(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년09월22일
(11) 등록번호 10-1658959
(24) 등록일자 2016년09월13일

(51) 국제특허분류(Int. Cl.)
G06F 21/10 (2013.01) *G06F 21/60* (2013.01)
(21) 출원번호 10-2013-7020692
(22) 출원일자(국제) 2011년12월28일
심사청구일자 2013년08월05일
(85) 번역문제출일자 2013년08월05일
(65) 공개번호 10-2013-0118940
(43) 공개일자 2013년10월30일
(86) 국제출원번호 PCT/US2011/067472
(87) 국제공개번호 WO 2012/094196
국제공개일자 2012년07월12일
(30) 우선권주장
12/984,737 2011년01월05일 미국(US)
(56) 선행기술조사문헌
KR1020070056133 A*
US07293178 B2*
Ernie Brickell, Jiangtao Li, 'Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities', Proceedings of the 6th WPES, IACR, 2007.10.*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
펜다쿠르, 라메시
미국 97119 오레곤주 가스톤 사우쓰웨스트 나이트 로드 44401
긴츠, 왈터, 씨.
미국 97034 오레곤주 레이크 오스웨고 리지 포인트 드라이브 2070
(뒷면에 계속)
(74) 대리인
양영준, 백만기

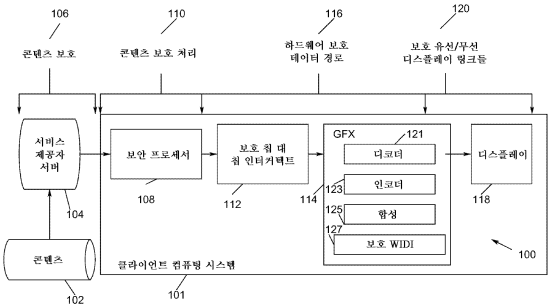
전체 청구항 수 : 총 31 항 심사관 : 서광훈

(54) 발명의 명칭 **하드웨어 신뢰 루트를 구축하고 보호 콘텐츠 처리를 개방 컴퓨팅 플랫폼 내에 제공하는 방법 및 장치**

(57) 요 약

시스템 아키텍처는 프리미엄 디지털 콘텐츠의 배포 및 재생을 지원하는 하드웨어 기반 신뢰 루트 해결법을 제공한다. 실시예에서, 디지털 콘텐츠 및 서비스들을 위한 하드웨어 신뢰 루트는 보안 목적들을 위한 신뢰 기반이 소프트웨어보다는 오히려 클라이언트 컴퓨팅 시스템 내의 하드웨어 및 펌웨어 메커니즘들에 정착되는 해결법이다. 이 신뢰 루트로부터, 클라이언트 컴퓨팅 시스템은 콘텐츠 인가 및 재생을 위해 보호되는 전체 미디어 처리 파이프라인을 구성한다. 본 발명의 실시예들에서, 콘텐츠 처리를 위한 클라이언트 컴퓨팅 시스템의 보안은 운영 체제(OS), 기본 입출력 시스템(BIOS), 미디어 플레이어 애플리케이션, 또는 다른 호스트 소프트웨어에 의존하지 않는다.

대 표 도



(72) 발명자

네미로프, 다니엘

미국 95630 캘리포니아주 폴섬 싱어 레인 152

하즈라, 모우수미, 엠.

미국 97006 오레곤주 비버톤 노쓰이스트 그랜브리어 파크웨이 15400

명 세 서

청구범위

청구항 1

콘텐츠를 클라이언트 컴퓨팅 장치에서 처리하는 방법으로서 - 콘텐츠는 별개의 보안 성질들 및 키 재료를 갖는 하나 이상의 동시 보호 콘텐츠 스트림들을 포함함 -,

상기 클라이언트 컴퓨팅 장치의 보안 프로세서에 의해, 상기 클라이언트 컴퓨팅 장치와 서비스 제공자 서버 사이에 하드웨어 기반 신뢰 루트를 설정하는 단계;

상기 클라이언트 컴퓨팅 장치에 의해, 상기 서비스 제공자 서버로부터 상기 서비스 제공자 서버의 암호화된 콘텐츠와 연관되는 암호화된 타이틀 키를 수신하는 단계;

상기 보안 프로세서에 의해, 상기 서비스 제공자 서버로부터 수신한 상기 암호화된 타이틀 키를 복호화하는 단계;

상기 보안 프로세서에 의해, 키 블랍(key blob)을 형성하도록 상기 복호화된 타이틀 키를 저장 키를 사용하여 암호화하는 단계;

상기 복호화된 타이틀 키를 암호화하는 것에 응답하여 상기 클라이언트 컴퓨팅 장치의 메모리에 저장을 위해 상기 클라이언트 컴퓨팅 장치의 상기 보안 프로세서로부터 중앙 프로세서에 상기 키 블랍을 전송하는 단계;

상기 보안 프로세서에 의해, 상기 암호화된 콘텐츠를 실행하라는 상기 클라이언트 컴퓨팅 장치의 사용자로부터의 요청에 응답하여 상기 중앙 프로세서로부터 상기 키 블랍을 수신하는 단계;

상기 보안 프로세서에 의해, 하드웨어-보호된 데이터 경로를 통해 상기 클라이언트 컴퓨팅 장치의 그래픽스 엔진으로 상기 키 블랍을 전송하는 단계;

상기 그래픽스 엔진에 의해, 상기 암호화된 콘텐츠의 적어도 하나의 슬라이스를 수신하는 단계;

상기 그래픽스 엔진에 의해, 상기 보안 프로세서로부터 수신한 상기 저장 키를 사용하여 상기 키 블랍을 복호화하는 단계;

상기 그래픽스 엔진 상에서, 상기 복호화된 키 블랍의 상기 타이틀 키를 사용하여 상기 암호화된 콘텐츠의 상기 적어도 하나의 슬라이스를 복호화하는 단계;

상기 그래픽스 엔진 상에서, 하나 이상의 재암호화된 콘텐츠 슬라이스를 생성하도록 상기 적어도 하나의 복호화된 콘텐츠 슬라이스를 암호화하는 단계;

상기 그래픽스 엔진 상에서, 적어도 하나의 복호화된 콘텐츠 슬라이스를 암호화하는 것에 응답하여 재암호화된 콘텐츠 슬라이스들에 기초하여 합성된 이미지 데이터를 생성하는 단계;

상기 그래픽스 엔진으로부터, 상기 하드웨어-보호된 데이터 경로를 통해 상기 보안 프로세서에 상기 합성된 이미지 데이터를 전송하는 단계; 및

상기 보안 프로세서로부터, 보호 디스플레이 인터페이스 링크를 통해 디스플레이에 상기 합성된 이미지 데이터를 전송하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 키 블랍을 형성하도록 상기 복호화된 타이틀 키를 암호화하는 단계는 상기 키 블랍을 상기 클라이언트 컴퓨팅 장치에 바인딩시키는 단계를 포함하는 방법.

청구항 3

제1항에 있어서, 상기 하드웨어 기반 신뢰 루트를 설정하는 단계는 제로 지식 증명들(zero-knowledge proofs)의

사용에 기초하여 사용자의 프라이버시를 보호하는 암호 인증 프로토콜을 수행하는 단계를 포함하는 방법.

청구항 4

제3항에 있어서, 상기 암호 인증 프로토콜을 수행하는 단계는 강화된 프라이버시 ID(EPID:Enhanced Privacy ID) 인증 프로토콜을 수행하는 단계를 포함하는 방법.

청구항 5

제3항에 있어서, 상기 클라이언트 컴퓨팅 장치의 상기 보안 프로세서 및 상기 하드웨어 기반 신뢰 루트와, 상기 서비스 제공자 서버 사이에 보안 통신 채널을 상기 암호 인증 프로토콜에 기초하여 설정하는 단계를 더 포함하는 방법.

청구항 6

제1항에 있어서, 상기 클라이언트 컴퓨팅 장치에 의해, 상기 서비스 제공자 서버로부터 상기 암호화된 콘텐츠의 사용 제약들을 수신하는 단계를 더 포함하는 방법.

청구항 7

제6항에 있어서, 상기 보안 프로세서 상에서, 상기 중앙 프로세서로부터 상기 키 블랍을 수신하는 것에 응답하여 상기 키 블랍의 서명 및 상기 암호화된 콘텐츠의 상기 사용 제약들을 검증하는 단계를 더 포함하는 방법.

청구항 8

제7항에 있어서, 상기 제약들을 검증하는 단계는 지정된 시간 기간 동안 상기 클라이언트 컴퓨팅 장치에 바인딩된 상기 키 블랍을 식별하는 단계를 포함하는 방법.

청구항 9

삭제

청구항 10

삭제

청구항 11

제1항에 있어서, 상기 암호화된 콘텐츠의 상기 적어도 하나의 슬라이스를 수신하는 단계는 각각의 슬라이스의 헤더가 암호화되지 않은 상기 암호화된 콘텐츠의 적어도 하나의 슬라이스를 수신하는 단계를 포함하는 방법.

청구항 12

제1항에 있어서, 상기 그래픽스 엔진 상에서, 상기 적어도 하나의 복호화된 콘텐츠 슬라이스를 디코딩하는 단계를 더 포함하고, 하나 이상의 재암호화된 콘텐츠 슬라이스를 생성하도록 상기 적어도 하나의 복호화된 콘텐츠 슬라이스를 암호화하는 단계는 상기 적어도 하나의 복호화된 콘텐츠 슬라이스를 디코딩하는 단계에 응답하는 것인 방법.

청구항 13

제1항에 있어서, 상기 콘텐츠는 복수의 동시발생하는 독립 콘텐츠 스트림들을 포함하며, 각각의 콘텐츠 스트림은 별개의 암호 컨텍스트(cryptographic context)를 갖는 방법.

