(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년05월14일
(11) 등록번호 10-0897075
(24) 등록일자 2009년05월04일

(51) Int. Cl.
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2007-7001023
(22) 출원일자 2007년01월15일
심사청구일자 2007년01월15일
번역문제출일자 2007년01월15일
(65) 공개번호 10-2007-0019790
(43) 공개일자 2007년02월15일
(86) 국제출원번호 PCT/US2005/024253
국제출원일자 2005년07월08일
(87) 국제공개번호 WO 2006/019614
국제공개일자 2006년02월23일
(30) 우선권주장
10/892,280 2004년07월14일 미국(US)
(56) 선행기술조사문헌
US20040103281 A1
MENEZES, VANSTONE, OORSCHOT, "Handbook of Applied Cryptography", pp.321-331,388-398, 1999
US6032260 A
전체 청구항 수 : 총 45 항

(73) 특허권자
인텔 코오퍼레이션
미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
서튼, 제임스, 2세
미국 97229 오레곤주 포틀랜드 노스웨스트 폴리나 드라이브 20205
할, 클리포드
미국 95662 캘리포니아주 오렌지베일 이스트사이드 코트 6940
(뒷면에 계속)
(74) 대리인
백만기, 이중희, 주성민

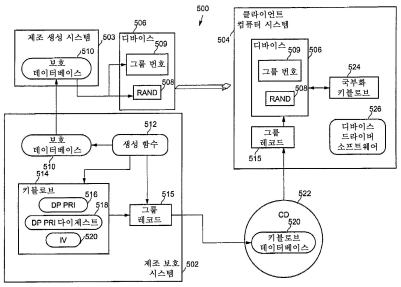
심사관 : 양종필

(54) 배포 CD를 사용하는 장치에 서명 그룹의 다이렉트 증명개인 키들을 전달하는 방법

(57) 요 약

본 분야에서 클라이언트 컴퓨터 시스템에 설치된 디바이스에 서명 키 그룹의 다이렉트 증명 개인 키를 전달하는 것은 디바이스에서 중요한 비휘발성 스토리지를 요구하지 않고 안전한 방식으로 달성될 수도 있다. 유일한 유사 랜덤 생성 값은 제조시 디바이스의 그룹 번호와 함께 생성 및 저장된다. 유사 랜덤 생성 값은 다이렉트 증명 개인 키 및 디바이스와 관련된 개인 키 다이제스트를 홀드하는 데이터 구조를 암호화하기 위한 대칭 키를 생성하는데 사용된다. 결과적인 암호화 데이터 구조는 서명 키 그룹(예를 들어, 서명 그룹 레코드)로 이동식 기억 매체(예를 들어, CD 또는 DVD)에 저장되고, 클라이언트 컴퓨터 시스템의 소유자에게 분배된다. 디바이스가 클라이언트 컴퓨터 시스템에서 초기화될 때, 시스템은 국부화되고 암호화 데이터 구조가 시스템에 존재하는지를 체크한다. 존재하지 않으면, 시스템은 이동식 기억 매체로부터 암호화 데이터 구조들의 관련 서명 그룹 레코드를 획득하고, 서명 그룹 레코드를 검증한다. 그룹 레코드가 유효할 때, 디바이스는 저장된 유사 랜덤 생성 값으로부터 재생된 대칭 키를 사용해서 암호화 데이터 구조를 해독해서, 다이렉트 증명 개인 키를 획득한다. 개인 키가 유효하면, 클라이언트 컴퓨터 시스템에서 디바이스에 의한 차후 인증 프로세싱에 사용될 수도 있다.

대 표 도 - 도5



(72) 발명자

브릭켈, 어니

미국 87111 오레곤주 포틀랜드 노스웨스트 루레이 테라스 3106

그라우룩, 데이비드

미국 97007 오레곤주 알로하 사우스웨스트 184번 애비뉴 8285

특허청구의 범위

청구항 1

개인 키 및 개인 키 다이제스트를 포함하며 디바이스와 관련된 암호화 데이터 구조를 생성하는 단계;

유사 랜덤 생성 값(pseudo-randomly generated value)에 기초하여, 상기 암호화 데이터 구조에 대한 식별자를 생성하는 단계;

상기 암호화 데이터 구조 및 상기 식별자를 이동식(removable) 기억 매체상의 서명 그룹 레코드에 저장하는 단계; 및

상기 서명 그룹 레코드에 대응하는 그룹 번호 및 상기 유사 랜덤 생성 값을 상기 디바이스 내의 비휘발성 스토리지에 저장하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 그룹 번호 및 상기 유사 랜덤 생성 값을 상기 디바이스 내에 저장하는 단계 후에, 상기 이동식 기억 매체 및 상기 디바이스를 배포하는 단계를 더 포함하는 방법.

청구항 3

제1항에 있어서,

상기 암호화 데이터 구조를 생성하는 단계 전에, 디바이스들의 클래스에 대한 다이렉트 증명(Direct Proof) 패밀리 키 쌍을 생성하는 단계를 더 포함하는 방법.

