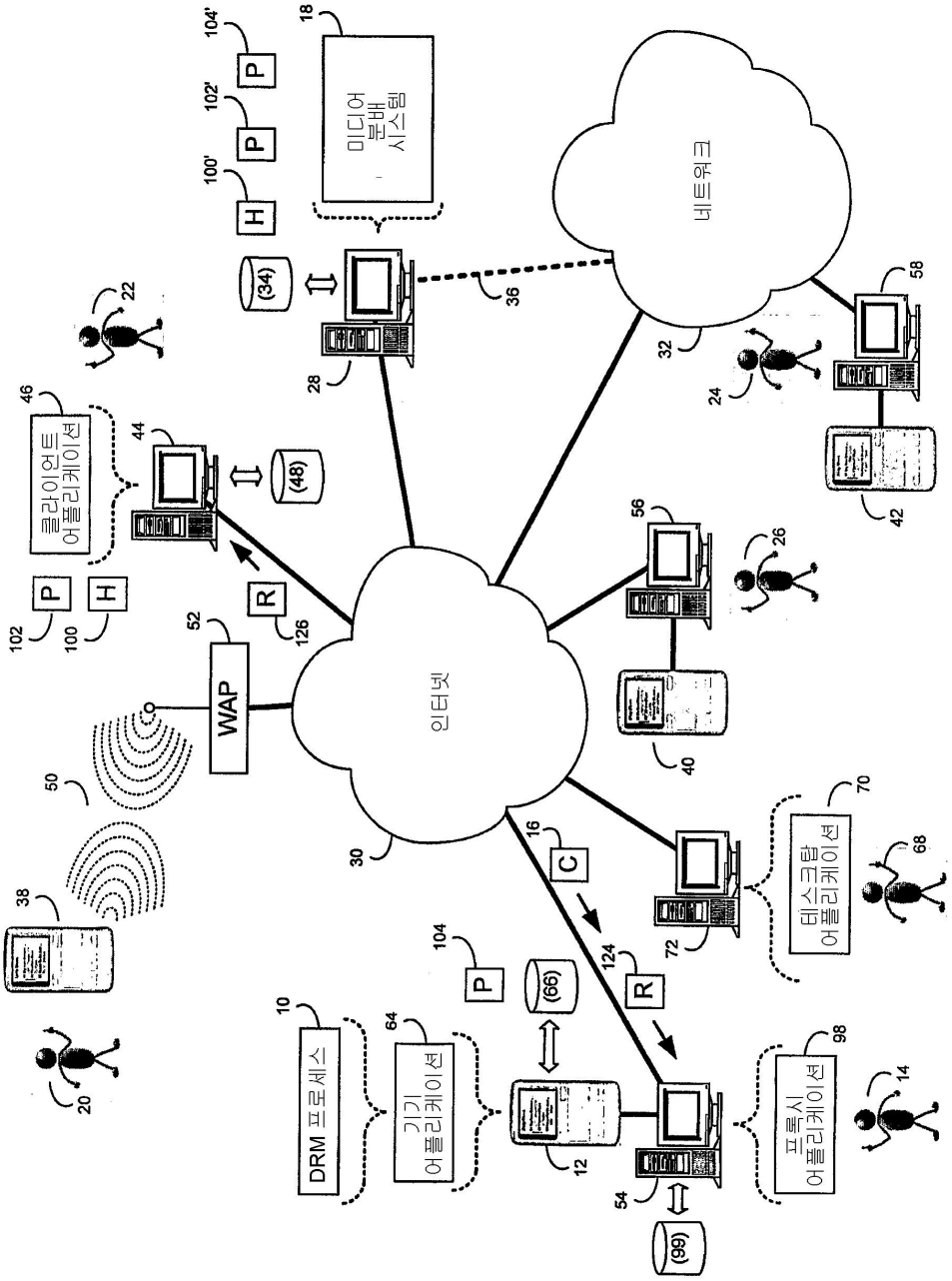
[0171] 예를 들면, 사용자 암호화 키(422)는 단일 대칭 키에 상반되는 것으로서, 대칭 키 블록일 수 있다. 또한 도 15를 참조하면, 32-바이트(이를 테면, 256-비트) 대칭 키 블록(700)이 도시된다. 상기 실시예를 위해 16-바이트(이를 테면, 128-비트) 키는 각 암호화된 CEK를 암호화하고 판독하는데 사용된다. 예를 들어, 256-비트 대칭 키 블록(700)의 한 사용을 통해, 다중의 128-비트 대칭 키들(예, 사용자 암호화 키들(702, 704, 706, 708))이 규정될 수 있다. 예를 들어, 제1 사용자 암호화 키(702)가 대칭 키 블록(700)의 비트들(000-127)로 규정될 수 있다. 제2 사용자 암호화 키(704)는 대칭 키 블록(700)의 비트들(004-131)로 규정될 수 있다. 제3 사용자 암호화 키(706)는 대칭 키 블록(700)의 비트들(128-255)로 규정될 수 있다. 그리고 제4 사용자 암호화 키(708)는 대칭 키 블록(700)의 비트들(124-251)로 규정될 수 있다. 따라서, 다수의 유일한 대칭 사용자 암호화 키들은 단일 대칭 키 블록(700)을 사용하여 규정될 수 있다. 따라서, 초기 사용자 암호화 키들을 적절히 규정하기 위해, 비트 시프트 파라미터(710)는 각 키의 시작점을 규정하는, 각 사용자 암호화 키(702, 704, 706, 708)를 위해 규정될 수 있다. 예를 들면, 사용자 암호화 키(702)는 대칭 키 블록(700)의 비트-0에서 시작하고, 이에 따라, 0-비트의 비트 시프트(710)를 갖는다. 사용자 암호화 키(704)는 대칭 키 블록(700)의 비트-4에서 시작하므로, 사용자 암호화 키(704)는 4-비트의 비트 시프트(710)를 갖는다. 사용자 암호화 키(706)는 대칭 키 블록(700)의 비트-128에서 시작하므로, 사용자 암호화 키(706)는 128-비트의 비트 시프트(710)를 갖는다. 사용자 암호화 키(708)는 대칭 키 블록(700)의 비트-124에서 시작하므로, 사용자 암호화 키(708)는 124-비트의 비트 시프트(710)를 갖는다.

[0172] 다양한 사용자 암호화 키들은 각 개별 사용자 암호화 키의 시작점을 시프팅함으로써 대칭 키 블록(700) 내에 규정되나, 다른 구성들이 가능하다. 예를 들면, 키들은 비트 시프트와 관련하여 단지 홀수 또는 짝수만을 사용하여 규정될 수 있다. 추가로 및/또는 대안적으로, 키들은 대칭 키 블록(700) 내에 알고리즘적으로 규정될 수 있으며, 즉 알고리즘은 유일한 사용자 암호화 키를 규정하기 위해 (대칭 키 블록(700) 내에) 사용된 개별 비트들을 규정하는데 사용될 수 있다.

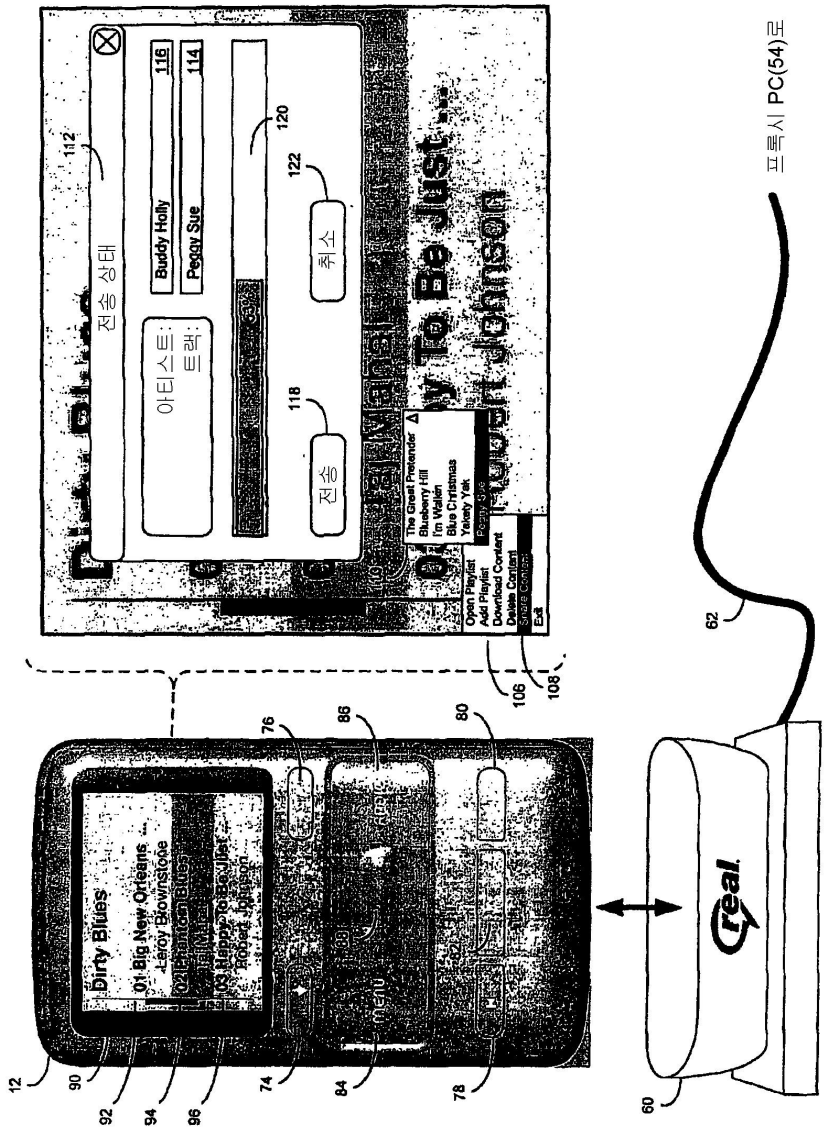
[0173] 많은 구현예들이 설명되었다. 그럼에도 불구하고, 다양한 변형이 있을 수도 있음이 이해될 것이다. 따라서, 다른 구현예들이 하기 청구항들의 범위 내에 있다.