청구항 14

별개의 보안 성질들 및 키 재료를 갖는 하나 이상의 동시 보호 콘텐츠 스트림들을 포함하는 콘텐츠를 처리하는 클라이언트 컴퓨팅 장치로서,

상기 클라이언트 컴퓨팅 장치는

하드웨어 보안 프로세서 및 하드웨어 그래픽스 엔진을 포함하고,

상기 보안 프로세서는,

상기 클라이언트 컴퓨팅 장치와 서비스 제공자 서버 사이에 하드웨어 기반 신뢰 루트를 설정하고;

상기 서비스 제공자 서버로부터, 상기 서비스 제공자 서버의 암호화된 콘텐츠와 연관되는 암호화된 타이틀 키를 수신하고;

상기 서비스 제공자 서버로부터 수신한 상기 암호화된 타이틀 키를 복호화하고;

키 블랍을 형성하도록 상기 복호화된 타이틀 키를 저장 키를 사용하여 암호화하고;

상기 복호화된 타이틀 키의 암호화에 응답하여 상기 클라이언트 컴퓨팅 장치의 메모리에 저장을 위해 상기 클라이언트 컴퓨팅 장치의 중앙 프로세서에 상기 키 블랍을 전송하고;

상기 암호화된 콘텐츠를 실행하라는 상기 클라이언트 컴퓨팅 장치의 사용자로부터의 요청에 응답하여 상기 중앙 프로세서로부터 상기 키 블랍을 수신하고;

하드웨어-보호된 데이터 경로를 통해 상기 클라이언트 컴퓨팅 장치의 그래픽스 엔진에 상기 키 블랍을 전송하도록 구성되고;

상기 그래픽스 엔진은,

상기 암호화된 콘텐츠의 적어도 하나의 슬라이스를 수신하고;

상기 보안 프로세서로부터 수신한 상기 저장 키를 사용하여 상기 키 블랍을 복호화하고;

상기 복호화된 키 블랍의 상기 타이틀 키를 사용하여 상기 암호화된 콘텐츠의 상기 적어도 하나의 슬라이스를 복호화하고;

하나 이상의 재암호화된 콘텐츠 슬라이스를 생성하도록 상기 적어도 하나의 복호화된 콘텐츠 슬라이스를 암호화하고;

상기 재암호화된 콘텐츠 슬라이스들의 생성에 응답하여 상기 재암호화된 콘텐츠 슬라이스들에 기초하여 합성된 이미지 데이터를 생성하고;

상기 하드웨어-보호된 데이터 경로를 통해 상기 보안 프로세서에 상기 합성된 이미지 데이터를 전송하도록 구성되고;

상기 보안 프로세서는 또한 보호 디스플레이 인터페이스 링크를 통해 디스플레이에 상기 합성된 이미지 데이터를 전송하는 클라이언트 컴퓨팅 장치.

청구항 15

제14항에 있어서, 상기 키 블랍을 형성하도록 상기 복호화된 타이틀 키를 암호화하는 것은 상기 키 블랍을 상기 클라이언트 컴퓨팅 장치에 바인딩하는 것을 포함하는 클라이언트 컴퓨팅 장치.

청구항 16

제14항에 있어서, 상기 하드웨어 기반 신뢰 루트를 설정하는 것은 제로 지식 증명들의 사용에 기초하여 사용자의 프라이버시를 보호하는 암호 인증 프로토콜을 수행하는 것을 포함하는 클라이언트 컴퓨팅 장치.

청구항 17

제16항에 있어서, 상기 암호 인증 프로토콜을 수행하는 것은 강화된 프라이버시 ID(EPID) 인증 프로토콜을 수행하는 것을 포함하는 클라이언트 컴퓨팅 장치.

청구항 18

제16항에 있어서, 상기 보안 프로세서는 또한 상기 암호 인증 프로토콜에 기초하여 상기 서비스 제공자 서버와 상기 클라이언트 컴퓨팅 장치의 상기 하드웨어 기반 신뢰 루트 사이에 보안 통신 채널을 설정하는 클라이언트 컴퓨팅 장치.

청구항 19

제14항에 있어서, 상기 보안 프로세서는 또한 상기 서비스 제공자 서버로부터, 상기 암호화된 콘텐츠의 사용 제약들을 수신하는 클라이언트 컴퓨팅 장치.

청구항 20

제19항에 있어서, 상기 보안 프로세서는 또한 상기 중앙 프로세서로부터의 상기 키 블랍의 수신에 응답하여 상기 암호화된 콘텐츠의 상기 사용 제약들 및 상기 키 블랍의 서명을 검증하는 클라이언트 컴퓨팅 장치.

청구항 21

제20항에 있어서, 상기 제약들을 검증하는 것은 지정된 시간 기간 동안 상기 클라이언트 컴퓨팅 장치에 바인딩된 상기 키 블랍을 식별하는 것을 포함하는 클라이언트 컴퓨팅 장치.

청구항 22

제14항에 있어서, 상기 콘텐츠는 복수의 동시발생하는 독립 콘텐츠 스트림들을 포함하며, 각각의 콘텐츠 스트림은 별개의 암호 컨텍스트를 갖는 클라이언트 컴퓨팅 장치.

청구항 23

제14항에 있어서, 상기 암호화된 콘텐츠의 상기 적어도 하나의 슬라이스를 수신하는 것은 각각의 슬라이스의 헤더가 암호화되지 않은 상기 암호화된 콘텐츠의 적어도 하나의 슬라이스를 수신하는 것을 포함하는 클라이언트 컴퓨팅 장치.

청구항 24

프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체로서, 상기 프로그램은 실행에 응답하여 컴퓨팅 장치로 하여금,

상기 컴퓨팅 장치의 보안 프로세서에 의해, 상기 컴퓨팅 장치와 서비스 제공자 서버 사이에 하드웨어 기반 신뢰 루트를 설정하고;

상기 서비스 제공자 서버로부터, 상기 서비스 제공자 서버의 암호화된 콘텐츠와 연관되는 암호화된 타이틀 키를 수신하고;

상기 보안 프로세서에 의해, 상기 서비스 제공자 서버로부터 수신한 상기 암호화된 타이틀 키를 복호화하고;

상기 보안 프로세서에 의해, 키 블랍을 형성하도록 상기 복호화된 타이틀 키를 저장 키를 사용하여 암호화하고;

상기 복호화된 타이틀 키의 암호화에 응답하여 상기 컴퓨팅 장치의 메모리에 저장을 위해 상기 컴퓨팅 장치의 상기 보안 프로세서로부터 중앙 프로세서에 상기 키 블랍을 전송하고;

상기 보안 프로세서에 의해, 상기 암호화된 콘텐츠를 실행하라는 상기 컴퓨팅 장치의 사용자로부터의 요청에 응답하여 상기 중앙 프로세서로부터 상기 키 블랍을 수신하고;

상기 보안 프로세서에 의해, 하드웨어-보호된 데이터 경로를 통해 상기 컴퓨팅 장치의 그래픽스 엔진에 상기 키 블랍을 전송하고;

상기 그래픽스 엔진에 의해, 상기 암호화된 콘텐츠의 적어도 하나의 슬라이스를 수신하고;

상기 그래픽스 엔진에 의해, 상기 보안 프로세서로부터 수신한 상기 저장 키를 사용하여 상기 키 블랍을 복호화하고;

상기 그래픽스 엔진에 의해, 상기 복호화된 키 블랍의 상기 타이틀 키를 사용하여 상기 암호화된 콘텐츠의 상기 적어도 하나의 슬라이스를 복호화하고;

상기 그래픽스 엔진 상에서, 하나 이상의 재암호화된 콘텐츠 슬라이스를 생성하도록 상기 적어도 하나의 복호화된 콘텐츠 슬라이스를 암호화하고;

상기 그래픽스 엔진 상에서, 재암호화된 콘텐츠 슬라이스들의 생성에 응답하여 상기 재암호화된 콘텐츠 슬라이스들에 기초하여 합성된 이미지 데이터를 생성하고;

상기 그래픽스 엔진으로부터, 상기 하드웨어-보호된 데이터 경로를 통해 상기 보안 프로세서에 상기 합성된 이

미지 데이터를 전송하고;

상기 보안 프로세서로부터, 보호 디스플레이 인터페이스 링크를 통해 디스플레이에 상기 합성된 이미지 데이터를 전송하게 하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 25

제24항에 있어서, 상기 키 블랍을 형성하도록 상기 복호화된 타이틀 키를 암호화하는 것은 상기 키 블랍을 상기 컴퓨팅 장치에 바인딩시키는 것을 포함하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 26

제24항에 있어서, 상기 하드웨어 기반 신뢰 루트를 설정하는 것은 제로 지식 증명들의 사용에 기초하여 사용자의 프라이버시를 보호하는 암호 인증 프로토콜을 수행하는 것을 포함하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 27

제26항에 있어서, 상기 암호 인증 프로토콜을 수행하는 것은 강화된 프라이버시 ID(EPID) 인증 프로토콜을 수행하는 것을 포함하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 28

제26항에 있어서, 상기 프로그램은 또한 상기 컴퓨팅 장치로 하여금, 상기 컴퓨팅 장치의 상기 보안 프로세서 및 상기 하드웨어 기반 신뢰 루트와, 상기 서비스 제공자 서버 사이의 보안 통신 채널을 상기 암호 인증 프로토콜에 기초하여 설정하게 하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 29

제24항에 있어서, 상기 프로그램은 또한 상기 컴퓨팅 장치로 하여금, 상기 서비스 제공자 서버로부터, 상기 암호화된 콘텐츠의 사용 제약들을 수신하게 하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 30

제29항에 있어서, 상기 프로그램은 또한 상기 컴퓨팅 장치로 하여금, 상기 중앙 프로세서로부터 상기 키 블랍을 수신하는 것에 응답하여 상기 키 블랍의 서명 및 상기 암호화된 콘텐츠의 상기 사용 제약들을 검증하게 하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 31

제30항에 있어서, 상기 제약들을 검증하는 것은 상기 키 블랍을 지정된 시간 기간 동안 상기 컴퓨팅 장치로 바인딩되었다고 식별하는 것을 포함하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 32

제24항에 있어서, 상기 콘텐츠는 복수의 동시발생하는 독립 콘텐츠 스트림들을 포함하며, 각각의 콘텐츠 스트림은 별개의 암호 컨텍스트를 갖는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 33

제24항에 있어서, 상기 암호화된 콘텐츠의 상기 적어도 하나의 슬라이스를 수신하는 것은 각각의 슬라이스의 헤더가 암호화되지 않은 상기 암호화된 콘텐츠의 적어도 하나의 슬라이스를 수신하는 것을 포함하는, 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 디지털 콘텐츠를 보안 처리하는 컴퓨팅 시스템 아키텍처들의 분야에 관한 것이다. 특히, 본 발명의 실시예는 하드웨어 신뢰 루트를 구축하고 디지털 콘텐츠 처리 단 대 단(end-to-end)을 컴퓨팅 시스템

에서 보호하는 것에 관한 것이다.

배 경 기 술

[0002] 예를 들어 개인용 컴퓨터(PC) 시스템과 같은 개방 컴퓨팅 플랫폼들 상에서, 프리미엄 콘텐츠를 (예컨대 DVD, 블루 레이 등으로부터) 플레이할 때, 디지털 저작권 관리(DRM) 처리 및 키 관리는 전형적으로 미디어 플레이어 애플리케이션 프로그램에 의해 소프트웨어로 수행된다. 이 방식들은 잘 보호되지 않고 해킹의 경우들이 있어 와서, 침해된 콘텐츠 및 수익 손실을 콘텐츠 소유자들에게 야기한다. 콘텐츠가 플레이될 때, 미디어 압축 해제(H.264, MPEG-2 등)가 하드웨어로 수행될지라도, 콘텐츠는 시스템 메모리 내에서 클리어(clear)로 있고 소프트웨어 기반 및/또는 하드웨어 기반 공격들에 의해 도난 당할 수 있다. 이렇게 알려져 있는 보안 약점으로 인해, 단지 더 낮은 정밀도(표준 선명(SD:standard definition) 등) 콘텐츠 또는 덜 귀중한 고선명(HD:high definition) 콘텐츠가 전형적으로 개방 컴퓨팅 플랫폼들에 배포된다. 개방 컴퓨팅 플랫폼들(예를 들어 PC 등)에 의한 디지털 콘텐츠의 보안 취급의 개선들이 요구된다.