청구항 4

제1항에 있어서,

상기 암호화 데이터 구조를 생성하는 단계 전에, 상기 서명 그룹 레코드를 서명 및 검증하기 위한 키 쌍을 생성하는 단계를 더 포함하는 방법.

청구항 5

제4항에 있어서,

상기 그룹 번호 및 상기 유사 랜덤 생성 값을 상기 디바이스 내에 저장하는 단계 후에, 상기 서명 그룹 레코드 키 쌍의 공개 키의 해시를 상기 디바이스의 비휘발성 스토리지에 저장하는 단계를 더 포함하는 방법.

청구항 6

제1항에 있어서,

상기 그룹 번호 및 상기 유사 랜덤 생성 값을 저장하는 단계 전에, 상기 서명 그룹 레코드에 대한 그룹 크기를 선택하는 단계를 더 포함하는 방법.

청구항 7

제3항에 있어서,

상기 개인 키는 상기 다이렉트 증명 패밀리 키 쌍의 공개 키와 관련된 다이렉트 증명 개인 키를 포함하고, 상기 개인 키 다이제스트를 생성하기 위해 상기 다이렉트 증명 개인 키를 해시하는 단계를 더 포함하는 방법.

청구항 8

제1항에 있어서,

상기 식별자를 생성하는 단계는 상기 디바이스에 대한 상기 유사 랜덤 생성 값에 기초하여 대칭 키를 생성하는

단계를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 식별자를 생성하는 단계는 상기 대칭 키를 사용해서 데이터 값을 암호화하는(encrypting) 단계를 더 포함하는 방법.

청구항 10

제8항에 있어서,

상기 대칭 키를 사용해서 상기 암호화 데이터 구조를 암호화하는 단계를 더 포함하는 방법.

청구항 11

제1항에 있어서,

상기 암호화 데이터 구조는 랜덤 초기화 벡터(random initialization vector)를 더 포함하는 방법.

청구항 12

제1항에 있어서,

상기 이동식 기억 매체는 CD 및 DVD(digital versatile disk) 중 적어도 하나를 포함하는 방법.

청구항 13

제1항에 있어서,

상기 디바이스에 대한 상기 유사 랜덤 생성 값은 고유한(unique) 것인 방법.

청구항 14

복수의 머신 판독 가능 명령어들을 갖는 기억 매체로서,

상기 명령어들이 프로세서에 의해 실행될 때, 상기 명령어들은,

개인 키 및 개인 키 다이제스트를 포함하며 디바이스와 관련된 암호화 데이터 구조를 생성하고;

유사 랜덤 생성 값에 기초하여, 상기 암호화 데이터 구조에 대한 식별자를 생성하며;

상기 암호화 데이터 구조 및 상기 식별자를 이동식 기억 매체상의 서명 그룹 레코드에 저장하고;

상기 서명 그룹 레코드에 대응하는 그룹 번호 및 상기 유사 랜덤 생성 값이 상기 디바이스 내의 비휘발성 스토리지에 저장되도록 함으로써,

서명 그룹들의 개인 키들을 디바이스들에게 전달하도록 하는 기억 매체.

청구항 15

제14항에 있어서,

상기 서명 그룹 레코드를 서명 및 검증하기 위한 키 쌍을 생성하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 16

제15항에 있어서,

상기 서명 그룹 레코드 키 쌍의 공개 키의 해시를 상기 디바이스의 비휘발성 스토리지에 저장하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 17

제14항에 있어서,

상기 서명 그룹 레코드에 대한 그룹 크기를 선택하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 18

제14항에 있어서,

디바이스들의 클래스에 대한 다이렉트 증명 패밀리 키 쌍을 생성하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 19

제14항에 있어서,

상기 개인 키는 다이렉트 증명 패밀리 키 쌍의 공개 키와 관련된 다이렉트 증명 개인 키를 포함하고, 상기 개인 키 다이제스트를 생성하기 위해 상기 다이렉트 증명 개인 키를 해시하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 20

제14항에 있어서,

상기 디바이스에 대한 상기 유사 랜덤 생성 값에 기초하여 대칭 키를 생성하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 21

제20항에 있어서,

상기 식별자를 생성하기 위한 명령어들은 상기 대칭 키를 이용하여 데이터 값을 암호화하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 22

제20항에 있어서,

상기 대칭 키를 이용하여 상기 암호화 데이터 구조를 암호화하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 23

제14항에 있어서,

상기 암호화 데이터 구조는 랜덤 초기화 벡터를 더 포함하는 기억 매체.

청구항 24

제14항에 있어서,

상기 디바이스에 대한 상기 유사 랜덤 생성 값은 고유한 것인 기억 매체.

청구항 25

컴퓨터 시스템에 설치된 디바이스와 관련된, 개인 키 및 개인 키 다이제스트를 포함하는 암호화 데이터 구조가 상기 컴퓨터 시스템 상의 메모리에 저장되어 있는지를 결정하는 단계; 및

상기 암호화 데이터 구조가 저장되어 있지 않은 경우, 상기 컴퓨터 시스템에 의해 액세스 가능하며 서명 그룹 레코드들의 데이터베이스를 저장한 이동식 기억 매체로부터 서명 그룹 레코드의 상기 디바이스와 관련된 상기 암호화 데이터 구조를 획득하는 단계

를 포함하는 방법.