도면

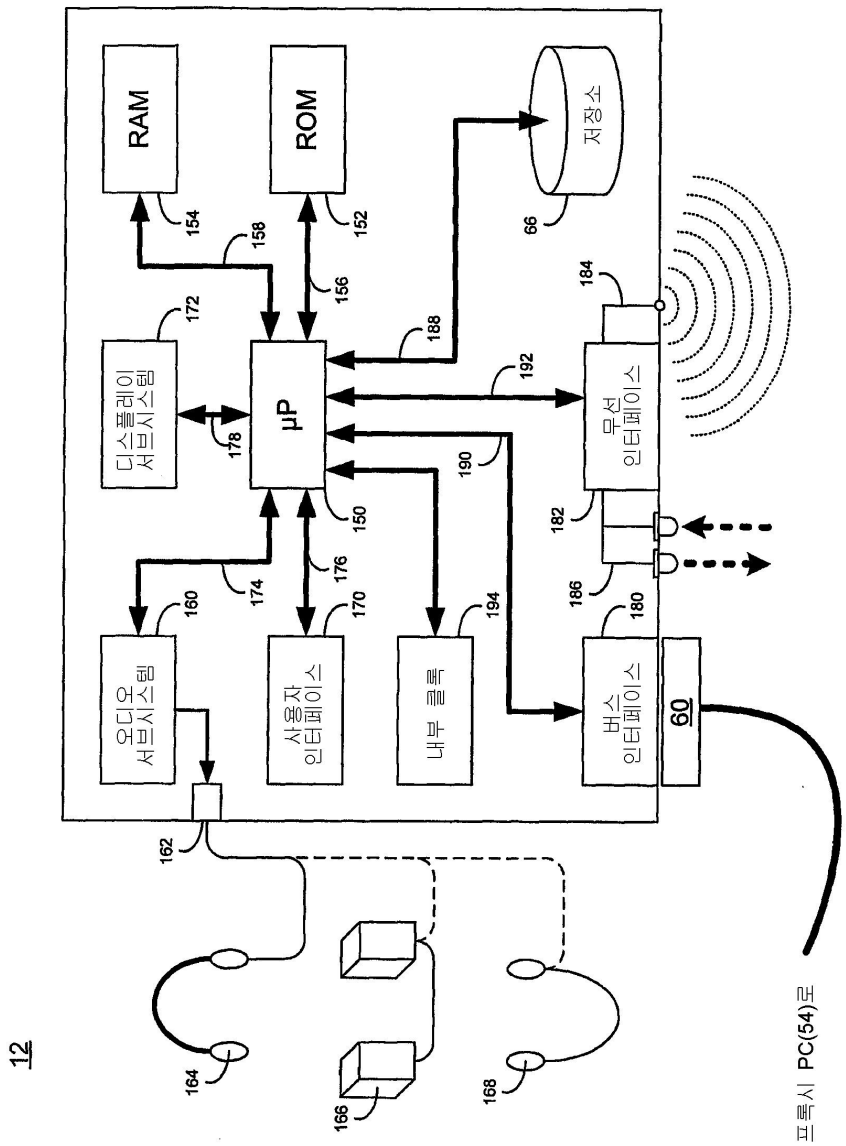
도면1


미디어 분배 시스템
네트워크
인터넷
WAP
클라이언트 어플리케이션
DRM 프로세스
기기 어플리케이션
데스크탑 어플리케이션
프록시 어플리케이션
P
H
R
C

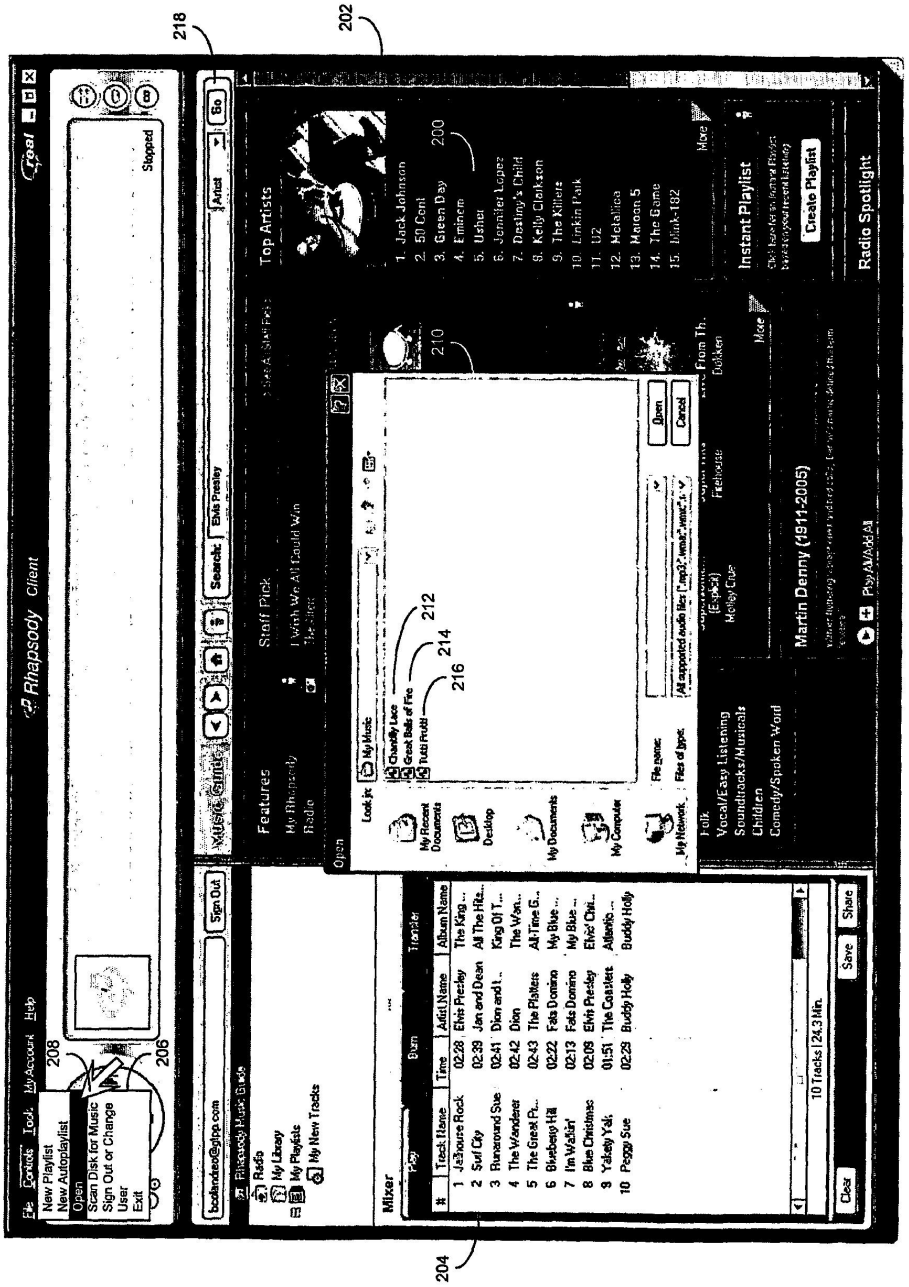
도면2


프록시 PC(54)로
전송 상태
아티스트:
트랙:
Buddy Holly
Peggy Sue
취소
전송
Dirty Blues
01 Big New Orleans ...
Leroy Brownstone
Menu
Real
12
60
62
74
76
78
80
84
86
90
92
94
96
106
108
112
114
116
118
120
122