도면의 간단한 설명

[0003] 상세한 설명은 첨부 도면들을 참조하여 제공된다. 상이한 도면들 내의 동일한 참조 번호들의 사용은 유사 또는 동일한 항목들을 나타낸다.

도 1은 본 발명의 실시예에 따른 보안 콘텐츠 처리 파이프라인의 도면이다.

도 2는 본 발명의 실시예에 따른 서비스 제공자 서버 및 보안 서비스 인프라스트럭처의 도면이다.

도 3은 본 발명의 실시예에 따른 클라이언트 컴퓨팅 시스템의 도면이다.

도 4는 본 발명의 실시예에 따른 보안 콘텐츠 처리의 흐름도이다.

도 5는 본 발명의 실시예에 따른 보안 콘텐츠 처리 시스템의 도면이다.

발명을 실시하기 위한 구체적인 내용

[0004] 본 발명의 실시예들은 프리미엄 디지털 콘텐츠의 배포 및 재생을 지원하는 하드웨어 기반 신뢰 루트(HW ROT, hardware-based root of trust) 해결법을 제공하는 시스템 아키텍처를 포함한다. 실시예에서, 디지털 콘텐츠 및 서비스들을 위한 HW ROT는 보안 목적들을 위한 신뢰 기반이 소프트웨어보다는 오히려 클라이언트 컴퓨팅 시스템 내의 하드웨어 및 펌웨어 메커니즘들에 정착되는(rooted) 해결법이다. 이 신뢰 루트로부터, 클라이언트 컴퓨팅 시스템은 콘텐츠 인가 및 재생을 위해 보호되는 전체 미디어 처리 파이프라인을 구성한다. 본 발명의 실시예들에서, 콘텐츠 처리를 위한 클라이언트 컴퓨팅 시스템의 보안은 운영 체제(OS), 기본 입출력 시스템(BIOS), 미디어 플레이어 애플리케이션, 또는 다른 호스트 소프트웨어에 의존하지 않는다. 시스템을 손상(compromise)시키기 위해, OS의 상부에서 실행하는 소프트웨어를 공격하는 것과는 대조적으로, 하드웨어 및/또는 펌웨어 메커니즘들을 손상시키는 것이 필요할 것이다.

[0005] 이하의 설명에서, 다양한 실시예들의 완전한 이해를 제공하기 위해 다수의 특정 상세들이 진술되어 있다. 그러나, 본 발명의 다양한 실시예들은 특정 상세들 없이 실시될 수 있다. 다른 경우들에서, 공지된 방법들, 절차들, 구성요소들, 및 회로들은 본 발명의 특정 실시예들을 모호하게 하지 않도록 상세히 설명되지 않았다. 게다가, 본 발명의 실시예들의 다양한 양태들은 집적된 반도체 회로들("하드웨어"), 컴퓨터 판독가능 저장 매체 상에 저장되는 하나 이상의 프로그램들로 조직되는 컴퓨터 판독가능 명령어들("소프트웨어"), 또는 하드웨어 및 소프트웨어의 일부 결합과 같은 다양한 수단을 사용하여 수행될 수 있다. 본 발명의 목적들을 위해, "로직"에 대한 언급은 하드웨어, 소프트웨어(예를 들어 프로세서의 동작들을 제어하는 마이크로코드를 포함함), 펌웨어, 또는 그의 일부 결합을 의미할 것이다.

[0006] 본 발명의 실시예들은 펌웨어 및 하드웨어를 클라이언트 컴퓨팅 시스템(101)의 CPU, 칩셋 및 통합된 그래픽스/미디어 엔진에 사용함으로써 콘텐츠 보호 처리, 키 관리 처리, 및 콘텐츠 재생을 보호하여 이 기능들을 수행한다. 본 발명의 실시예들은 콘텐츠가 컴퓨팅 시스템 내의 구성요소들에 의해 처리될 때 콘텐츠의 단 대 단 보호를 제공한다. 도 1은 본 발명의 실시예에 따른 보안 콘텐츠 처리 파이프라인(100)의 도면이다. 콘텐츠(102)는 서비스 제공자(SP) 서버(104)에 의해 액세스가능할 수 있다. 콘텐츠(102)는 오디오, 비디오, 또는 오디오/비디오 데이터와 같은 임의의 디지털 정보, 이미지들, 텍스트, 책들, 잡지들, 게임들, 또는 애플리케이션 프로그램들일 수 있다. 서비스 제공자 서버(104)는 콘텐츠를 임의의 전기통신 채널(인터넷, 셀룰러 네트워크들, 유선

또는 무선 네트워크들 등)을 통해 클라이언트 컴퓨팅 시스템에 제공하는 하나 이상의 서버들을 포함할 수 있다. 콘텐츠는 SP 서버에 저장되는 동안 및 클라이언트 컴퓨팅 시스템(101)으로의 전송 동안 임의의 공지된 콘텐츠 보호 기술(106)(예를 들어, 디지털 저작권 관리(DRM) 기술, 암호 기술들 등)에 의해 보호될 수 있다. 일 실시예에서, 콘텐츠는 본 명세서에 논의되는 바와 같은 강화된 프라이버시 ID(EPID:Enhanced Privacy ID) 서명 검증 프로토콜에 의해 보호될 수 있다. 일 실시예에서, 비디오 데이터는 CTR 모드와 고급 암호화 표준(AES:Advanced Encryption Standard) 암호 처리를 사용하여 암호화될 수 있다. 클라이언트 컴퓨팅 시스템(101)은 PC, 랩톱, 넷북, 태블릿 컴퓨터, 핸드헬드 컴퓨터, 스마트폰, 개인 휴대 정보 단말기(PDA), 셋톱 박스, 소비자 전자 장비, 또는 콘텐츠를 수신, 저장 및 렌더링하는 임의의 다른 컴퓨팅 장치일 수 있다.

[0007] 클라이언트 컴퓨팅 시스템 내에서, 콘텐츠 보호 처리(110)는 보안 프로세서(108)에 의해 수행될 수 있다. 일 실시예에서, 보안 프로세서는 클라이언트 컴퓨팅 시스템의 칩셋 내에 있을 수 있다. 실시예에서, 칩셋은 플랫폼 제어 허브(PCH)를 포함한다. 다른 실시예에서, 보안 프로세서는 클라이언트 컴퓨팅 시스템의 CPU 내에 있을 수 있다. 시스템 온 칩(SOC) 구성을 갖는 다른 실시예에서, 보안 프로세서는 단일 칩 상의 다른 시스템 구성요소들과 일체형일 수 있다. 일 실시예에서, 보안 프로세서는 매니지어빌리티 엔진(ME:Manageability Engine)을 포함한다. 다른 실시예들에서, 다른 타입들의 보안 프로세서들이 사용될 수 있다. 보안 프로세서는 클라이언트 컴퓨팅 시스템의 다른 구성요소들과 상호 작용하는 하드웨어 및 펌웨어로 구현되는 서브시스템이다. 보안 프로세서는 보호 플래시 메모리 영역으로부터 펌웨어 코드를 로드하고 펌웨어 코드를 보호 메모리에서 실행함으로써 동작한다. 콘텐츠 보호 처리가 보안 프로세서 내의 하드웨어 및 펌웨어에서 수행되므로, 콘텐츠의 보호는 소프트웨어 기반 시스템들보다 개선될 수 있다.

[0008] 암호 키 정보는 보안 프로세서로부터 보호 칩 대 칩 인터커넥트(protected chip to chip interconnect)(112)를 통해 중앙 처리 유닛(CPU) 및 통합된 그래픽스(GFX)/미디어 엔진을 포함하는 구성요소로 송신될 수 있다. 실시예에서, 보호 칩 대 칩 인터커넥트(112)는 CPU/GFX 구성요소에 대한 보안 다이렉트 미디어 인터페이스(DMI:Direct Media Interface) 통신 링크를 포함한다. DMI는 동시발생하는 데이터 트래픽의 2개의 단방향 레인들을 갖는 칩 대 칩 인터커넥트, 및 개선된 서비스 품질을 갖는 등시(isochronous) 전송을 포함한다. DMI 링크를 통해 전송되는 데이터는 공지된 암호 처리 기술들에 의해 보호될 수 있다. 실시예에서, 칩 대 칩 보안 링크는 암호화된 타이틀 키들을 DMI를 통해 전달하는데 사용될 수 있다. 보안은 PCH와 CPU 사이의 공유 비밀에 기초한다. 이 공유 비밀은 각각의 파워 사이클 상에 설정될 수 있고 필요에 따라 제품군들, 세대들(generations) 및 랜덤 그룹화들 사이에서 변할 수 있어 공유 비밀의 보호 및 무결성을 보장한다. DMI 메커니즘은 OS, BIOS, 및 CPU 상에 실행하는 소프트웨어로부터 독립적이다. 보안 프로세서(PCH 내)와 CPU 사이의 신뢰 관계를 생성하기 위해 DMI 메커니즘이 사용될 수 있다.

[0009] GFX 엔진(114)은 콘텐츠를 복호화하기 위해 콘텐츠 보호 처리를 포함할 수 있다. GFX 엔진은 또한 복호화된 오디오/비디오 콘텐츠를 처리/디코딩하고 오디오/비디오 콘텐츠를 미디어 블록들로서 GFX 엔진(114) 내의 그래픽스 처리 유닛(GPU)에 전달하는 디코더 로직(121)을 포함한다. GPU는 미디어 블록들을 처리 동안 메모리에서 보호하기 위해, 인코더 로직(123)을 사용하는 것을 포함하는 보안 기술들을 포함한다. GFX 엔진(114)은 또한 디스플레이(118) 상에 보여지는 이미지 데이터를 합성하는 합성 로직(125)을 포함한다. 콘텐츠가 PCH 내의 보안 프로세서 및 CPU/GFX 구성요소 내의 GFX 엔진 내에서 및 이들 사이에서 취급되고 있을 때, 콘텐츠는 하드웨어 보호 데이터 경로(116)에 의해 보호될 수 있다. 실시예에서, 하드웨어 보호 데이터 경로는 콘텐츠의 보안을 유지하기 위해 보호 오디오 비디오 경로(PAVP:Protected Audio Video Path)를 포함한다. PAVP는 또한 시스템 구성요소들 사이의 암호화된 연결 상태를 지원한다. PAVP를 사용함으로써, 시스템은 또한 콘텐츠를 시스템 구성요소들 사이의 전송 동안 및 메모리 내에서 보호할 수 있다.