청구항 26

제25항에 있어서,

상기 이동식 기억 매체는 상기 디바이스의 제조자에 의해 생성된 CD 및 DVD 중 적어도 하나를 포함하는 방법.

청구항 27

제25항에 있어서,

상기 암호화 데이터 구조 획득 단계는 개인 키 획득 프로세스를 개시하기 위해 상기 디바이스에 획득 키 커맨드를 발행하는 단계를 더 포함하는 방법.

청구항 28

제25항에 있어서,

상기 개인 키는 디바이스들의 클래스에 대한 다이렉트 증명 패밀리 키 쌍의 공개 키와 관련된 다이렉트 증명 개인 키를 포함하는 방법.

청구항 29

제27항에 있어서,

상기 개인 키 획득 프로세스는 상기 획득 키 커맨드를 발행하는 단계 후에, 상기 디바이스에 저장된 고유한 유사 랜덤 생성 값에 기초하여 대칭 키를 생성하는 단계를 더 포함하는 방법.

청구항 30

제29항에 있어서,

상기 개인 키 획득 프로세스는 상기 유사 랜덤 생성 값에 기초하여 상기 암호화 데이터 구조에 대한 디바이스 식별자를 생성하는 단계를 더 포함하는 방법.

청구항 31

제27항에 있어서,

상기 개인 키 획득 프로세스는 상기 획득 키 커맨드를 발행하는 단계 후에, 상기 디바이스의 그룹 번호에 대응하는 상기 서명 그룹 레코드를 상기 이동식 기억 매체로부터 획득하는 단계를 더 포함하는 방법.

청구항 32

제30항에 있어서,

상기 개인 키 획득 프로세스는 그룹 번호, 그룹 공개 키, 및 상기 디바이스 식별자에 대응하는 상기 암호화 데이터 구조를 획득하기 위해 상기 서명 그룹 레코드를 분석하는(parsing) 단계를 더 포함하는 방법.

청구항 33

제31항에 있어서,

상기 개인 키 획득 프로세스는 상기 서명 그룹 레코드를 획득하는 단계 후에, 상기 서명 그룹 레코드를 검증하는 단계를 더 포함하는 방법.

청구항 34

제32항에 있어서,

상기 개인 키 획득 프로세스는 상기 개인 키 및 상기 개인 키 다이제스트를 획득하기 위해 상기 대칭 키를 사용해서 상기 이동식 기억 매체로부터 수신된 상기 암호화 데이터 구조를 암호 해독하는(decrypting) 단계를 더 포함하는 방법.

청구항 35

제34항에 있어서,

상기 개인 키 획득 프로세스는 새로운 개인 키 다이제스트를 생성하기 위해 상기 개인 키를 해시하고, 상기 암호 해독된 데이터 구조로부터의 상기 개인 키 다이제스트를 상기 새로운 개인 키 다이제스트와 비교하고, 상기

다이제스트들이 매치할 때 상기 개인 키를 상기 디바이스에 대해 유효한 것으로서 수용하는 단계를 더 포함하는 방법.

청구항 36

복수의 머신 판독 가능 명령어들을 갖는 기억 매체로서,

상기 명령어들이 프로세서에 의해 실행될 때, 상기 명령어들은,

컴퓨터 시스템에 설치된 디바이스와 관련된, 개인 키 및 개인 키 다이제스트를 포함하는 암호화 데이터 구조가 상기 컴퓨터 시스템 상의 메모리에 저장되어 있는지를 결정하고;

상기 암호화 데이터 구조가 저장되어 있지 않은 경우, 상기 컴퓨터 시스템에 의해 액세스 가능하며 서명 그룹 레코드들의 데이터베이스를 저장한 이동식 기억 매체로부터 서명 그룹 레코드의 상기 디바이스와 관련된 상기 암호화 데이터 구조를 획득함으로써,

컴퓨터 시스템에 설치된 디바이스에 대한 서명 그룹 레코드로부터 개인 키를 획득하도록 하는 기억 매체.

청구항 37

제36항에 있어서,

상기 암호화 데이터 구조를 획득하기 위한 명령어들은 개인 키 획득 프로세스를 개시하기 위해 상기 디바이스에 획득 키 커맨드를 발행하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 38

제36항에 있어서,

상기 개인 키는 디바이스들의 클래스에 대한 다이렉트 증명 패밀리 키 쌍의 공개 키와 관련된 다이렉트 증명 개인 키를 포함하는 기억 매체.

청구항 39

제37항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 상기 획득 키 커맨드를 발행한 후에, 상기 디바이스에 저장된 고유한 유사 랜덤 생성 값에 기초하여 대칭 키를 생성하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 40

제39항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 상기 유사 랜덤 생성 값에 기초하여 상기 암호화 데이터 구조에 대한 디바이스 식별자를 생성하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 41

제37항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 상기 획득 키 커맨드를 발행한 후에, 상기 디바이스의 그룹 번호에 대응하는 상기 서명 그룹 레코드를 상기 이동식 기억 매체로부터 획득하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 42

제40항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 그룹 번호, 그룹 공개 키, 및 상기 디바이스 식별자에 대응하는 상기 암호화 데이터 구조를 획득하기 위해 상기 서명 그룹 레코드를 분석하기(parsing) 위한 명령어들을 더 포함하는 기억 매체.