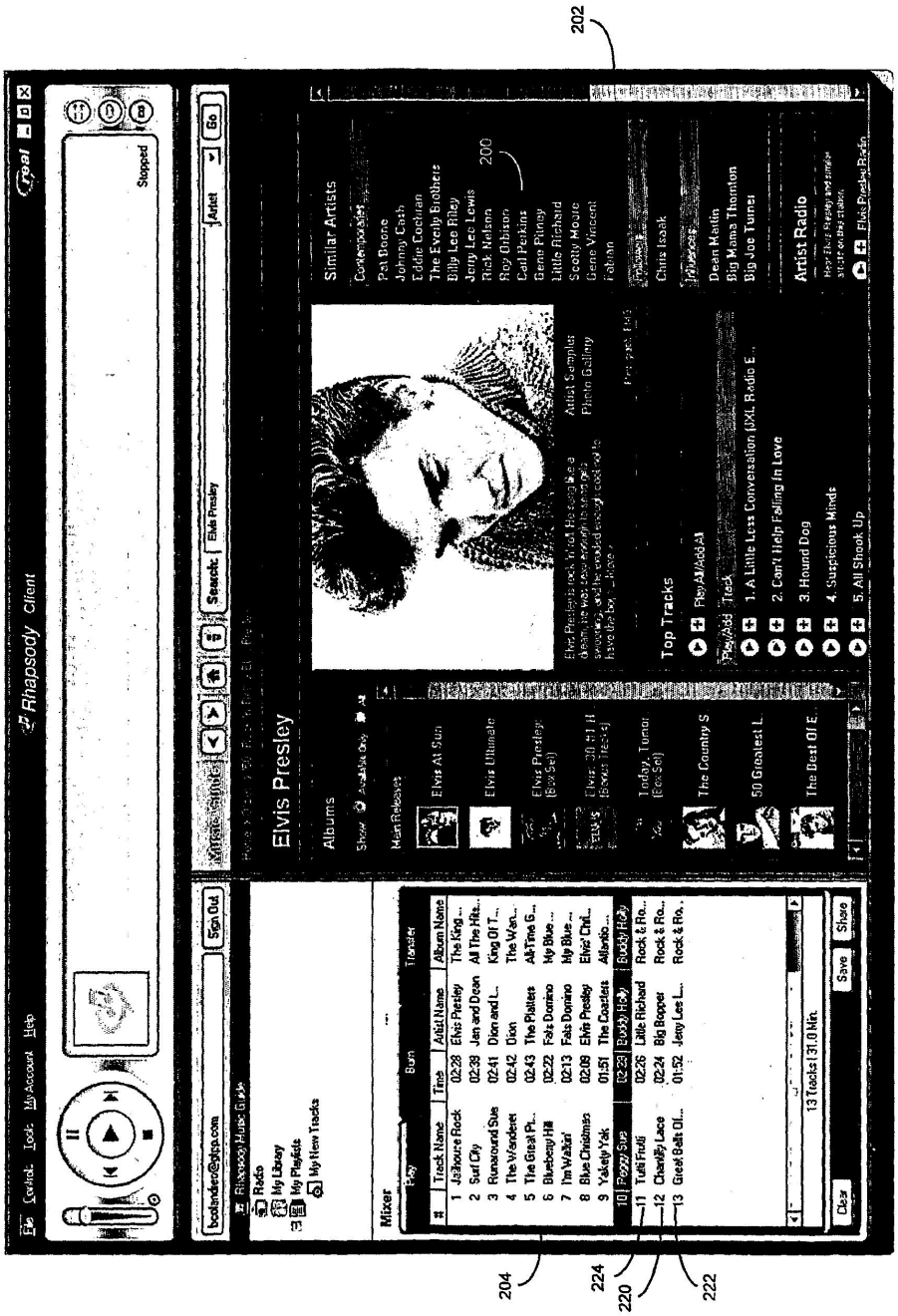
도면3


12
RAM
ROM
저장소
154
158
152
156
66
172
188
184
디스플레이
서브시스템
μP
192
무선
인터페이스
178
190
150
182
174
176
186
160
170
194
180
오디오
서브시스템
사용자
인터페이스
내부 클록
버스
인터페이스
60
162
164
166
168
프록시 PC(54)로

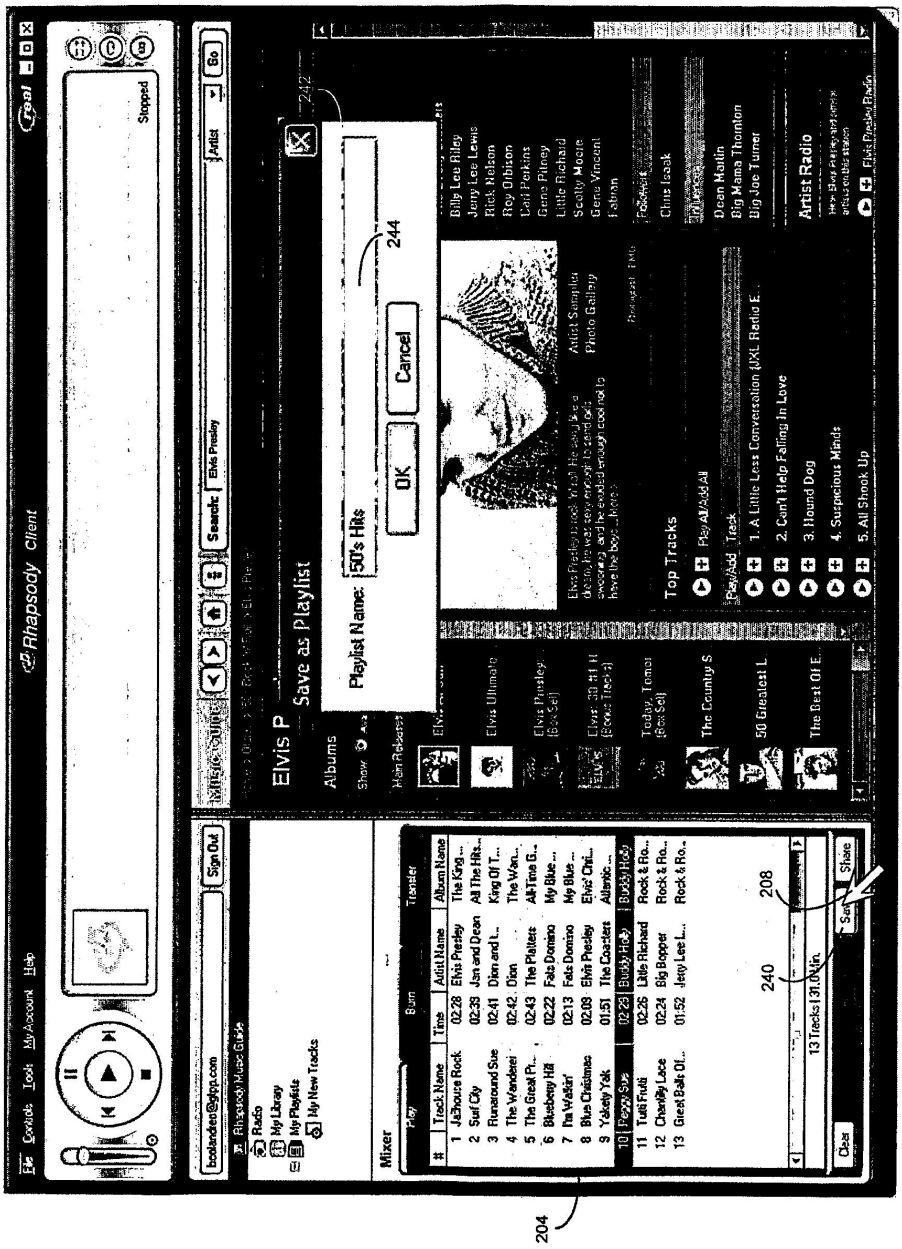
도면4


218
202
208
206
204
200
210
212
214
216
Rhapsody Client
Features
Staff Pick
Top Artists
Mixer
Instant Playlist
Radio Spotlight
Martin Denny (1911-2005)
Create Playlist