[0010] GFX 엔진, PCH, 및 디스플레이(118) 사이의 인터페이스는 보호 유선/무선 디스플레이 링크들(120)에 의해 구현될 수 있다. 일 실시예에서, GFX 엔진으로부터 메모리를 경유하여 PCH를 통해 디스플레이로 송신되는 디스플레이 데이터는 고대역폭 디지털 콘텐츠 보호(HDCP:High-Bandwidth Digital Content Protection) 콘텐츠 보호 방식에 의해 보호될 수 있다. HDCP 사양은 디지털 엔터테인먼트 콘텐츠를 호환(compliant) 디지털 디스플레이들에 송신 및 수신하는 견고하고, 비용 효율적이며 투명한 방법을 제공한다. 실시예에서, 유선 링크는 Digital Content Protection, LLC로부터 이용가능한 HDCP 사양, 개정 2.0, 또는 후속 개정들에 따라 구현될 수 있다. HDCP는 디스플레이 데이터가 디스플레이포트, 디지털 비주얼 인터페이스(DVI:Digital Visual Interface), 고선명 멀티미디어 인터페이스(HDMI:High-Definition Multimedia Interface), 기가비트 비디오 인터페이스(GVIF:Gigabit Video Interface), 또는 통합 디스플레이 인터페이스(UDI:Unified Display Interface) 연결을 통해 이동할 때 데이터의 카피를 저지하기 위해 이용될 수 있다. HDCP 개정 2.0 사양은 최종 사용자들이 디스

플레이들, 장치들 및 홈 시어터 시스템들을 TCP/IP, USB, Wi-Fi 및 WirelessHD와 같은 표준 프로토콜들 및 인터페이스들을 통해 편리하게 연결시키는 최근 생겨난 사용 모델들을 다룬다. HDCP 개정 2.0 사양은 견고한 콘텐츠 보호를 위해 표준 기반 RSA 공개 키 및 고급 암호화 표준(AES) 128비트 암호화를 사용한다. HDCP 시스템에서, 2개 이상의 HDCP 장치들은 HDCP 보호 인터페이스를 통해 상호 연결된다. HDCP에 의해 보호되는 오디오비주얼 콘텐츠는 최고의 업스트림 HDCP 송신기에서 업스트림 콘텐츠 제어 기능으로부터 HDCP 시스템으로 흐른다. 거기서부터, HDCP 시스템에 의해 암호화되는 HDCP 콘텐츠는 HDCP 보호 인터페이스들을 통해 HDCP 수신기들의 트리형 토폴로지를 통과하여 흐른다.

[0011] HDCP 콘텐츠 보호 메커니즘은 3개의 요소들을 포함한다: 1) 그의 즉시 업스트림 연결(HDCP 송신기)에 대한 HDCP 수신기들의 인증. 인증 프로토콜은 HDCP를 수신하기 위해 주어진 HDCP 수신기가 라이센싱되는 것을 HDCP 송신기가 검증하는 메커니즘이다. 2) 무효가 되도록 DCP에 의해 결정되는 HDCP 수신기들의 철회. 3) HDCP 송신기들과 그의 다운스트림 HDCP 수신기들 사이의 HDCP 보호 인터페이스들을 통한 오디오비주얼 콘텐츠의 HDCP 암호화. HDCP 수신기들은 HDCP 콘텐츠를 인간 소비를 위한 오디오 및 비주얼 형태로 렌더링할 수 있다. HDCP 수신기들은 HDCP 콘텐츠를 하나 이상의 부가 HDCP 수신기들까지 더 먼 다운스트림으로 방출하는 다운스트림 HDCP 송신기들의 역할을 하는 HDCP 리피터들일 수 있다. 일 실시예에서, 디스플레이(118)에 송신되는 디스플레이 데이터는 802.11n 무선 근거리 통신망(WLAN) 기술을 사용하여 보호 무선 디스플레이(WiDi:wireless display) 링크(127)를 통해 송신될 수 있다.

[0012] 도 1에서 알 수 있는 바와 같이, 본 발명의 실시예들에서, 콘텐츠가 서비스 제공자 서버(104)로부터 수신될 때부터 콘텐츠가 디스플레이(118) 상에 디스플레이될 때까지, 어떤 암호 키 또는 콘텐츠도 비암호화된 형태로 컴퓨팅 시스템 상에 실행하는 임의의 소프트웨어 또는 비인가된 하드웨어에 이용가능하지 않다. 게다가, 비디오 데이터를 위한 메모리 보호는 복호화, 디코딩/인코딩, 합성 및 디스플레이 파이프라인들을 가로질러 전체 체인을 통해 제공된다. 이 능력은 전체 시스템 성능을 손상시키지 않고 전체 메모리 대역폭에서 제공된다.

[0013] 도 2는 본 발명의 실시예에 따른 서비스 제공자 서버(104) 및 보안 서비스 구성요소(202)의 도면이다. 실시예에서, 보안 서비스 구성요소(202)는 하나 이상의 서버들 및/또는 구성요소들을 포함할 수 있다. 실시예에서, 보안 서비스 구성요소는 클라이언트 컴퓨팅 시스템의 하나 이상의 구성요소들의 제조자에 의해 조작될 수 있다. 보안 서비스 구성요소는 현장에서 클라이언트 컴퓨팅 시스템들을 제어하는 능력들을 제공한다. 보안 서비스 구성요소는 제조 구성요소 및 배포 구성요소를 포함한다. 제조 구성요소는 인증서 발행 구성요소(218), 키 생성(Key Gen) 구성요소(220), 및 퓨즈 프로그래밍(Fuse Prog) 구성요소(222)를 포함한다. 인증서 발행(218)은 공개 키 인증서들을 클라이언트 컴퓨팅 플랫폼들 각각에 생성 및 발행한다. Key Gen(220)은 클라이언트 컴퓨팅 플랫폼들에 내장되는 개인 및 공개 키 쌍을 요구대로 생성할 책임이 있다. 퓨즈 프로그래밍(222)은 제조 작업장에서 퓨즈들을 적절한 값들을 사용하여 견고한 보안 방식으로 프로그래밍할 책임이 있다. 이 값들은 트러스트 앵커들(trust anchors) 및 키 래더들(key ladders)을 보안 프로세서 내에 구축하기 위해 클라이언트 컴퓨팅 플랫폼에 의해 사용될 것이다.

[0014] 배포 구성요소는 인증서 발행 구성요소(204), 키 생성(Key Gen) 구성요소(206), 및 철회 매니저(208)를 포함한다. 인증서(Cert) 발행 구성요소(204)는 디지털 인증서를 SP 서버 및 클라이언트 구성요소들에게 발행하여 그들에게 인가를 제공하여 서비스 배포를 위한 그러한 클라이언트 시스템들과 상호 작용한다. 키 생성(Key Gen) 구성요소(206)는 암호 서명 키 쌍, 루트 키 쌍, 디지털 인증서들, 및 그룹 공개 키들을 생성하고, 각 그룹에 대한 그룹 공개 키들에 서명한다. 철회 매니저(208)는 철회 리스트(RL:revocation list)에 추가되는 클라이언트 컴퓨팅 시스템들의 식별자들 및 서명들을 결정하고, RL을 갱신하며, 갱신된 RL들을 배포한다.

[0015] SP 서버(104)는 네트워크(201)(인터넷 등)를 통해 클라이언트 컴퓨팅 시스템과 통신한다. 서비스 제공자 서버는 SP 서버 애플리케이션(212) 및 SP 서버 에이전트(210)를 포함한다. SP 서버 애플리케이션은 콘텐츠 브라우징 능력들을 제공한다. SP 서버 에이전트(210)는 클라이언트 특정 메시지들의 송신을 제어하고, 암호 키들 및 인가된 사용자 토큰들을 관리하며, 콘텐츠 전달 서비스 상태를 유지한다(배포 목적들을 위해 212 및 210은 파이어월되고(firewalled) 분리되는 물리적으로 상이한 서버들일 수도 있음). 콘텐츠 암호화기(214)는 콘텐츠(102)를 수락하고 콘텐츠를 클라이언트 컴퓨팅 시스템으로의 보안 전달을 위해 암호화한다. 콘텐츠 서버(216)는 암호화된 콘텐츠를 클라이언트에 송신한다. 키 서버(226)는 타이틀 키들을 인증된 세션 내의 클라이언트 컴퓨팅 시스템들에 프로비저닝할 책임이 있다. 서버 인증서(224)는 클라이언트 컴퓨팅 시스템들과의 인증된 세션의 상호 인증 및 설정에 참여하기 위해 SP 서버 에이전트에 의해 사용된다. SP 서버 에이전트(210), 키 서버(226), 및 콘텐츠 서버(216) 사이의 통신 링크들은 적절히 수락된 정보 보안 실행들에 의해 보호된다. 키 서버는 최고의 네트워크 및 액세스 보호를 가져서 인가된 당사자들만이 그것에 도달할 수 있고 키 서버에 의해 관리

되는 키들이 외부 네트워크 엔티티들로부터의 공격자들로부터 분리되고 파이어월되는 것을 보장한다. SP 서버 에이전트 또는 키 서버는 서버 인증서(224)와 연관되는 개인 키에 액세스할 수 있다. 실시예에서, 이 개인 키 및 이 개인 키로 수행되는 모든 동작들은 서버 상의 하드웨어 보안 모듈(HSM:hardware security module)(도 2에 도시되지 않음)을 사용하여 보호된다.

[0016] 실시예에서, SP 서버와 함께 클라이언트 컴퓨팅 시스템을 인증하기 위해 사용되는 암호 방식은 제로 지식 증명들(zero-knowledge proofs)의 사용에 기초하여 사용자의 프라이버시를 보호하는 암호 인증 프로토콜을 포함한다. 실시예에서, 암호 인증 프로토콜은 강화된 프라이버시 ID(EPID) 방식, 강화된 철회 능력들을 갖는 직접적인 익명의 증명(DAA:Direct Anonymous Attestation) 방식을 포함한다. EPID는 공통 RSA(Rivest, Shamir, Adleman) - 모든 개인이 각각의 트랜잭션에 대해 고유하게 식별되는 공개 키 인프라스트럭처(PKI) 보안 구현들 - 의 프라이버시 문제들을 완화시킨다. 그 대신에, EPID는 원격 증명(attestation)의 능력을 제공하지만 단지 클라이언트 컴퓨팅 시스템을 특정 기술 세대로부터 구성요소(칩셋 등)를 갖는 것으로서 식별한다. EPID는 그룹 서명 방식이며, 한 그룹의 공개 키는 다수의 개인 키들에 대응하고, 개인 키들은 그룹 공개 키에 의해 검증되는 그룹 서명을 생성한다. EPID는 익명이고 링크가능하지 않은 보안 성질을 제공하며 - 2개의 서명들을 고려해 볼 때, 서명들이 1개 또는 2개의 개인 키들로부터 생성되는지를 판단할 수 없다. EPID는 또한 위조불가인(unforgeable) 보안 성질을 제공하며 - 개인 키 없이, 유효 서명을 생성할 수 없다.