청구항 43

제41항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 상기 서명 그룹 레코드를 획득한 후에, 상기 서명 그룹 레코드를 검증하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 44

제42항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 상기 개인 키 및 상기 개인 키 다이제스트를 획득하기 위해 상기 대칭 키를 이용하여 상기 이동식 기억 매체로부터 수신된 상기 암호화 데이터 구조를 암호 해독하기 위한 명령어들을 더 포함하는 기억 매체.

청구항 45

제44항에 있어서,

상기 개인 키 획득 프로세스를 수행하기 위한 명령어들은, 새로운 개인 키 다이제스트를 생성하기 위해 상기 개인 키를 해시하고, 상기 암호 해독된 데이터 구조로부터의 상기 개인 키 다이제스트를 상기 새로운 개인 키 다이제스트와 비교하고, 상기 다이제스트들이 매치할 때 상기 개인 키를 상기 디바이스에 대해 유효한 것으로서 수용하기 위한 명령어들을 더 포함하는 기억 매체.

명 세 서

기 술 분 야

<1> 본 발명은 일반적으로 컴퓨터 보안에 관한 것으로, 특히, 프로세싱 시스템의 디바이스에 안전하게 암호 키들을 분배하는 것에 관한 것이다.

배 경 기 술

<2> 콘텐츠 보호 및/또는 컴퓨터 보안 기능들을 지원하는 몇몇 프로세싱 시스템 아키텍처들은 특별 보호 또는 "신뢰" 소프트웨어 모듈들이 프로세싱 시스템의 특별 보호 또는 "신뢰" 하드웨어 디바이스들(예를 들어, 그래픽 컨트롤러 카드)과의 인증 암호화 통신 세션을 생성할 수 있을 것을 요구한다. 디바이스를 식별하고 동시에 암호화 통신 세션을 설정하는 흔히 사용되는 한 방법은 원사이드 인증 DH(Diffie-Helman) 키 교환 프로세스를 사용하는 것이다. 본 프로세스에서는, 유일한 공개/개인 RSA(Rivest, Shamir and Adelman) 알고리즘 키 쌍 또는 유일한 ECC(Elliptic Curve Cryptography) 키 쌍이 디바이스에 할당된다. 그러나, 상기 인증 프로세스는 RSA 또는 ECC 키들을 사용하기 때문에, 디바이스는 유일한 입증 가능 아이덴티티를 갖는데, 이는 프라이버시 개념을 야기할 수 있다. 최악의 경우, 상기 개념은 이러한 종류의 보안을 제공하는 신뢰할만한 디바이스들을 생성하는 고유 장치 제조자(OEM)들로부터의 지원 부족을 야기할 수도 있다.

발명의 상세한 설명

<14> 보호/신뢰 디바이스들이 자신을 인증하고 신뢰 소프트웨어 모듈들로 암호화 통신 세션을 설정할 수 있도록 다이렉트 증명 기반 디피-헬먼(Diffie-Helman) 키 교환 프로토콜을 사용함으로써, 프로세싱 시스템에서 임의의 유일한 아이덴티티 정보가 생성되는 것이 방지되며, 따라서, 프라이버시 개념 야기가 방지된다. 그러나, 제조 라인에서 디바이스에 다이렉트 증명 개인 키를 직접 내장하는 것은 디바이스에서 다른 방법들 보다 더 많은 보호 비휘발성 스토리지를 요구하기에, 디바이스 코스트가 증가한다. 본 발명의 한 실시예는 서명 그룹들의 다이렉트 증명 개인 키들(예를 들어, 서명을 위해 사용되는 키들)이 안전한 방식으로 배포 컴팩트 디스크-판독 전용 메모리(CD-ROM 또는 CD)에 전달되어 디바이스 자체에 의해 디바이스에 차후에 설치될 수 있게 해준다. 한 실시예에서, 상기 성능을 지원하는데 필요한 디바이스 스토리지는 대략 300 내지 700 바이트들에서 대략 20-25 바이트들로 감소될 수도 있다. 디바이스들을 위한 다이렉트 증명 기반 디피-헬먼 키 교환을 구현하는데 필요한 비휘발성 스토리지의 양의 상술된 감소는 상기 기술의 보다 광범위한 적응을 야기할 수도 있다.

<15> 본 명세서에서 본 발명의 "하나의 실시예" 또는 "한 실시예"라는 말은 실시예와 관련해서 기술된 특정 기능, 구조 또는 특징이 본 발명의 적어도 하나의 실시예에 포함됨을 의미한다. 따라서, 본 명세서의 다양한 위치들에서 나타나는 "한 실시예에서"라는 구절은 반드시 모두 동일한 실시예를 말하는 것은 아니다.