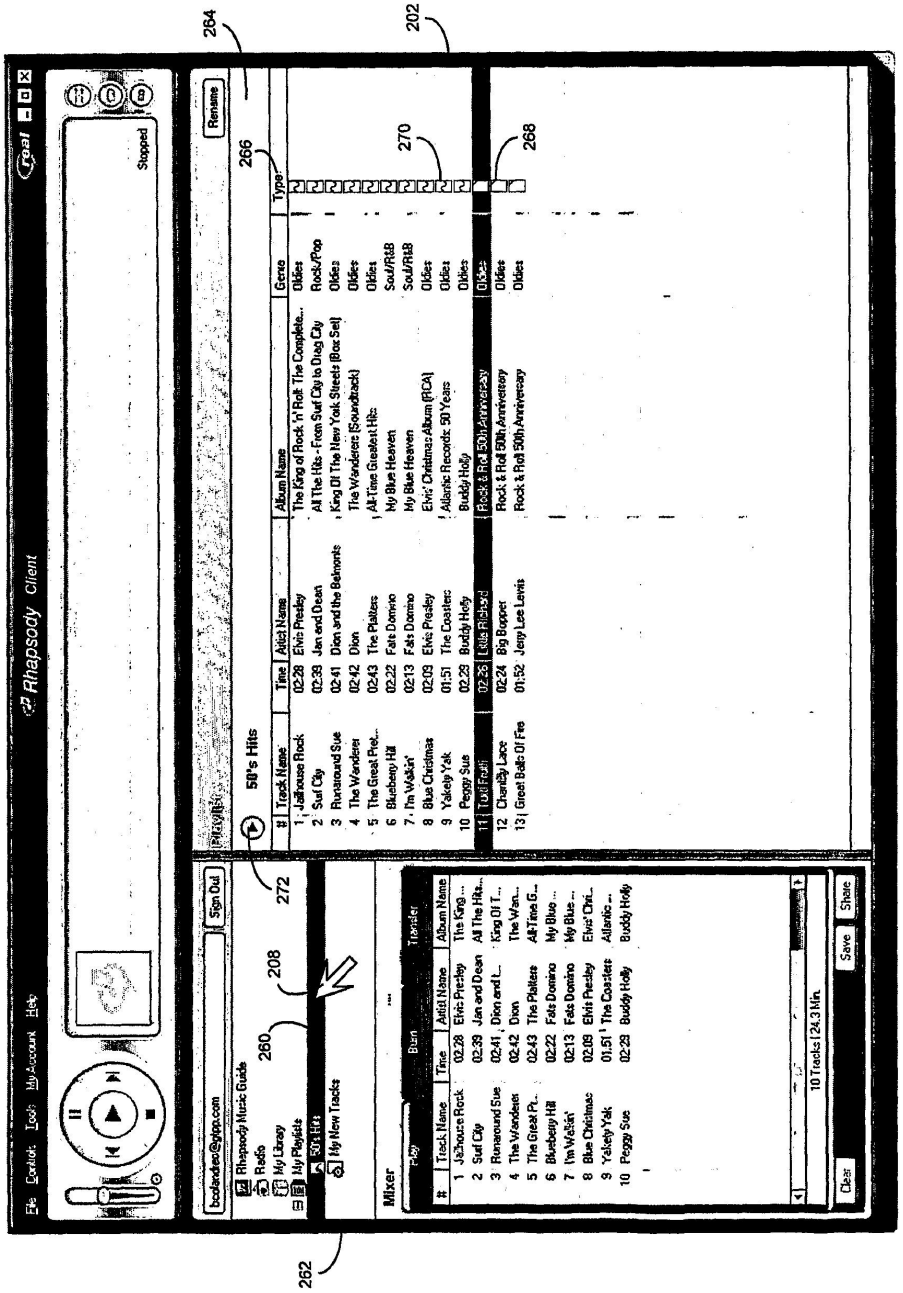
도면5


202
200
204
224
220
222
Rhapsody Client
Elvis Presley
Albums
Similar Artists
Top Tracks
Artist Radio
Mixer

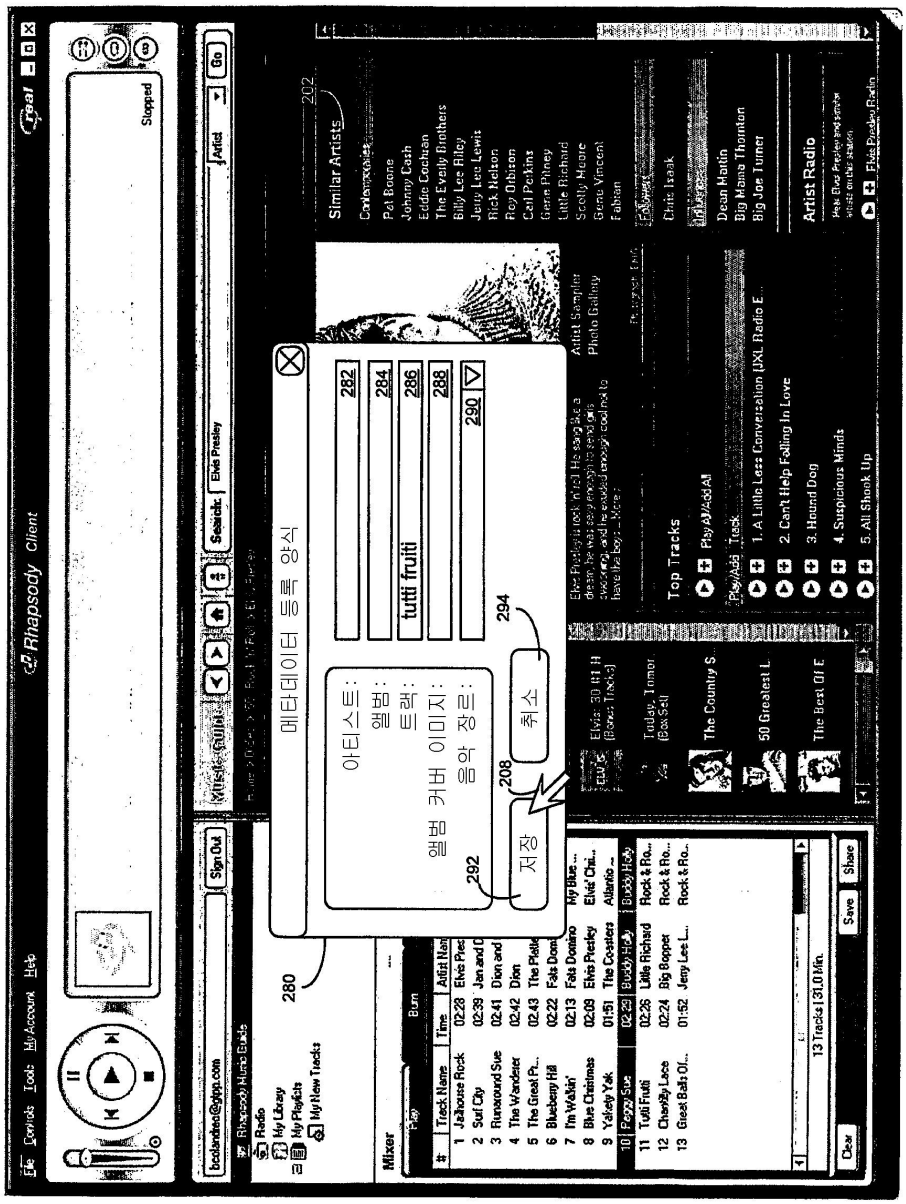
도면6


Rhapsody Client
Elvis P
Save as Playlist
Albums
Playlist Name:
50's Hits
OK
Cancel
244
242
Top Tracks
Artist Radio
Mixer
Play
Burn
Transfer
Track Name
Time
Artist Name
Album Name
13 Tracks | 31.0Mb
240
208
204