[0017] 일반적으로, EPID와 보안 통신 채널을 설정하는 것은 이하와 같이 달성될 수 있다. 제1 당사자(클라이언트 컴퓨팅 시스템 등)는 EPID 인증서를 제2 당사자(서비스 제공자 서버 등)에게 송신한다. 제1 당사자의 아이덴티티를 결코 인식하지 못하고 단지 제1 당사자를 인식하는 것은 신뢰된 보안 프로세서를 갖는 컴퓨팅 플랫폼이며, 제2 당사자는 제1 당사자를 인증한다. 그 다음, 제1 당사자는 제2 당사자의 공개 키 인증서를 사용하여 제2 당사자를 인증한다. 제2 당사자는 프라이버시를 필요로 하지 않으므로, 제2 당사자의 공개 키 인증서는 EPID 인증서가 아닐 수 있다(그러나 그것은 EPID 인증서일 수도 있음). 그 다음, 당사자들은 디피 헬만(DH:Diffie-Hellman) 키 교환 협정을 시작할 수 있다.

[0018] DAA 및 EPID의 각종 적절한 실시예들은 본 명세서에 참조에 의해 포함되는 이하의 공동특허 출원들에 설명되어 있다: 일련 번호 제11/778,804호이고, 2007년 7월 7일자로 출원된 Ernest F. Brickell 및 Jingtao Li에 의한 "An Apparatus and Method of Direct Anonymous Attestation from Bilinear Maps"; 일련 번호 제12/208,989호이고, 2008년 9월 11일자로 출원된 Ernest F. Brickell 및 Jingtao Li에 의한 "An Apparatus and Method for a Direct Anonymous Attestation Scheme from Short-Group Signatures"; 및 일련 번호 제12/286,303호이고, 2008년 9월 29일자로 출원된 Ernest F. Brickell 및 Jingtao Li에 의한 "Direct Anonymous Attestation Scheme with Outsourcing Capability". 다른 실시예들에서, 다른 인증 및 증명 방식들이 사용될 수도 있다.

[0019] 클라이언트 컴퓨팅 시스템은 적어도 3개의 주요 구성요소들 - 호스트 소프트웨어, 칩셋 하드웨어/펌웨어, 및 CPU/GFX/미디어 엔진들 - 을 포함한다. 본 발명의 실시예들에서 호스트 소프트웨어가 신뢰되지 않은 것으로 가정된다. 호스트 소프트웨어가 공격을 당하더라도, 어떤 비밀들도 손상되지 않을 것이다. 호스트 소프트웨어는 SP 서버(104)로의 네트워크 연결에 책임이 있고 콘텐츠 서버(216)로부터 미디어를 다운로드할 책임이 있다. 호스트 소프트웨어는 다양한 SP 서버들과 칩셋 하드웨어/펌웨어 사이의 프록시의 역할을 한다. 호스트 소프트웨어는 칩셋 하드웨어/펌웨어가 타이틀 키 언랩(unwrap) 및 주입을 CPU/GFX 구성요소에 완료한 후에 암호화된 콘텐츠를 그래픽스 하드웨어에 직접 송신한다.

[0020] 칩셋 하드웨어/펌웨어는 모든 보호 처리에 책임이 있어, 콘텐츠 보호 처리에 대한 보호 장치의 역할을 취한다. 실시예에서, 칩셋 하드웨어/펌웨어는 DMI 메커니즘을 사용하여 보호 타이틀 키들을 그래픽스 하드웨어에 송신한다.

[0021] CPU/GFX 구성요소는 최종 스트림 복호화, 디코딩 및 디스플레이에 책임이 있다. GFX 엔진은 수동 장치이며, 어떤 정책도 결정하지 않는다. 요청될 때, GFX 엔진은 콘텐츠를 간단히 복호화하고, 그 후에 제출된 비디오 슬라이스들을 디코딩한다. 실시예에서, GFX 엔진(보호 미디어 인코더들을 가짐)은 HDCP 출력 보호를 위하여 디스플레이 콘텐츠를 HDMI 및 무선(예를 들어, WiDi) 디스플레이들을 통해 재암호화한다.

[0022] 보호 클라이언트 컴퓨팅 시스템은 매우 민감한 정보를 송신하기 전에 서비스 제공자에 의해 원격으로 식별되어야 한다. 플랫폼을 식별하기 위해 사용되는 메커니즘은 사용자 프라이버시를 침해하지 않아야 한다. 본 발명의 실시예들은 서비스 제공자 서버가 적절한 클라이언트 컴퓨팅 시스템에 통신하고 있는 것을 네트워크를 통해 검증하고 타이틀 키들 및 다른 비밀 자료를 그 클라이언트 컴퓨팅 시스템에 전송하기 위해 보호 메커니즘을 서비스 제공자에게 제공한다. 일 실시예에서, 서비스 제공자 서버와 클라이언트 컴퓨팅 시스템 사이의 보호 세션

을 설정하기 위해 이용되는 프로토콜은 EPID이다. EPID는 N-개인 키들에 의해 생성되는 서명을 소위 EPID 그룹에서 익명으로 검증하기 위해 단일 공개 키를 고려한다. EPID를 구현하기 위해, 각각의 칩셋은 실리콘 제조 동안 플랫폼 제어 허브(PCH) 퓨즈들에 블로잉되는(blown) 고유 개인 키를 포함한다. 실시예에서, 칩셋 제조자는 1,000,000개의 개인 키들을 단일 그룹에 배치하고 제조되는 각각의 칩셋에 대해 400개의 그룹들을 생성한다. EPID 검증기의 역할을 하기 위해, 각각의 서비스 제공자에게는 이 400개의 공개 키들이 프로비저닝될 것이다.

[0023] 보호 EPID 세션이 설정되어 있다면, 서비스 제공자 서버는 보호 비밀 정보를 보호 클라이언트 컴퓨팅 시스템과 자유롭게 교환할 수 있다. 콘텐츠 스트리밍을 위해, 보호 타이틀 키들은 SP 서버로부터 칩셋 내의 보안 프로세서로 전달될 수 있다. 보안 프로세서는 보호 타이틀 키들을 그래픽스 및 오디오 하드웨어에 송신한다. 이 점에서, 암호화된 비디오 및 오디오 콘텐츠는 콘텐츠 서버(216)로부터 콘텐츠를 복호화, 디코딩, 및 디스플레이하는 클라이언트 컴퓨팅 시스템 그래픽스 및 오디오 하드웨어로 직접 송신될 수 있다. 콘텐츠를 다운로딩하기 위해, 보안 프로세서는 고유 플랫폼 저장 키를 사용하여 타이틀 키들을 클라이언트 컴퓨팅 시스템에 바인딩시키고 (다시 제조 동안 PCH 퓨즈들에 버닝됨(burned)) 바인딩된 키들을 미디어 플레이어 소프트웨어에 리턴시킨다. 재생이 요구될 때, 바인딩된 타이틀 키들은 보안 프로세서에 다시 제출되며, 보안 프로세서는 그들을 보호 방식으로 바인딩 해제(unbind)시키고 그래픽스 및 오디오 하드웨어에 송신한다.

[0024] 도 3은 본 발명의 실시예에 따른 클라이언트 컴퓨팅 시스템(101)의 도면이다. 서비스 제공자(SP) 플레이어/미디어 브라우저 소프트웨어 애플리케이션(302)은 인터넷과 같은 네트워크(201)를 통해 SP 서버(104)와 인터페이스하기 위해 소프트웨어 스택에 포함될 수 있다. SP 플레이어/미디어 브라우저(302)는 사용자가 서비스 제공자의 콘텐츠 오퍼링들(offerings)을 브라우징하고 SP 서버로부터 클라이언트 컴퓨팅 시스템으로 전달되는 콘텐츠를 선택하는 것을 허용한다. SP 플레이어/미디어 브라우저는 콘텐츠 라이브러리를 관리하고 콘텐츠의 선택, 다운로딩, 및 재생을 제어하기 위해 사용자 인터페이스 제어들을 사용자에게 제공한다. SP 플레이어/미디어 브라우저는 서비스 에이전트(304)와 상호 작용한다. 서비스 에이전트(304)는 본 발명의 실시예들에 따른 단 대 단 콘텐츠 보호를 지원하는 클라이언트 컴퓨팅 시스템의 특징들에 액세스하기 위해 인가되는 서비스 제공자에 의해 제공되는 소프트웨어 애플리케이션을 포함한다. 서비스 에이전트는 다양한 SP 플레이어/미디어 브라우저 애플리케이션 프로그래밍 인터페이스들(API들)(도 2에 도시되지 않음)과 인터페이스한다. 서비스 에이전트(304)는 미디어 플레이어 구성요소(306)를 포함한다. 미디어 플레이어는 콘텐츠 플레이어 기능성을 제공한다(예를 들어, 재생을 제어함).

[0025] SP 클라이언트 애플리케이션(308)은 SP 플레이어/미디어 브라우저(302) 및 서비스 에이전트(304)가 클라이언트 컴퓨팅 시스템의 하드웨어 및 펌웨어 상의 콘텐츠 보호 특징들에 액세스하고 메시지들을 서비스 제공자 서버(104)에 중계할 수 있게 한다. 실시예에서, SP 클라이언트 애플리케이션은 콘텐츠 보호 API들을 포함하는 호스트 에이전트 소프트웨어 개발 키트(SDK)를 포함한다. 실시예에서, SP 클라이언트 애플리케이션은 칩셋의 플랫폼 제어 허브(PCH)(312) 내의 보안 프로세서(314)와 통신한다.

[0026] 오디오 드라이버(311)는 미디어 플레이어와 오디오 복호화 하드웨어(316) 사이에 인터페이스를 제공한다. 유사하게, 그래픽스(GFX) 드라이버(310)는 미디어 플레이어와 GFX 엔진(320) 사이에 인터페이스를 제공한다. 실시예에서, PCH(312)는 보안 프로세서(314)를 포함하며, 보안 프로세서는 펌웨어를 실행시켜 다른 공지된 시스템 기능들과 함께, 콘텐츠 보호 기능성을 제공한다. 실시예에서, 보안 프로세서는 매니지어빌리티 엔진(ME)에 의해 구현될 수 있다. 콘텐츠가 PCH(312) 및 GFX 엔진(320)에 의해 취급될 때, 콘텐츠는 PCH 하드웨어/펌웨어 및 GFX 엔진 하드웨어 각각 내의 보호 오디오 비디오 경로(PAVP) 구성요소들(318, 322)에 의해 적어도 부분적으로 보호될 수 있다.

[0027] 도 4는 본 발명의 실시예에 따른 보안 콘텐츠 처리의 흐름도이다. 블록(402)에서, 클라이언트 컴퓨팅 시스템의 사용자는 하나 이상의 서비스 제공자들로부터 콘텐츠를 브라우징하고, 발견하며, 구입하기 위해 SP 플레이어/미디어 브라우저(302)를 사용한다. 블록(404)에서, SP 서버(104) 및 클라이언트 컴퓨팅 플랫폼(101)의 상호 인증이 수행된다. 인증된 세션이 설정된다. 주어진 콘텐츠 세트에 대한 사용 권리들을 갖는 키 블랍들(key blobs)이 프로비저닝된다. 키 블랍들은 클라이언트 컴퓨팅 시스템에 바인딩되어 시스템이 필요에 따라 보호되는 비밀성(confidentiality) 및 무결성(integrity) 둘 다의 것임을 보장한다.