<16> 이하의 설명에서, 특정 용어는 본 발명의 하나 이상의 실시예들의 특정 특징들을 기술하는데 사용된다. 예를 들어, "플랫폼"은 정보를 송신하고 수신하도록 적응된 임의의 타입의 통신 디바이스로서 정의된다. 다양한 플랫폼의 일례는 컴퓨터 시스템, 퍼스널 디지털 어시스턴트, 셀룰러 폰, 셋탑 박스, 팩스, 프린터, 모뎀, 라우터 등을 포함하지만, 이들로만 제한되지 않는다. "통신 링크"는 플랫폼에 적응된 하나 이상의 정보-전달 매체들로서 광범위하게 정의된다. 다양한 타입들의 통신 링크의 예들은 전기 배선(들), 광 섬유(들), 케이블(들), 버스 트레이스(들), 또는 무선 시그널링 기술을 포함하지만, 이들로만 제한되지 않는다.

<17> "챌린저(challenger)"는 다른 엔티티로부터 몇몇 인증 검증 또는 허가 검증을 요청하는 임의의 엔티티(예를 들어, 사람, 플랫폼, 시스템, 소프트웨어 및/또는 디바이스)를 말한다. 통상, 이는 요청된 정보를 기술하거나 제공하기 전에 실행된다. "응답기(reponder)"는 허가, 유효성 및/또는 아이덴티티의 증명을 제공하기 위해 요청된 임의의 엔티티를 말한다. "증명 제조자"와 상호 교환되어 사용될 수도 있는 "디바이스 제조자"는 플랫폼 또는 디바이스를 제조하거나 구성하는 임의의 엔티티를 말한다.

<18> 본 명세서에서 사용된 바와 같이, 응답기가 몇몇 암호 정보(예를 들어, 디지털 서명, 키와 같은 시크리트 등)의 소유 또는 지식을 가짐을 챌린저에게 "증명"해주거나 또는 "확신"을 주는 것은, 챌린저에게 기술된 정보 및 증명을 근거로, 응답기가 암호 정보를 가질 확률이 높음을 의미한다. 암호 정보를 챌린저에게 "누설"하고나 "노출"하지 않고 챌린저에게 이를 증명하는 것은, 챌린저에게 노출된 정보를 근거로, 챌린저가 암호 정보를 결정하는 것인 계산적으로 실행 불가능함을 의미한다.

<19> 이러한 증명을 이후부터 다이렉트 증명이라고 한다. 상기 타입의 증명들은 통상 본 분야에서 공지된 것으로, "다이렉트 증명"이라는 용어는 제로-지식 증명(zero-knowledge proofs)이라고 한다. 특히, 본 명세서에서 참조된 특정 다이렉트 증명 프로토콜은 본 출원의 소유자에게 양도된 "System and Method for Establishing Trust Without Revealing Identity"이라는 제목으로 2002년 11월 27일에 출원된 공동 계류중인 특허 출원 일련번호 제10/306,336호의 주제이다. 다이렉트 증명은 발행인이 발행인에 의해 정의된 공통 특징들을 공유하는 다수의 멤버들의 패밀리를 정의하는 프로토콜을 정의한다. 발행인은 패밀리를 총체적으로 표현하는 패밀리 공개 및 개인 키 쌍(Fpub 및 Fpri)을 생성한다. Fpri를 사용해서, 발행인은 패밀리의 각각의 개별 멤버에 대한 고유의 다이렉트 증명 개인 서명 키(DPpri)를 생성할 수 있다. 개별 DPpri에 의해 서명된 임의의 메시지는 패밀리 공개 키 Fpub를 사용해서 검증될 수 있다. 그러나, 상기 검증은 단지 서명인이 패밀리의 멤버임을 식별한다; 개별 멤버에 대한 유일한 식별 정보는 공개되지 않는다. 한 실시예에서, 발행인은 디바이스 제조자 또는 대리자일 수도 있다. 즉, 발행인은 공유 특징을 근거로 디바이스 Families를 정의하고, Family 공개/개인 키 쌍을 생성하고, DP 개인 키들을 디바이스에 주입하는 기능을 가진 엔티티일 수도 있다. 발행인은 키의 소스 및 디바이스 패밀리의 특징들을 식별하는 Family 공개 키에 대한 증명서를 생성할 수도 있다.

<20> 이제 도 1을 참조하면, 본 발명의 실시예에 따라 동작하는 신뢰 하드웨어 디바이스로 구현된 플랫폼("신뢰 플랫폼 모듈" 또는 "TPM"이라고 함)을 특징으로 하는 시스템의 한 실시예가 도시되어 있다. 제1 플랫폼(102)(챌린저)은 제2 플랫폼(104)(응답기)이 자체에 대한 정보를 제공할 것을 요청하는 요청(106)을 송신한다. 요청(106)에 응답해서, 제2 플랫폼(104)은 요청된 정보(108)를 제공한다.