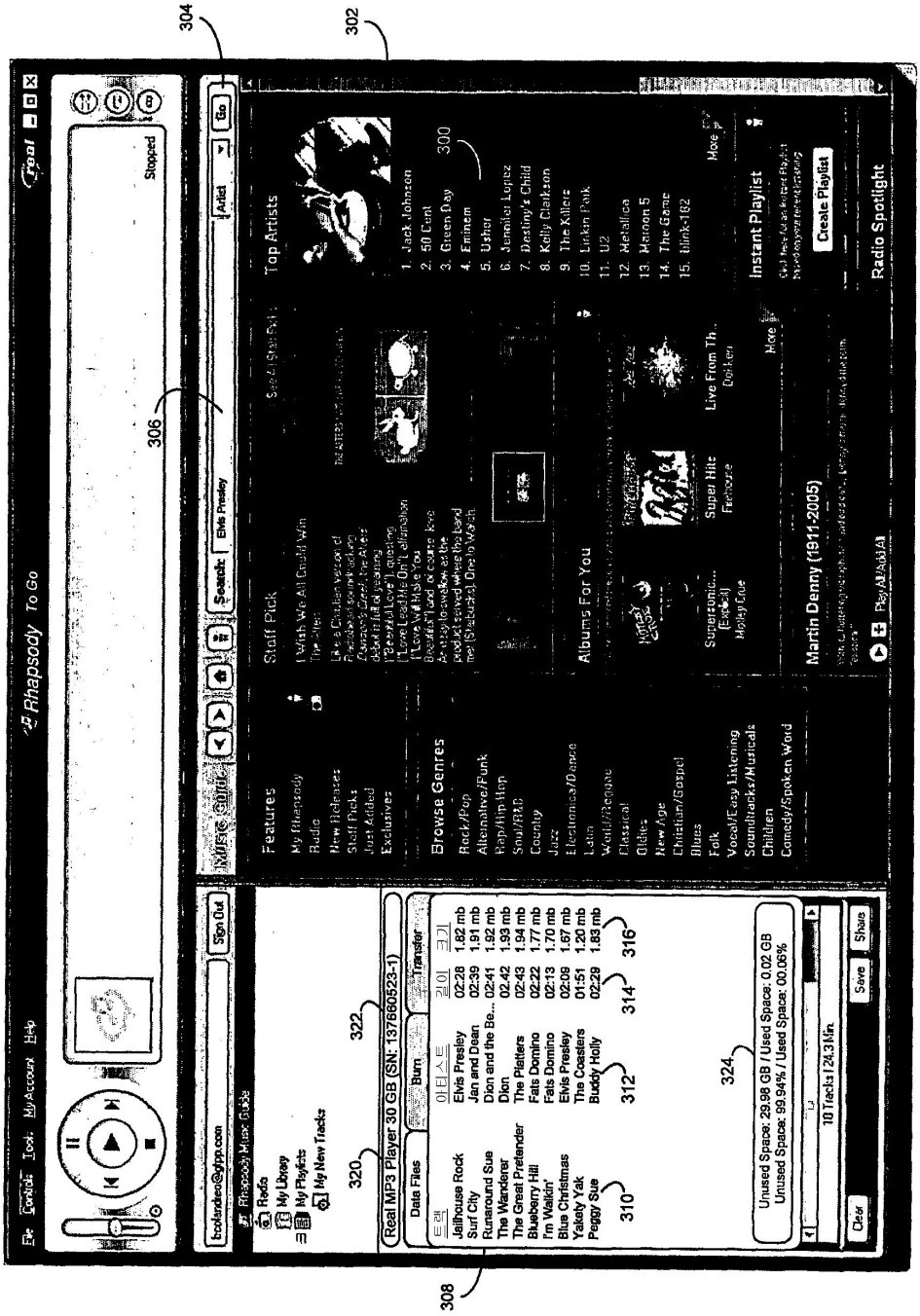
도면7


264
202
266
270
268
262
260
208
272
Rhapsody Client
50's Hits
Rhapsody Music Guide
Radio
My Library
My Playlists
My New Tracks
Mixer
Burn
Transfer
Clear
Save
Share
10 Tracks | 24.3 Min

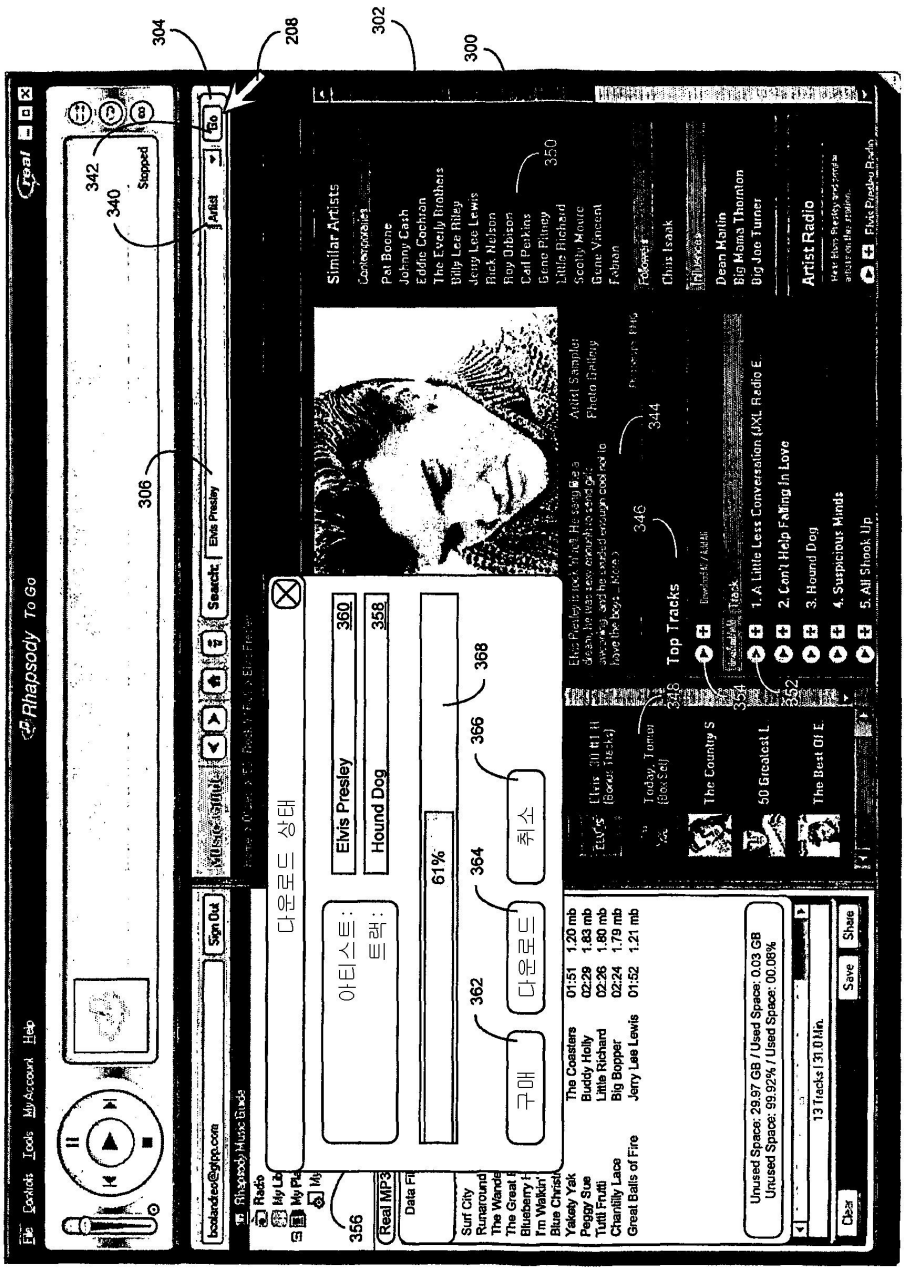
도면8


메타데이터 등록 양식
아티스트:
앨범:
트랙:
앨범 커버 이미지:
음악 장르:
tutti fruiti
280
282
284
286
288
290
292
294
208
저장
취소

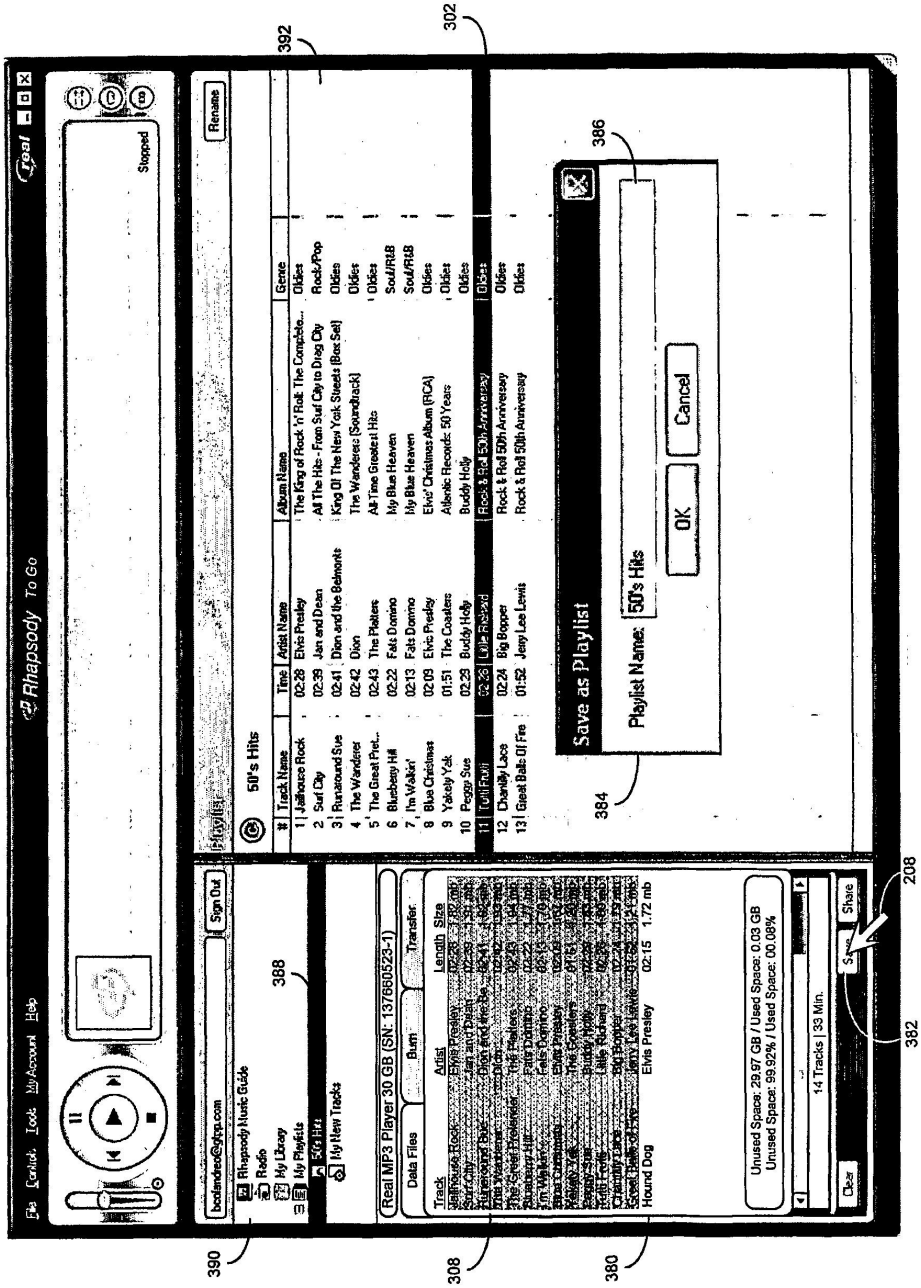
도면9


304
302
306
308
320
322
310
312
314
316
324
300
Rhapsody To Go
Features
Staff Pick
Top Artists
Browse Genres
Albums For You
Instant Playlist
Radio Spotlight
Martin Denny (1911-2005)
Create Playlist
Real MP3 Player 30 GB (SN: 137660523-1)
Data Files
Burn
Transfer
Unused Space: 29.98 GB / Used Space: 0.02 GB
Unused Space: 99.94% / Used Space: 00.06%
10 Tracks | 24.3 Min.
Clear
Save
Share