[0028] 그 다음, 블록(406)에서 클라이언트 컴퓨팅 시스템은 암호화된 콘텐츠를 콘텐츠 서버(216)로부터 네트워크(201)를 통해(스트리밍 동작을 위함) 또는 (이전에 구입되고, 다운로딩되며, 저장되는 콘텐츠에 대한) 클라이언트 컴퓨팅 시스템 상의 로컬 스토리지로부터 획득한다. 비디오 슬라이스들(예를 들어, 서브프레임)에 작업하기 위해 시스템이 준비된다. 그 결과, 하드웨어는 데이터의 제1 슬라이스가 제출되자마자 데이터를 처리할 수 있다.

[0029] 블록(408)에서, 사용자는 SP 플레이어/미디어 브라우저(302)를 사용하여 선택된 콘텐츠의 재생을 개시한다. 키 블랍은 타이틀 키의 언패킹(unpacking) 및 추출을 위해 보안 프로세서(314)에 제출된다. 그것이 수행될 때, 타이틀 키는 보안 프로세서에 의해 그래픽스 하드웨어(320)로 복호화를 위해 로드된다. 블록(410)에서 SP 플레이어/미디어 브라우저는 암호화된 콘텐츠를 GFX 엔진(320) 내의 미디어 처리 엔진에 제출한다. GFX 엔진은 타이틀 키들을 사용하여 콘텐츠를 복호화하고 로컬 보호 키를 사용하여 콘텐츠를 재암호화한다. 재암호화된 데이터는 보호 로컬 또는 시스템 메모리에 저장될 수 있다. 재암호화된 콘텐츠는 블록(414)에서 이어서 획득되고, 복호화되며, 압축해제된다. 복호화가 우선 수행된다. 데이터가 복호화되면, 데이터가 디코딩/압축해제된다. 데이터가 압축해제되면, 데이터는 재암호화되고 시스템 메모리를 통해 합성 엔진에 전달된다. 합성이 완료되면, 데이터는 다시 보호되고 시스템 메모리를 사용하여 디스플레이 엔진에 전달된다. 실시예에서, 방식에 따른 각각의 구성요소는 필요에 따라 복호화, 처리 및 재암호화하는 능력을 갖는다.

[0030] 블록(416)에서, GFX 엔진은 HDCP 기술(실시예에서)을 사용하여 미디어 콘텐츠를 재암호화하고 콘텐츠를 사용자에 의해 보여지는 디스플레이에 전달한다. 프로세스의 각각의 단계에서, 콘텐츠는 그것이 클라이언트 컴퓨팅 시스템 상에서 실행하는 소프트웨어 또는 비인가된 하드웨어 구성요소들에 의해 액세스가능한 클리어로 결코 있지 않는다.

[0031] 도 5는 본 발명의 실시예에 따른 보안 콘텐츠 처리 시스템의 도면이다. SP 서버(104)는 네트워크(201)를 통해 클라이언트 컴퓨팅 시스템(101)과 상호 작용한다. 클라이언트 컴퓨팅 시스템은 제1 구성요소(500) 및 제2 구성요소(502)를 포함한다. 실시예에서, 제1 구성요소는 CPU 및 GFX 구성요소를 포함하고, 제2 구성요소는 플랫폼 제어 허브(PCH)를 포함한다. 다른 실시예에서, 제1 및 제2 구성요소들은 시스템 온 칩(SOC) 구현 내의 단일 구성요소로 결합될 수 있다. 제1 구성요소(500)는 복수의 프로세서 코어들(504), 및 GFX 엔진(320)을 포함한다. 프로세서 코어들(504)은 호스트 소프트웨어(SW)(506)(도 3에 도시된 바와 같음), 클라이언트 인증서(508), 퓨즈들(521), 및 공유 비밀(519)의 다양한 구성요소들을 실행시킨다. 호스트 SW는 SP 서버 또는 유형 매체(DVD, 블루 레이, 또는 다른 저장 기술 등), 하드 디스크 드라이브(HDD)/ 고체 상태 드라이브(SSD)(510)로부터 이전에 획득되는 암호화된 콘텐츠를 포함하는 데이터를 판독한다. 실시예에서, 호스트 SW는 적어도 SP 플레이어/미디어 브라우저 애플리케이션(302), 서비스 에이전트(304), 및 SP 클라이언트 애플리케이션(308)을 포함한다.

[0032] GFX 엔진(320)은 복수의 구성요소들을 포함한다. 미디어 암호화/복호화 엔진(520)은 콘텐츠를 암호화 및 복호화하는 로직을 포함한다. 미디어 인코딩/디코딩 엔진(522)은 콘텐츠를 인코딩 및 디코딩하는 로직을 포함한다. GFX 합성(Comp) 엔진(524)은 디스플레이 이미지들을 구성하는 로직을 포함한다. 디스플레이 엔진(526)은 합성된 디스플레이 이미지들을 디스플레이에 전달하는 로직을 포함한다. 디스플레이 암호화/복호화 엔진(528)은 디스플레이 데이터를 보호 링크(527)를 통해 디스플레이(538)에 송신하기 전에 디스플레이 데이터를 암호화 및 복호화하는 로직을 포함한다. 메모리 암호화/복호화 엔진(530)은 메모리(536) 내의 보호 중간 표면들(534)에 저장되는 데이터를 암호화 및 복호화하는 로직을 포함한다. 메모리(536)는 또한 비밀성 및 무결성 보호 메모리 동작들(532)을 구현하는 로직을 포함한다.

[0033] 제2 구성요소(502)는 복수의 구성요소들을 포함하며, 그의 일부는 도 5를 간소화하기 위해 도시되지 않는다. 제2 구성요소는 보안 프로세서(314)를 포함한다. 보안 프로세서는 클라이언트 컴퓨팅 시스템에 대한 증명, 프로비저닝 키 관리, 및 출력 제어 동작들(516)을 제공하기 위해 펌웨어 및/또는 하드웨어 로직을 포함한다. 보안 프로세서는 또한 검증 키들 및 키 계층 정보와 같은 PKI를 지원하기 위해 퓨즈들(517), 공유 비밀(519), 및 트러스트 앵커들(518)을 포함한다. 퓨즈들(521, 517)은 EPID 사용을 위한 키 재료에 의한 칩셋의 제조 동안 제1 및 제2 구성요소들의 하드웨어에 프로그래밍된다. 하드웨어 신뢰 루트는 클라이언트 컴퓨팅 시스템이 제조될 때 제조 작업장 상의 퓨즈들에 프로그래밍되는 정보로부터 구축된다. 이것은 각각의 개별 클라이언트 컴퓨팅 시스템이 고유하고, 게다가 프라이버시 보호되는 것을 보장한다. 공유 비밀(519)은 칩셋 및 CPU/GFX 구성요소들의 제조 동안 제1 및 제2 구성요소들의 하드웨어에 하드코딩된다. 실시예에서, 공유 비밀은 보안 칩 대 칩 통신 채널을 DMI 링크(538)를 통해 설정하는데 사용될 수 있다.

[0034] 클라이언트 컴퓨팅 시스템은 또한 보안 클록 서비스들을 제공하는 보호 실시간 클록(513), 디스플레이(538), 및 비휘발성 메모리(NVM)(512)를 포함한다. 실시예에서, 보호 실시간 클록은 제3자에 의해 배정(seed)될 수 있고, 다수의 서비스 제공자들을 위해 가상화될 수 있다. 제2 구성요소를 위한 펌웨어 이미지를 저장할 뿐만 아니라, 보안 프로세서 처리 동작들을 위한 일시적 데이터(무결성 및 상태 정보 등)을 저장하기 위해 NVM이 사용될 수 있다.

[0035] 실시예에서, 처리 흐름이 이하와 같이 설명될 수 있다. SP 플레이어/미디어 브라우저(302)는 사용자 인터페이

스를 사용자에게 제공한다. 사용자는 이용가능한 콘텐츠를 브라우징하기 위해 서비스 제공자의 웹 사이트로 진행한다. SP 웹 사이트는 사용자의 클라이언트 컴퓨팅 시스템이 그것 내에 SP 서버(104)와 함께 인증하는 능력을 통합했는지를 판단하는 자동 검출 능력을 갖는다. 할 수 있다면, 사용자는 콘텐츠를 선택하는 것이 허용된다. 콘텐츠는 구입되거나, 임대되거나, 가입될 수 있거나, 또는 스트리밍될 수 있다. 사용자는 콘텐츠의 대금을 지불한다. SP 플레이어/미디어 브라우저(302)는 클라이언트 컴퓨팅 시스템(101)을 SP 서버(104)와 함께 인증하기 위해 보안 프로세서(316)를 호출한다. 실시예에서, 인증은 EPID 기술을 사용한다. 클라이언트 컴퓨팅 시스템(101)은 SP 서버(104)가 클라이언트 컴퓨팅 시스템의 인증서(508)를 검증하고, 철회 체크를 수행하고, 인증 경로를 인증 기관(일 실시예에서 EPID 프로토콜을 사용함)에 검증하게 함으로써 적어도 부분적으로 인증된다. 클라이언트 컴퓨팅 시스템(101) 및 SP 서버(104) 둘 다가 인증될 때, 보안 통신 채널은 일 실시예에서 EPID 프로토콜에 기초하여 설정될 수 있다. 실시예에서, 보안 통신 채널이 설정되면, 커맨드 세트는 단 대 단 콘텐츠 보호 능력들에 사용될 수 있다.

[0036] SP 서버(104)는 콘텐츠의 사용 제약들(예를 들어, 시간)이 있는 경우, 암호화된 타이틀 키를 클라이언트 컴퓨팅 시스템에 프로비저닝한다. SP 서버는 암호화된 타이틀 키를 보안 채널을 통해 보안 프로세서(314)에 송신한다. 보안 프로세서(314)는 그 자체의 키 계층을 사용하여 암호화된 타이틀 키를 복호화한다. 보안 프로세서(314)는 새롭게 복호화된 타이틀 키를 재암호화하여 키 블랍을 형성하기 위해 저장 키를 사용한다. 키 블랍은 지정된 시간 기간 동안 클라이언트 컴퓨팅 시스템에 바인딩된다. 보안 프로세서(314)는 키 블랍을 CPU 코어에서 실행하는 SP 플레이어/미디어 브라우저(302)에 송신한다. SP 플레이어/미디어 브라우저(302)는 키 블랍을 HDD/SSD(510)에 저장한다. 그 다음, SP 플레이어/미디어 브라우저(302)는 사용자 선택 암호화된 콘텐츠를 다운로딩한다. 일 실시예에서, 다운로딩된 암호화된 콘텐츠는 HDD/SSD(510)에 저장될 수 있다.