<21> 또한, 강조된 보안을 위해, 제1 플랫폼(102)은 선택된 디바이스 제조자 또는 선택된 그룹의 디바이스 제조자들(이후부터 "디바이스 제조자(들)(110)"라고 함)에 의해 제조된 디바이스로부터의 요청 정보(108)를 검증할 필요가 있을 수도 있다. 예를 들어, 본 발명의 한 실시예의 경우, 제1 플랫폼(102)은 디바이스 제조자(들)(110)에 의해 생성된 암호 정보(예를 들어, 서명)를 가짐을 보여주도록 제2 플랫폼(104)에게 요구한다. 상기 요구는 (도시된 대로) 요청(106)에 포함되거나 개별적으로 송신될 수도 있다. 제2 플랫폼(104)은 암호 정보를 폭로하지 않고, 디바이스 제조자(들)(110)에 의해 생성된 암호 정보를 제2 플랫폼(104)이 가짐을 제1 플랫폼(102)에게 확신시키기 위해 응답 형태로 정보를 제공함으로써 상기 요구에 응답한다. 응답은 (도시된 대로) 요청 정보(108)의 일부일 수도 있거나 개별적인 송신일 수도 있다.

<22> 본 발명의 한 실시예에서, 제2 플랫폼(104)은 신뢰 플랫폼 모듈(TPM; 115)을 포함한다. TPM(115)은 디바이스 제조자(들)(110)에 의해 제조된 암호 디바이스이다. 본 발명의 한 실시예에서, TPM(115)은 팩키지 내에 포함된 소량의 온-칩 메모리를 갖는 프로세서를 포함한다. TPM(115)은 응답이 유효 TPM으로부터 송신됨을 결정할 수 있게 해주는 정보를 제1 플랫폼(102)에게 제공하도록 구성된다. 사용된 정보는 TPM의 아이덴티티 또는 제2 플랫폼의 아이덴티티가 결정될 수 있게 해주지 않을 콘텐츠이다.

<23> 도 2는 TPM(115)을 갖는 제2 플랫폼(104)의 제1 실시예를 도시한다. 본 발명의 상기 실시예의 경우, 제2 플랫폼(104)은 TPM(115)에 결합된 프로세서(202)를포함한다. 일반적으로, 프로세서(202)는 정보를 처리하는 디바이

스이다. 예를 들어, 본 발명의 한 실시예에서, 프로세서(202)는 마이크로프로세서, 디지털 신호 프로세서, 마이크로-컨트롤러 또는 상태 기기로서 구현될 수도 있다. 또한, 본 발명의 다른 실시예에서, 프로세서(202)는 FPGA(Field Programmable Gate Array), TTL(transistor-transistor logic), 또는 심지어 ASIC(Application Specific Integrated Circuit)과 같은 프로그래머블 또는 하드-코드 로직으로서 구현될 수도 있다.

<24> 본 명세서에서, 제2 플랫폼(104)은 키들, 해시값들, 서명들, 증명서들 등 중 하나 이상과 같은 암호 정보의 저장을 가능케 하는 스토리지 유닛(206)을 더 포함한다. "X"의 해시값은 "Hash(X)"로 표현될 수도 있다. 상기 정보가 도 3에 도시된 바와 같이 스토리지 유닛(206) 대신 TPM(115)의 내부 메모리(220) 내에 저장될 수도 있다. 암호 정보는, 특히 TPM(115) 외부에 저장되는 경우 암호화될 수도 있다.

<25> 도 4는 도 2의 TPM(115)으로 구현된 컴퓨터 시스템(300)을 포함하는 플랫폼의 한 실시예를 도시한다. 컴퓨터 시스템(300)은 버스(302)에 결합된 프로세서(310)와 버스(302)를 포함한다. 컴퓨터 시스템(300)은 메인 메모리 유닛(304) 및 정적 메모리 유닛(306)을 더 포함한다.

<26> 본 명세서에서, 메인 메모리 유닛(304)은 프로세서(310)에 의해 실행되는 명령 및 정보를 저장하기 위한 휘발성 반도체 메모리이다. 메인 메모리(304)는 프로세서(310)에 의해 명령이 실행되는 중에 임시 변수들 또는 다른 중간 정보를 저장하는데 사용될 수도 있다. 정적 메모리 유닛(306)은 프로세서(310)를 위한 명령들 및 정보를 보다 영구적으로 저장하기 위한 비휘발성 반도체 메모리이다. 정적 메모리(306)의 예들은 판독 전용 메모리(ROM)를 포함하지만, 이로만 제한되지 않는다. 메인 메모리 유닛(304) 및 정적 메모리 유닛(306) 둘 다 버스(302)에 결합된다.

<27> 본 발명의 한 실시예에서, 컴퓨터 시스템(300)은 자기 디스크 또는 광 디스크와 같은 데이터 스토리지 디바이스(308)를 더 포함하고 대응 드라이브는 정보 및 명령들을 저장하기 위해 컴퓨터 시스템(300)에 결합될 수도 있다.

<28> 컴퓨터 시스템(300)은 엔드 유저에게 정보를 디스플레이하기 위한 음극선관(CRT), 액정 디스플레이(LCD) 또는 임의의 플랫 패널 디스플레이와 같은 디스플레이(도시되지 않음)를 제어하는 그래픽 컨트롤러 디바이스(314)에 버스(302)를 통해 결합될 수도 있다. 한 실시예에서, 그래픽 컨트롤러 또는 다른 주변 디바이스가 프로세서에 의해 실행중인 소프트웨어 모듈과의 인증 암호화 통신 세션을 설정할 수 있는 것이 바람직할 수도 있다.