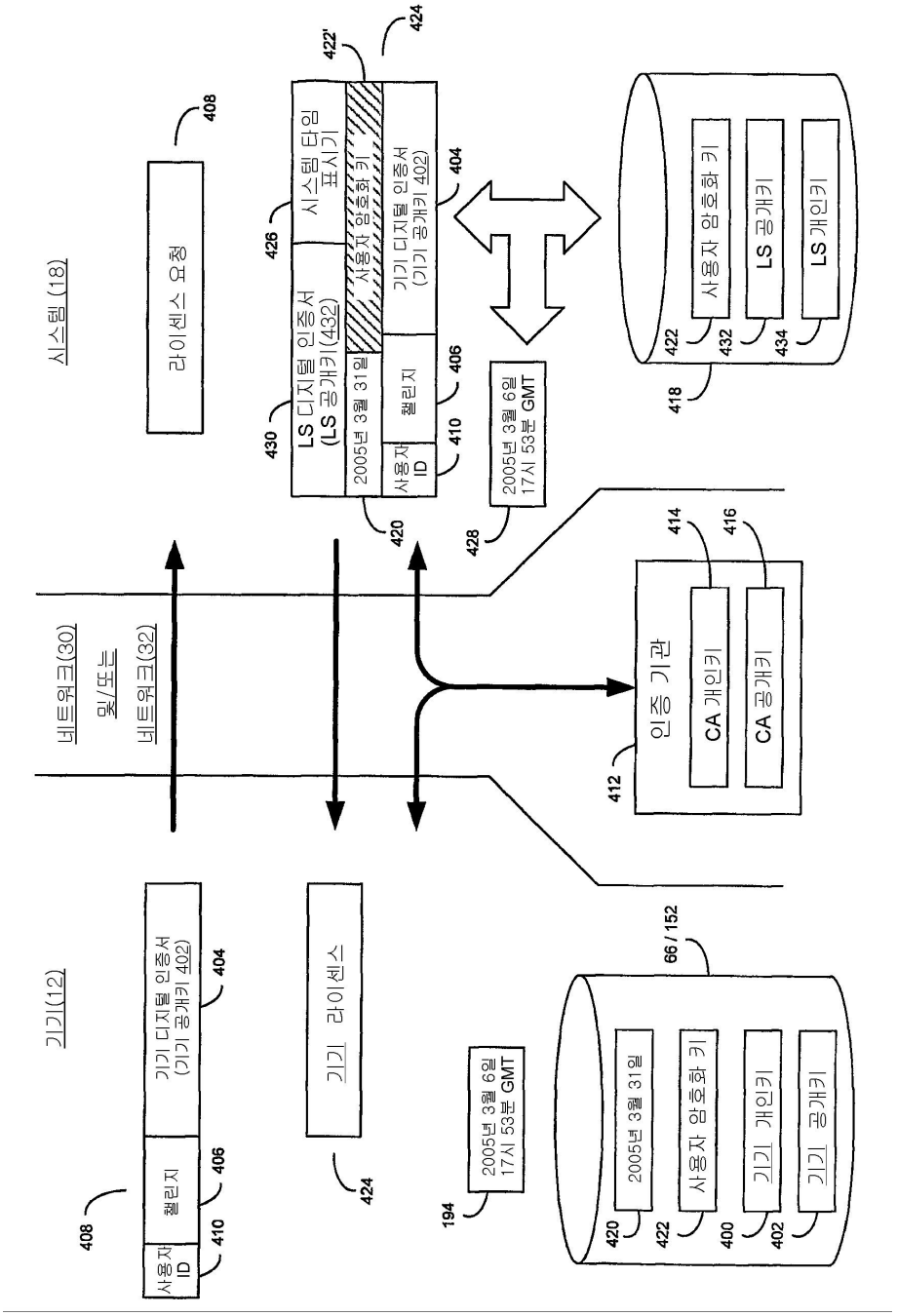
도면10


304
208
302
300
342
340
306
356
362
364
366
368
360
358
344
346
350
Rhapsody To Go
Stopped
Elvis Presley
다운로드 상태
아티스트:
트랙:
Hound Dog
61%
구매
다운로드
취소
Top Tracks
Similar Artists
Artist Radio
Pat Boone
Johnny Cash
Eddie Cochran
The Everly Brothers
Billy Lee Riley
Jerry Lee Lewis
Rick Nelson
Roy Orbison
Carl Perkins
Gene Pitney
Little Richard
Scotty Moore
Gene Vincent
Fabian
Chris Isaak
Dean Martin
Big Mama Thornton
Big Joe Turner
1. A Little Less Conversation (MXL Radio E
2. Can't Help Falling In Love
3. Hound Dog
4. Suspicious Minds
5. All Shook Up
The Coasters 01:51 1.20 mb
Buddy Holly 02:29 1.83 mb
Little Richard 02:26 1.80 mb
Big Bopper 02:24 1.79 mb
Jerry Lee Lewis 01:52 1.21 mb
Unused Space: 29.97 GB / Used Space: 0.03 GB
Unused Space: 99.92% / Used Space: 00.08%
13 Tracks | 31.0 Min.

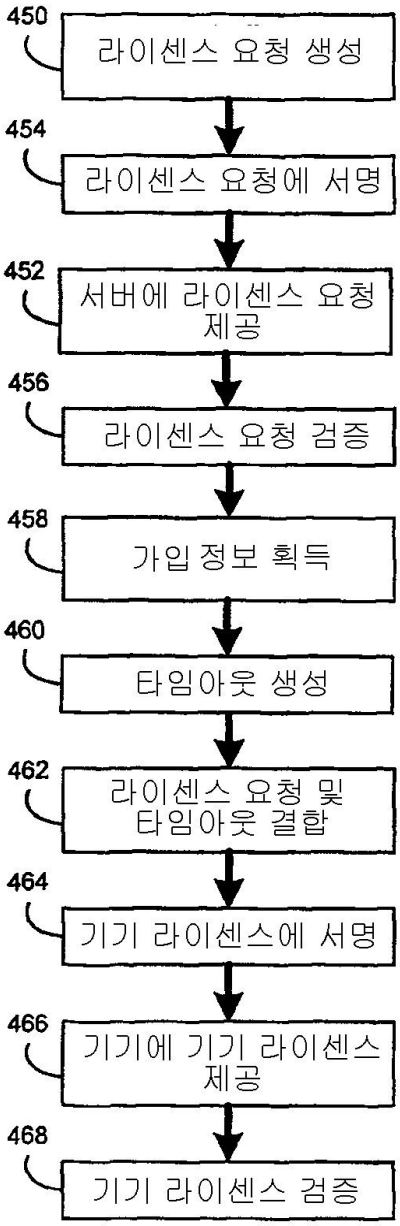
도면11


Rhapsody To Go
Stopped
Rhapsody Music Guide
Radio
My Library
My Playlists
50's Hits
My New Tracks
Sign Out
Rename
50's Hits
Track Name
Time
Artist Name
Album Name
Genre
Save as Playlist
Playlist Name:
50's Hits
OK
Cancel
Real MP3 Player 30 GB (SN: 137660523-1)
Data Files
Burn
Transfer
Unused Space: 29.97 GB / Used Space: 0.03 GB
Unused Space: 99.92% / Used Space: 00.08%
14 Tracks | 33 Min.
Clear
Save
Share
390
388
392
302
308
380
384
386
382
208