[0037] 사용자가 콘텐츠를 플레이하기를 원할 때, SP 플레이어/미디어 브라우저(302)는 키 블랍을 다시 보안 프로세서(314)에 제출한다. 보안 프로세서는 키 블랍의 서명을 검증하고, 예를 들어 시간과 같은 사용 제약들을 체크한다. 보안 프로세서(314)는 암호화된 타이틀 키를 암호화된 채널(예를 들어, DMI 링크(538))을 통해 GFX 엔진(320)의 미디어 암호화/복호화 구성요소(520)에 송신한다. 보안 프로세서는 SP 플레이어/미디어 브라우저에게 GFX/미디어 엔진이 암호화된 콘텐츠를 처리할 준비를 하라고 명령한다. SP 플레이어/미디어 브라우저(302)는 암호화된 콘텐츠를 HDD/SDD(510)로부터 판독하거나, 암호화된 콘텐츠를 SP 서버(104)로부터 네트워크(201)를 통해 획득하고(스트리밍 애플리케이션을 위함), 암호화된 콘텐츠를 GFX 엔진에 슬라이스 바이 슬라이스(slice by slice)로 송신한다.

[0038] GFX 엔진(320)은 암호화된 콘텐츠를 슬라이스 바이 슬라이스 방식으로 처리한다. 각각의 슬라이스에 대해, SP 플레이어/미디어 브라우저는 슬라이스 헤더들을 클리어에서 판독한다. 슬라이스의 나머지는 SP 플레이어/미디어 브라우저가 콘텐츠에 액세스할 수 없도록 암호화된다. SP 플레이어/미디어 브라우저는 초기화 벡터를 사용하여 재생 상태 정보의 트랙을 유지한다. 미디어 암호화/복호화 엔진(520)은 보안 프로세서로부터 수신되는 암호화된 타이틀 키를 복호화한 후에, 타이틀 키를 사용하여 콘텐츠를 복호화한다. 일 실시예에서, 미디어 암호화/복호화 엔진의 출력 데이터는 여전히 공지된 H.264 인코딩 방식에 따라 압축된다. 다른 실시예들에서, 다른 인코딩 방식들이 사용될 수 있다. 미디어 인코딩/디코딩 엔진(522)은 각각의 슬라이스를 디코딩하고 그 후에 메모리 암호화/복호화(530)를 사용하여 슬라이스를 재암호화한다. 재암호화된 콘텐츠 슬라이스는 메모리(536) 내의 보호 중간 표면들(534)에 저장된다. GFX 합성 엔진(524)은 전경 및 배경 이미지들, 윈도우들 등을 포함하는 디스플레이 상에 디스플레이되는 이미지의 합성을 제어한다. GFX 합성 엔진은 합성된 이미지를 생성하기 위해 메모리(536) 내의 보호 중간 표면들(534)로부터 재암호화된 콘텐츠 슬라이스들을 획득한다. GFX 합성 엔진(524)은 합성된 이미지 데이터를 디스플레이 엔진(526)에 송신한다.

[0039] 디스플레이 엔진은 콘텐츠 슬라이스들을 메모리(536)에 저장하기 위해 사용되었던 암호화로부터 합성된 이미지를 복호화하기 위해 디스플레이 암호화/복호화 엔진(528)을 사용한다. 디스플레이 엔진(526)은 일 실시예에서 합성된 이미지 데이터를 HDCP 기술에 따라 재암호화하기 위해 디스플레이 암호화/복호화 엔진을 사용한다. 암호화된 합성 이미지 데이터는 GFX 엔진(320)에 의해, 보호 칩 대 칩 데이터 인터페이스(예를 들어, DMI 링크)(538)를 통해 제2 구성요소(502)에 송신되어, 보호 디스플레이 인터페이스 링크(527)를 통해 디스플레이(538)에 전송된다.

[0040] 실시예에서, 클라이언트 컴퓨팅 시스템에 의해 처리되는 임의의 수의 동시발생하는 독립 콘텐츠 스트림들이 있을 수 있다. 각각의 콘텐츠 스트림은 다른 스트림들과 간섭되지 않도록 그 자체의 암호 컨텍스트(cryptographic context)를 갖는다. 이것은 또한 클라이언트 컴퓨팅 시스템이 하나의 스트림에 관한 임의의 종

류의 공격 또는 손상이 다른 콘텐츠 스트림들에 영향을 미치지 않는 것을 보장하게 할 수 있다.

[0041] 본 발명의 실시예들은 이하의 사용 모델들을 지원한다:

[0042] 1. 고선명(HD)/표준 선명(SD)/이동 선명(PD, Portable Definition) 콘텐츠 타이틀들의 다운로딩. 서비스 제공자들은 콘텐츠를 주어진 클라이언트 컴퓨팅 시스템에 대해 올바른 포맷으로 배포한다. 사용자들은 물리적 광 디스크들(DVD 또는 블루 레이 디스크들 등)을 획득하는 대신에 콘텐츠 타이틀의 전자 카피를 선택할 수 있다.

[0043] 2. HD/SD/PD 콘텐츠 타이틀들의 스트리밍. 서비스 제공자들은 필요에 따라 세션을 설정하고 콘텐츠를 클라이언트 컴퓨팅 시스템에 스트리밍할 수 있다. 클라이언트 컴퓨팅 시스템은 콘텐츠 소비 경험의 전체 기간 동안 서비스에 계속 연결되어 있다.

[0044] 3. HD/SD/PD 콘텐츠 타이틀들의 임대. 서비스 제공자들은 타이틀들을 설정된 시간 기간 동안 온 디맨드(on-demand) 방식으로 소비자들에게 임대할 수 있다. 보호 및 정책 집행은 본 발명의 실시예에 의해 수행된다.

[0045] 4. 콘텐츠 타이틀들의 시간 기반 언록킹(unlocking). 서비스 제공자들은 콘텐츠 릴리스 일자 또는 가용성 스케줄보다 빨리 콘텐츠를 클라이언트 컴퓨팅 시스템들에 푸시하고 클라이언트 컴퓨팅 시스템이 주어진 장래 시간에 사용하기 위해 타이틀을 언록킹하게 할 수 있다.

[0046] 5. 사용자의 장치 배치(constellation) 및 용이한 공유. 본 발명의 실시예들은 클라이언트 컴퓨팅 시스템들의 "도메인"을 주어진 사용자에게 제공한다. 이것은 콘텐츠가 사용자의 도메인 내의 이 인가된 장치들 사이에서 자유롭게 흐를 수 있게 한다.

[0047] 6. 오프라인 트랜잭션들. 본 발명의 실시예들은 트랜잭션을 나중의 조정 동안 기록하는 능력을 제공한다. 이것은 서비스 제공자들이 콘텐츠를 클라이언트 컴퓨팅 시스템들에 미리 로드하거나 추측하여(speculatively) 배포하고 그들이 인터넷에 연결되었는지 여부의 트랜잭션을 완료하는 것을 허용한다.

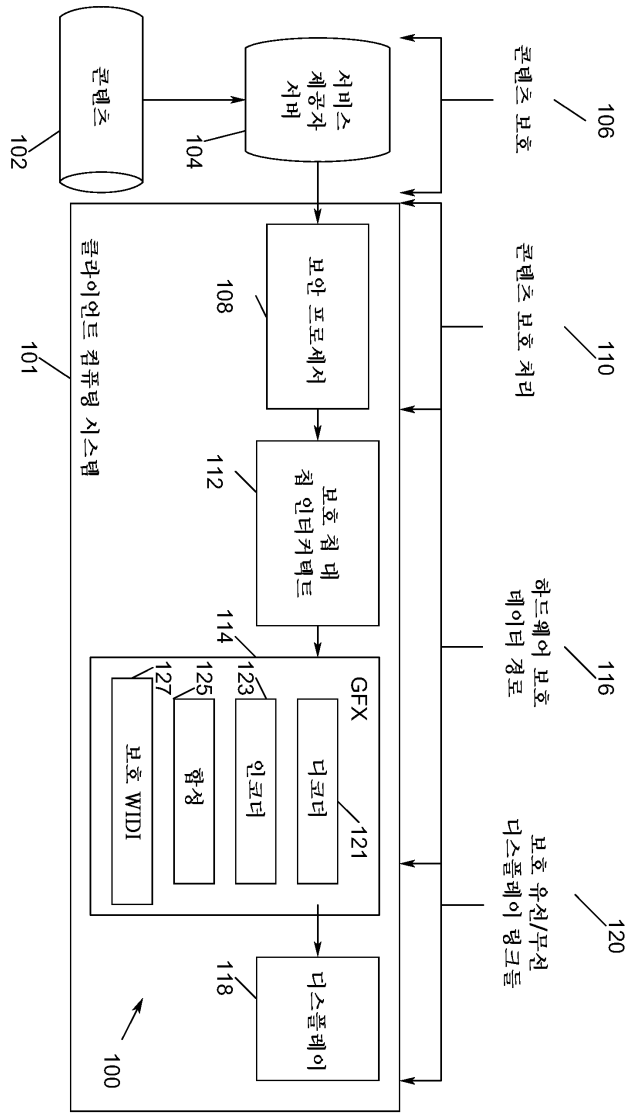
[0048] 본 명세서에서 "일 실시예" 또는 "하나의 실시예"에 대한 언급은 실시예와 관련하여 설명되는 특정 특징, 구조, 또는 특성이 적어도 구현에 포함될 수 있는 것을 의미한다. 본 명세서 내의 다양한 위치들에서 "일 실시예에서"라는 구의 출현들은 모두 동일한 실시예를 지칭할 수 있거나 지칭하지 않을 수 있다.

[0049] 또한, 설명 및 청구항들에서, "결합된" 및 "연결된"이라는 용어들이 그의 파생어들과 함께, 사용될 수 있다. 본 발명의 일부 실시예들에서, 2개 이상의 요소들이 서로 직접 물리적으로 또는 전기적으로 접촉되는 것을 나타내기 위해 "연결된"이 사용될 수 있다. "결합된"은 2개 이상의 요소들이 직접 물리적으로 또는 전기적으로 접촉되는 것을 의미할 수 있다. 그러나, "결합된"은 2개 이상의 요소들이 서로 직접 접촉되지 않을 수 있지만, 여전히 서로 협력하거나 상호 작용할 수 있는 것을 의미할 수도 있다.