<29> 통상, 영숫자 입력 장치(316)(예를 들어, 키보드, 키패드 등)는 정보 및/또는 커맨드 선택을 프로세서(310)에 전달하기 위해 버스(302)에 결합될 수도 있다. 다른 타입의 사용자 입력 장치는 프로세서(310)에게 방향 정보 및 커맨드 선택을 전달하고 디스플레이(314)에서의 커서 이동을 제어하기 위한 마우스, 트랙볼, 터치 패드, 스타일러스 또는 커서 방향 키들과 같은 커서 제어 유닛(318)이다.

<30> 통신 인터페이스 유닛(320)이 또한 버스(302)에 결합된다. 인터페이스 유닛(320)의 예들은 모뎀, 네트워크 인터페이스 카드 또는 근거리 또는 광역 통신망의 일부를 형성하는 통신 링크에 결합하는데 사용되는 다른 잘 공지된 인터페이스들을 포함한다. 이러한 방식으로, 컴퓨터 시스템(300)은 예를 들어, 회사의 인트라넷 및/또는 인터넷과 같은 종래의 네트워크 기본 시스템을 통해 다수의 클라이언트들 및/또는 서버들에 결합될 수도 있다.

<31> 상술된 보다 더 적거나 많은 장치를 가진 컴퓨터 시스템이 특정 구현을 위해 바람직할 수도 있음을 알 것이다. 따라서, 컴퓨터 시스템(300)의 구성은 가격 제한, 성능 요구 사항, 기술 향상 및/또는 다른 상황들과 같은 다수의 요인들에 좌우되어 실시예마다 다양하게 구현될 것이다.

<32> 적어도 하나의 실시예에서, 컴퓨터 시스템(300)은 메인 메모리(304) 및/또는 대용량 기억 장치(308)에 저장되고 시스템의 다른 부적당한 소프트웨어에 있는 경우에도 특정 활동들을 실행하기 위해 프로세서(310)에 의해 실행중인 특별 보호 "신뢰" 소프트웨어 모듈들(예를 들어, 손을 타기 어려운(tamper-resistant) 소프트웨어, 또는 보호 프로그램들을 실행하는 기능을 갖는 시스템들)의 사용을 지원할 수도 있다. 상기 신뢰 소프트웨어 모듈들 중 몇몇은 단지 다른 플랫폼들이 아닌 예를 들어, 그래픽 컨트롤러(314)와 같은 동일한 플랫폼 내의 하나 이상의 디바이스들에게 동일하게 "신뢰할만한" 보호 액세스를 요구한다. 일반적으로, 이러한 액세스는 디바이스의 성능 및/또는 특정 아이덴티티를 식별하고, 시스템의 다른 소프트웨어에 의해 속여질 수 없는 데이터의 교환을 허용하도록 디바이스와의 암호화 세션을 설정할 수 있을 것을 신뢰 소프트웨어 모듈에게 요구한다.

<33> 디바이스를 식별하고 동시에 암호화 세션을 설정하는 한 종래 기술의 방법은 원사이드 인증 디피-헬먼(DH) 키 교환 프로세스를 사용하는 것이다. 본 프로세스에서, 디바이스는 유일한 공개/개인 RSA 또는 ECC 키 쌍을 할당받는다. 디바이스는 개인 키를 홀드 및 보호하고, 인증 증명서와 함께 공개 키는 소프트웨어 모듈에 공개될 수도 있다. DH 키 교환 프로세스 중에, 디바이스는 소프트웨어 모듈이 대응 공개 키를 사용해서 검증할 수 있는

개인 키를 사용해서 메시지에 서명한다. 이는 메시지가 해당 디바이스로부터 온 것임을 소프트웨어 모듈이 인증할 수 있게 해준다.

<34> 그러나, 상기 인증 프로세스가 RSA 또는 ECC 키를 사용하기 때문에, 디바이스는 유일한 입증 가능 아이덴티티를 갖는다. 디바이스가 개인 키로 메시지에 서명하게 할 수 있는 임의의 소프트웨어 모듈은 상기 특정한 유일 디바이스가 컴퓨터 시스템에 존재함을 입증할 수 있다. 디바이스가 프로세싱 시스템들 간에 거의 이동하지 않는 경우, 이는 입증 가능 유일한 컴퓨터 시스템 아이덴티티를 나타낸다. 또한, 디바이스의 공개 키 자체는 유일한 상수 값을 나타낸다; 실제로 영구 "쿠키"라고 한다. 몇몇 경우, 상기 특징들은 중요한 프라이버시 문제점으로 해석될 수도 있다.