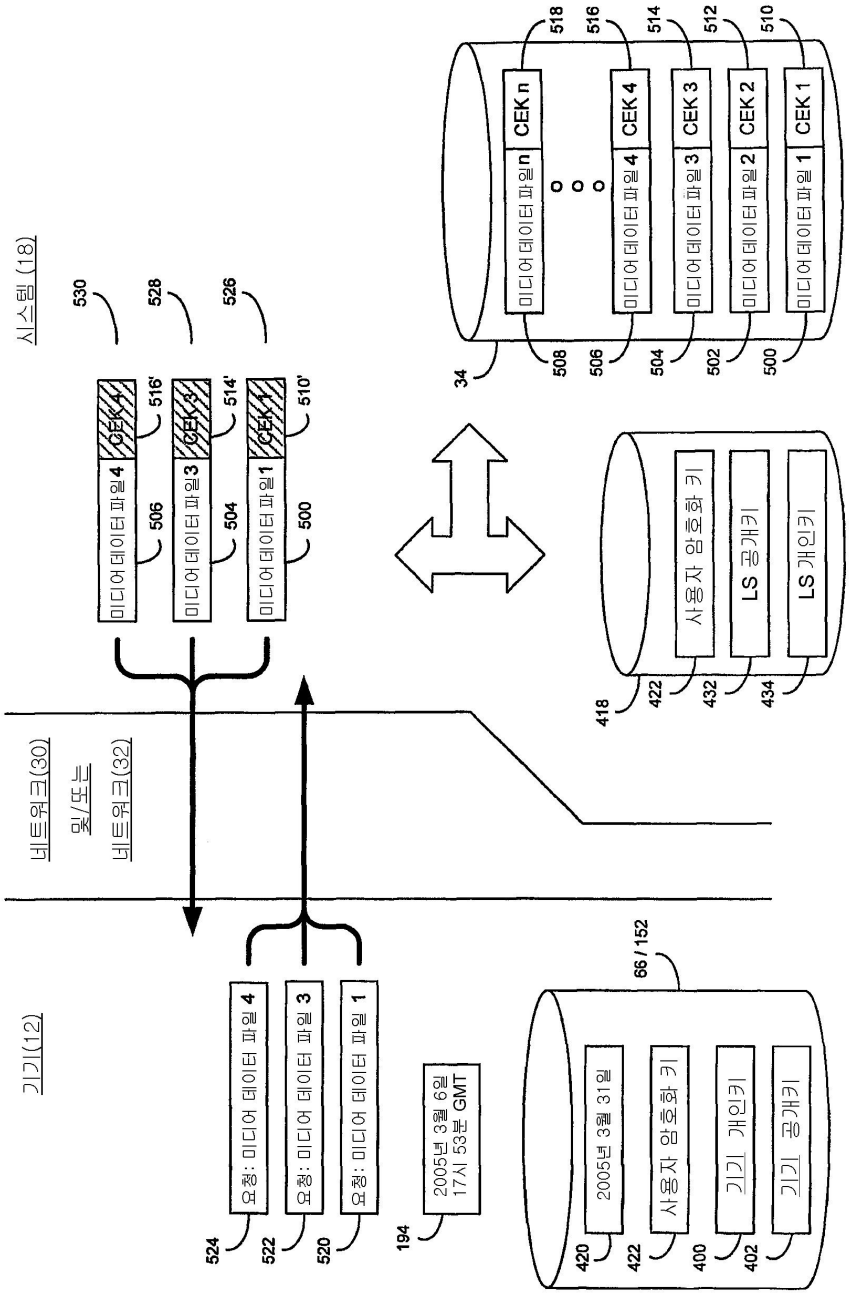
도면12a


시스템(18)
라이센스 요청
408
422'
424
426
시스템 타임 표시기
사용자 암호화 키
기기 디지털 인증서 (기기 공개키 402)
404
LS 디지털 인증서 (LS 공개키(432)
2005년 3월 31일
챌린지
사용자 ID
406
410
430
420
2005년 3월 6일 17시 53분 GMT
428
422
432
434
418
사용자 암호화 키
LS 공개키
LS 개인키
네트워크(30) 및/또는 네트워크(32)
인증 기관
CA 개인키
CA 공개키
414
416
412
기기(12)
사용자 ID
챌린지
기기 디지털 인증서 (기기 공개키 402)
408
410
406
404
기기 라이센스
424
194
2005년 3월 6일 17시 53분 GMT
66 / 152
2005년 3월 31일
사용자 암호화 키
기기 개인키
기기 공개키
420
422
400
402

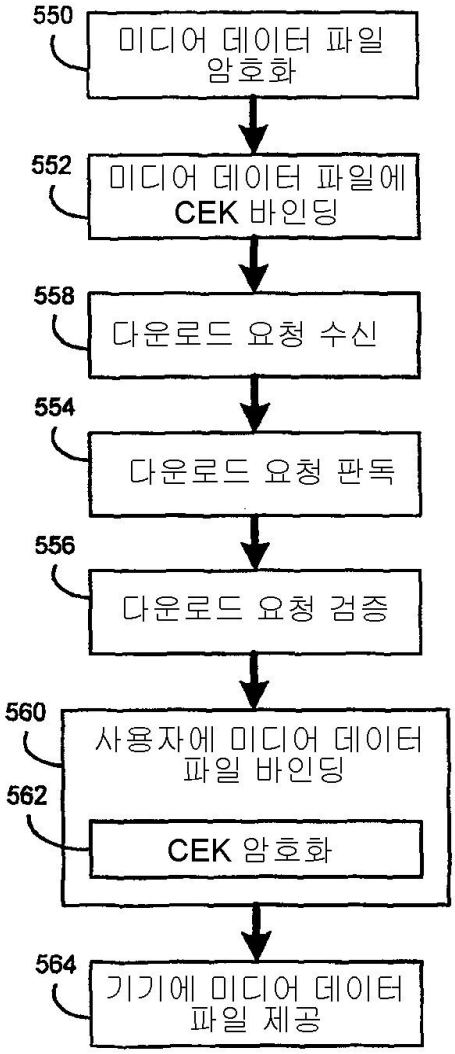
도면12b


450
라이센스 요청 생성
454
라이센스 요청에 서명
452
서버에 라이센스 요청 제공
456
라이센스 요청 검증
458
가입 정보 획득
460
타임아웃 생성
462
라이센스 요청 및 타임아웃 결합
464
기기 라이센스에 서명
466
기기에 기기 라이센스 제공
468
기기 라이센스 검증

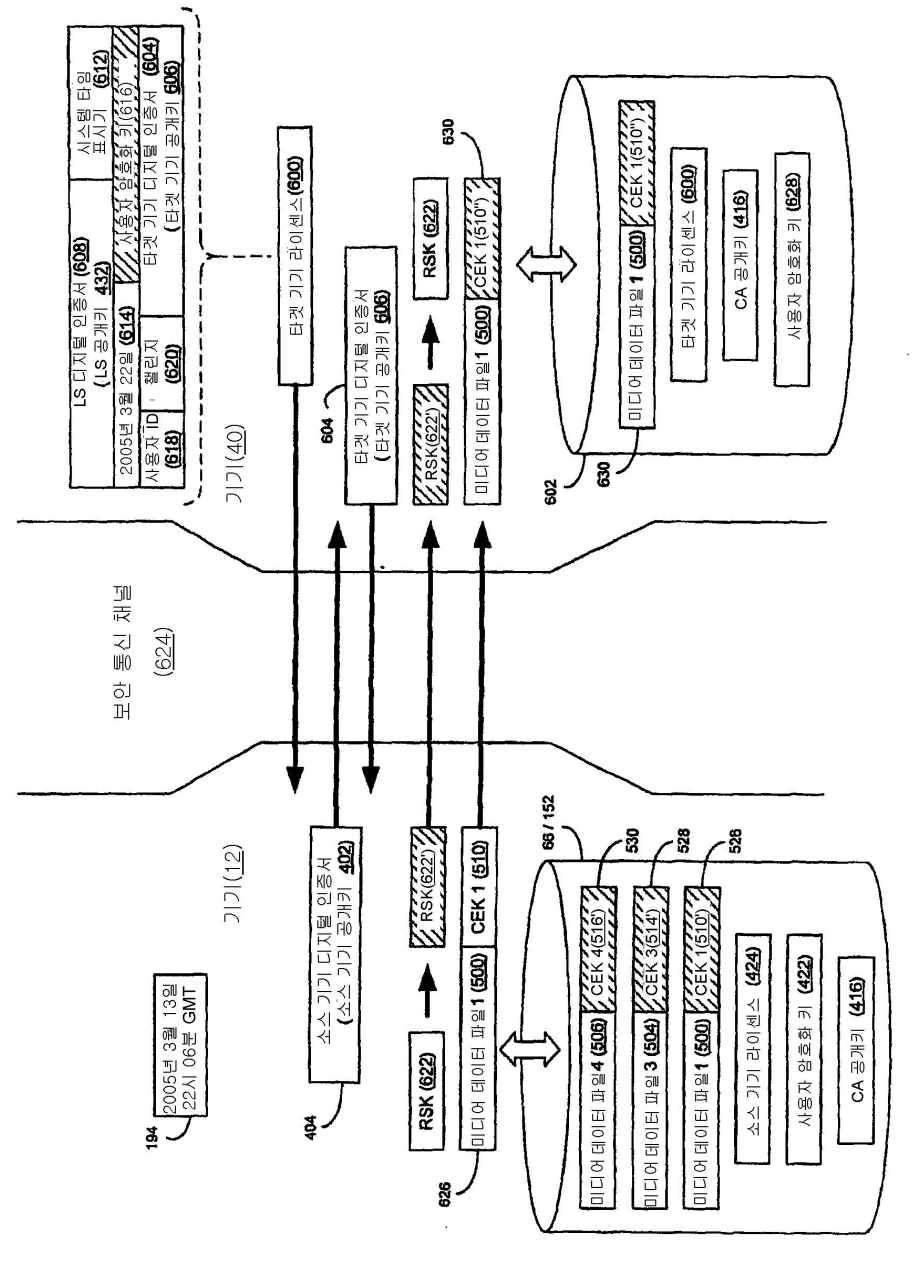
도면13a


시스템(18)
530
528
526
미디어 데이터 파일 4
CEK 4
516'
506
미디어 데이터 파일 3
CEK 3
514'
504
미디어 데이터 파일 1
CEK 1
510'
500
네트워크(30)
및/또는
네트워크(32)
기기(12)
요청: 미디어 데이터 파일 4
요청: 미디어 데이터 파일 3
요청: 미디어 데이터 파일 1
524
522
520
2005년 3월 6일
17시 53분 GMT
194
66 / 152
2005년 3월 31일
사용자 암호화 키
기기 개인키
기기 공개키
420
422
400
402
34
518
516
514
512
510
미디어 데이터 파일 n
CEK n
미디어 데이터 파일 4
CEK 4
미디어 데이터 파일 3
CEK 3
미디어 데이터 파일 2
CEK 2
미디어 데이터 파일 1
CEK 1
508
506
504
502
500
418
사용자 암호화 키
LS 공개키
LS 개인키
422
432
434