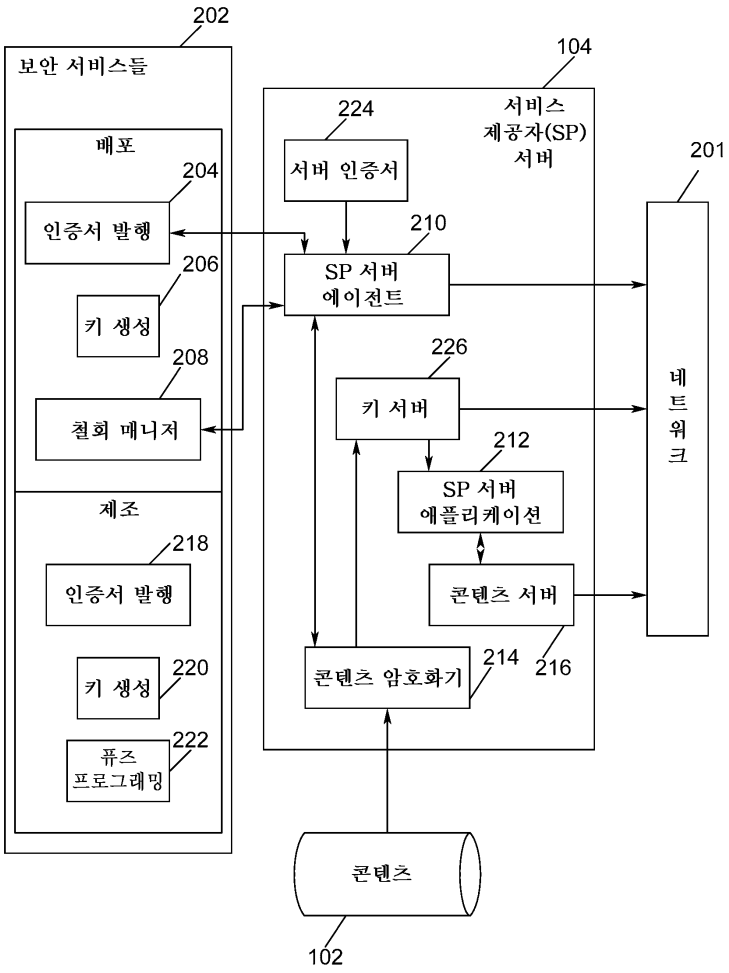
[0050] 따라서, 본 발명의 실시예들은 구조적 특징들 및/또는 방법론적 동작들에 특정되는 언어로 설명되었을지라도, 청구된 발명 대상은 설명되는 특정 특징들 또는 동작들에 제한되지 않을 수 있다는 점이 이해되어야 한다. 오히려, 특정 특징들 및 동작들은 청구된 발명 대상을 구현하는 샘플 형태들로서 개시된다.

도면

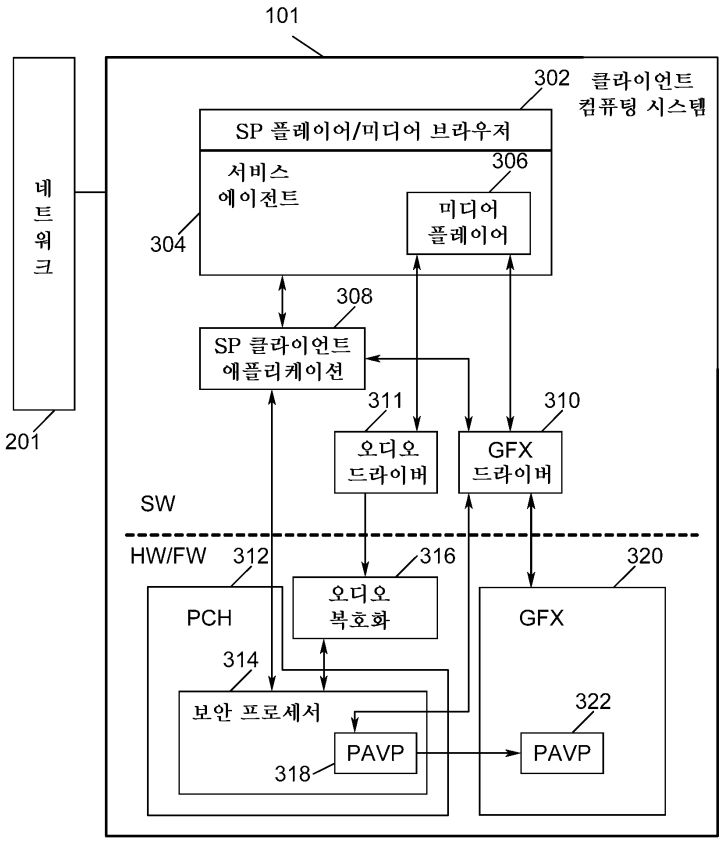
도면1


콘텐츠
102
서비스 제공자 서버
104
콘텐츠 보호
106
클라이언트 컴퓨팅 시스템
101
보안 프로세서
108
콘텐츠 보호 처리
110
보호 채널 인터커넥트
112
하드웨어 보호 데이터 경로
116
GFX
114
디코더
121
인코더
123
합성
125
보호 WIDI
127
보호 유선/무선 디스플레이 링크들
120
디스플레이
118
100

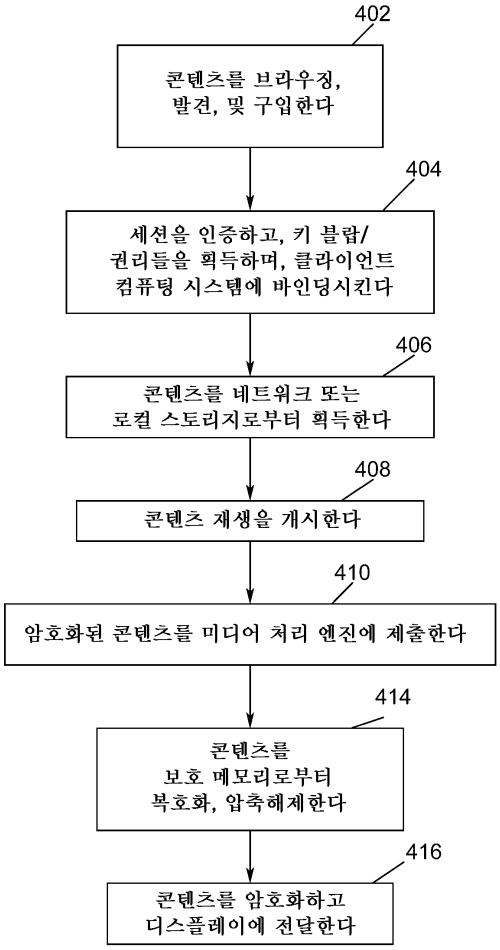
도면2


202
보안 서비스들
배포
204
인증서 발행
206
키 생성
208
철회 매니저
제조
218
인증서 발행
220
키 생성
222
퓨즈 프로그래밍
104
서비스 제공자(SP) 서버
224
서버 인증서
210
SP 서버 에이전트
226
키 서버
212
SP 서버 애플리케이션
콘텐츠 서버
214
콘텐츠 암호화기
216
201
네트워크
콘텐츠
102

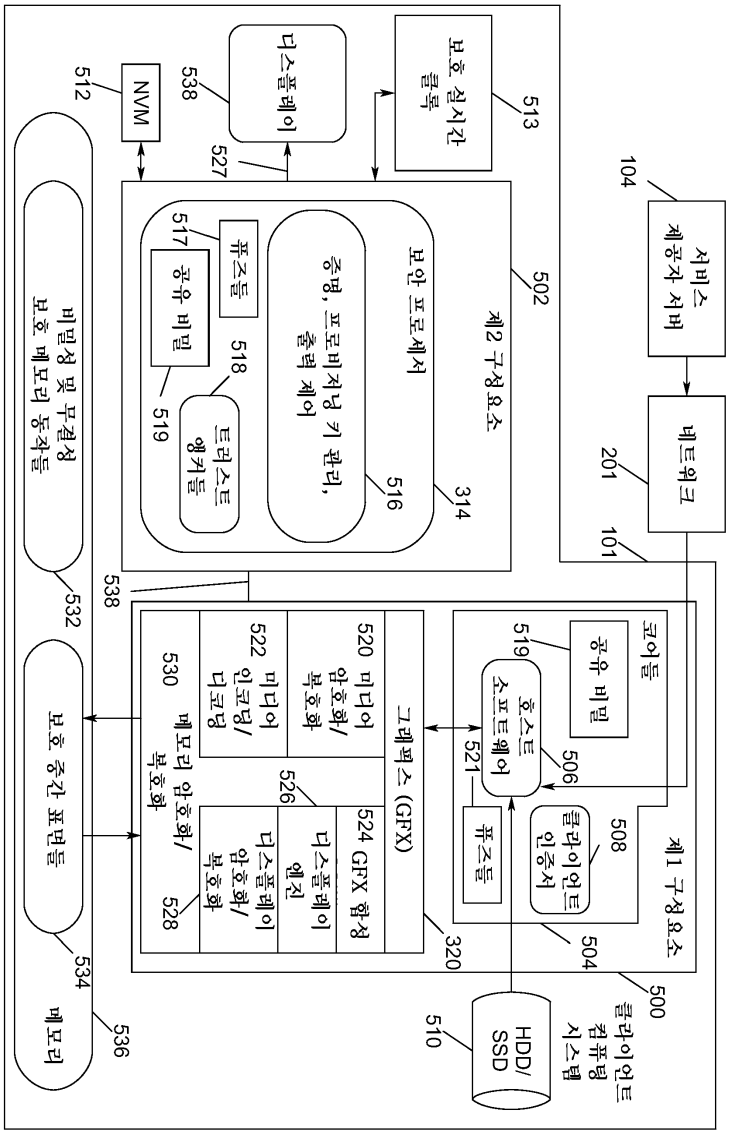
도면3


101
302
클라이언트
컴퓨팅 시스템
SP 플레이어/미디어 브라우저
서비스
에이전트
306
미디어
플레이어
304
308
SP 클라이언트
애플리케이션
311
310
오디오
드라이버
GFX
드라이버
네
트
워
크
201
SW
HW/FW
312
316
320
PCH
오디오
복호화
GFX
314
보안 프로세서
322
PAVP
PAVP
318

도면4


402
콘텐츠를 브라우징,
발견, 및 구입한다
404
세션을 인증하고, 키 블랍/
권리들을 획득하며, 클라이언트
컴퓨팅 시스템에 바인딩시킨다
406
콘텐츠를 네트워크 또는
로컬 스토리지로부터 획득한다
408
콘텐츠 재생을 개시한다
410
암호화된 콘텐츠를 미디어 처리 엔진에 제출한다
414
콘텐츠를
보호 메모리로부터
복호화, 압축해제한다
416
콘텐츠를 암호화하고
디스플레이에 전달한다

도면5


서비스 제공자 서버
104
네트워크
201
101
클라이언트 컴퓨팅 시스템
500
제1 구성요소
504
코어들
519
공유 비밀
호스트 소프트웨어
506
521
퓨즈들
508
플라이언트 인증서
HDD/ SSD
510
320
그래픽스 (GFX)
520 미디어 암호화/ 복호화
522 미디어 인코딩/ 디코딩
530 메모리 암호화/ 복호화
524 GFX 합성 엔진
526
디스플레이 암호화/ 복호화
528
538
제2 구성요소
502
보안 프로세서
314
증명, 프로비저닝 키 관리, 출력 제어
516
퓨즈들
518
공유 비밀
517
519
트러스트 앵커들
보호 실시간 클록
513
디스플레이
538
527
NVM
512
비밀성 및 무결성 보호 메모리 동작들
532
보호 중간 표면들
534
메모리
536