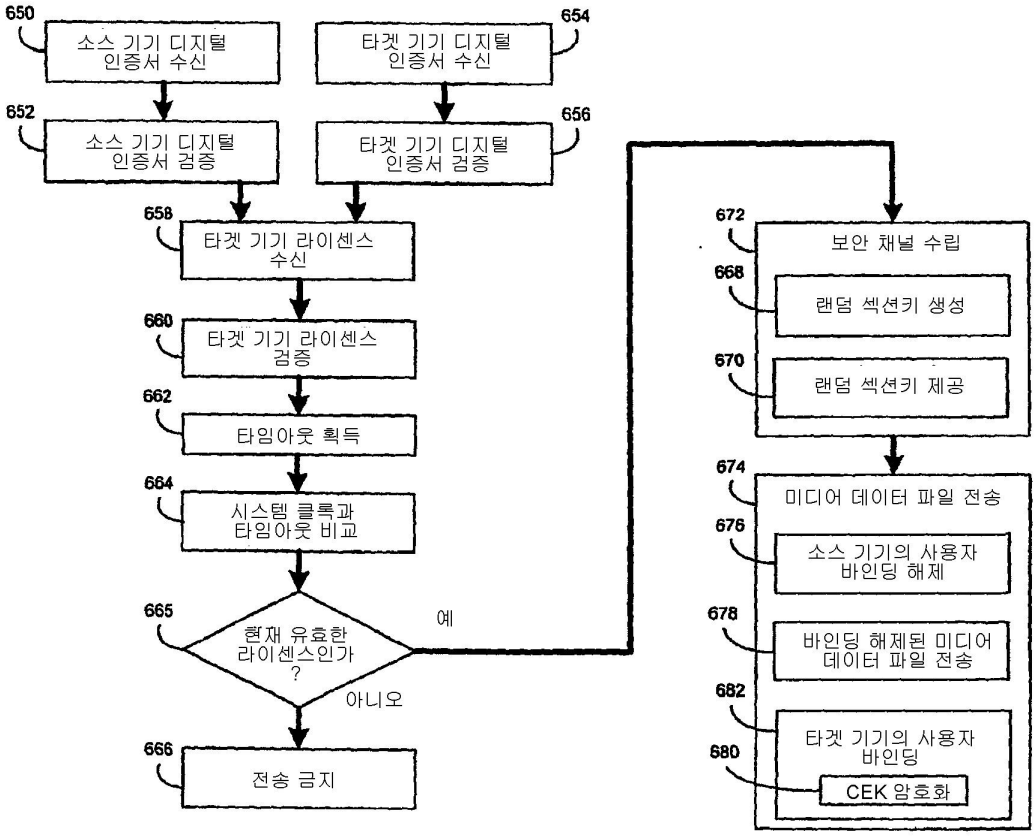
도면13b


550
미디어 데이터 파일 암호화
552
미디어 데이터 파일에 CEK 바인딩
558
다운로드 요청 수신
554
다운로드 요청 판독
556
다운로드 요청 검증
560
사용자에 미디어 데이터 파일 바인딩
562
CEK 암호화
564
기기에 미디어 데이터 파일 제공

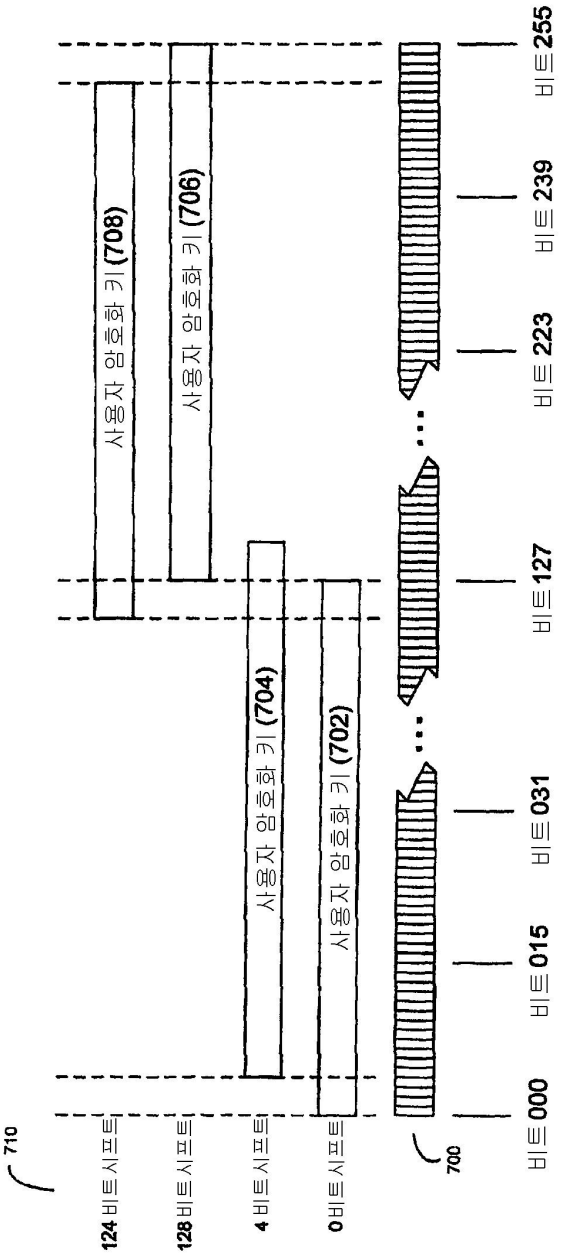
도면14a


LS 디지털 인증서 (608)
(LS 공개키 432)
2005년 3월 22일 (614)
사용자 ID (618)
챌린지 (620)
시스템 타임 표시기 (612)
사용자 암호화 키(616)
타겟 기기 디지털 인증서 (604)
(타겟 기기 공개키 606)
기기(40)
타겟 기기 라이센스(600)
604
타겟 기기 디지털 인증서 (타겟 기기 공개키 606)
RSK (622)
RSK(622')
630
CEK 1(510")
미디어 데이터 파일 1 (500)
602
630
미디어 데이터 파일 1 (500)
CEK 1(510")
타겟 기기 라이센스 (600)
CA 공개키 (416)
사용자 암호화 키 (628)
보안 통신 채널
(624)
기기(12)
194
2005년 3월 13일
22시 06분 GMT
404
소스 기기 디지털 인증서
(소스 기기 공개키 402)
RSK (622)
RSK(622')
CEK 1 (510)
미디어 데이터 파일 1 (500)
626
66 / 152
530
528
528
미디어 데이터 파일 4 (506)
CEK 4(516')
미디어 데이터 파일 3 (504)
CEK 3(514')
미디어 데이터 파일 1 (500)
CEK 1(510')
소스 기기 라이센스 (424)
사용자 암호화 키 (422)
CA 공개키 (416)

도면14b


650
소스 기기 디지털 인증서 수신
654
타겟 기기 디지털 인증서 수신
652
소스 기기 디지털 인증서 검증
656
타겟 기기 디지털 인증서 검증
658
타겟 기기 라이센스 수신
660
타겟 기기 라이센스 검증
662
타임아웃 획득
664
시스템 클록과 타임아웃 비교
665
현재 유효한 라이센스인가 ?
예
아니오
666
전송 금지
672
보안 채널 수립
668
랜덤 섹션키 생성
670
랜덤 섹션키 제공
674
미디어 데이터 파일 전송
676
소스 기기의 사용자 바인딩 해제
678
바인딩 해제된 미디어 데이터 파일 전송
682
타겟 기기의 사용자 바인딩
680
CEK 암호화

도면15


710
124 비트 시프트
128 비트 시프트
4 비트 시프트
0 비트 시프트
사용자 암호화 키 (708)
사용자 암호화 키 (706)
사용자 암호화 키 (704)
사용자 암호화 키 (702)
700
비트 000
비트 015
비트 031
비트 127
비트 223
비트 239
비트 255