<35> 다른 방법은 본 출원의 소유자에게 양도된 "An Apparatus and Method for Establishing an Authenticated Encrypted Session with a Device Without Exposing Privacy-Sensitive Information"라는 제목의 2004년 11월 20일에 출원된 공동 계류중인 특허 출원 일련 번호 제10/999,576호에 기술되어 있다. 상기 방법에서, 원 사이드 인증 디피-헬먼 프로세스에서 사용되는 RSA 또는 ECC 키들은 다이렉트 증명 키들로 대체된다. 상기 방법을 사용하는 디바이스는 디바이스의 동작 또는 신뢰 상태에 대한 보증을 포함할 수도 있는 디바이스의 특정 패밀리에 속한 것으로 인증될 수도 있다. 본 방법은 프로세싱 시스템을 나타내는 유일 아이덴티티를 설정하는데 사용될 수 있는 임의의 유일 식별 정보를 공개하지 않는다.

<36> 상기 방법이 양호하게 작용하더라도, RSA 또는 ECC 키 보다 더 클 수도 있는 다이렉트 증명 개인 키를 홀드하기 위한 디바이스의 추가 스토리지가 필요하다. 추가 스토리지 요구 사항의 부담을 경감시키기 위해, 본 발명의 실시예들은 디바이스의 상당한 추가 스토리지를 요구하지 않고, 키가 필요할 때 디바이스가 다이렉트 증명 개인 키를 가짐을 보증하기 위한 시스템 및 프로세스를 정의한다. 한 실시예에서, DP 키들은 클라이언트 컴퓨터 시스템에 서명 그룹들로 전달된다.

<37> 본 발명의 적어도 하나의 실시예에서, 디바이스 제조자는 디바이스가 제조 라인에서 생성중일 때 디바이스에 128-비트 유사 랜덤 수만을 저장하는 한편, 보다 큰 다이렉트 증명 개인 키(DPpri)가 배포 CD를 사용해서 암호화 및 전달될 수도 있다. 다른 실시예들은 128 비트들 보다 길거나 짧은 수를 디바이스에 저장할 수도 있다. 상기 프로세스는 특정 디바이스만이 할당된 DPpri 키를 해독 및 사용할 수 있음을 보증한다.

<38> 본 발명의 적어도 하나의 실시예에서, "키블로브(keyblob)"라고 하는 DPpri 암호화 데이터 구조들은 디바이스 제조자에 의해 서명된 그룹 레코드들로 전달될 수도 있다. 전체 그룹 레코드는 자신의 암호화 키블로브만을 추출하는 디바이스로 전달되어야만 한다. 디바이스가 전체 레코드를 분석하고(parse), 전체 레코드가 분석될 때까지 추출된 키블로브 처리를 시작하지 않을 것을 요구함으로써, 침해자(attacker)가 타이밍 침해를 근거로 어떤 키블로브가 선택되었는지를 추정할 수 없다. 레코드에 서명하고, 디바이스가 키블로브 처리 전에 서명을 검증할 것을 요구함으로써, 침해자가 디바이스의 응답을 테스트하기 위해 싱글 키블로브의 다수의 복사본들을 공급할 수 없음을 보증할 수도 있다. 한 실시예에서, 침해자가 결정할 수 있는 최상은 디바이스가 그룹의 멤버라는 점이다. 한 실시예에서, 디바이스는 선정된 크기(예를 들어, 128 비트)의 유사 랜덤 값, 그룹 식별자(예를 들어, 4 바이트) 및 디바이스 제조자의 그룹 공개 키의 20-바이트 해시값을 저장하는데, 총 대략 40 바이트 데이터이다.

<39> 도 5는 본 발명의 한 실시예에 따른 서명 그룹의 다이렉트 증명 키들을 분배하기 위한 시스템(500)의 도면이다. 본 시스템에는 3개의 엔티티들, 디바이스 제조 보호 시스템(502), 디바이스 제조 생성 시스템(503) 및 클라이언트 컴퓨터 시스템(504)이 있다. 디바이스 제조 보호 시스템은 디바이스(506)의 제조 전에 셋업 프로세스에서 사용되는 프로세싱 시스템을 포함한다. 보호 시스템(502)은 디바이스 제조자 또는 다른 엔티티에 의해 동작될 수도 있어서, 보호 시스템이 디바이스 제조 사이트 외부에서의 해커의 침해로부터 보호된다(예를 들어, 폐쇄 시스템이다). 제조 생성 시스템(503)은 디바이스의 제조시 사용될 수도 있다. 한 실시예에서, 보호 시스템 및 생성 시스템은 동일한 시스템일 수도 있다. 디바이스(506)는 클라이언트 컴퓨터 시스템에 포함되는 임의의 하드웨어 디바이스(예를 들어, 메모리 컨트롤러, 그래픽스 컨트롤러, 입출력 장치와 같은 주변 장치, I/O장치, 다른 디바이스들 등)을 포함한다. 본 발명의 실시예들에서, 디바이스는 디바이스의 비휘발성 스토리지에 저장된 유사 랜덤 값 RAND(508) 및 그룹 번호(509)를 포함한다.

<40> 제조 보호 시스템은 보호 데이터베이스(510) 및 생성 함수(512)를 포함한다. 보호 데이터베이스는 후술되는 방식으로 생성 함수(512)에 의해 생성된 다수의 유사 랜덤 값들(제조되는 디바이스 당 적어도 하나)을 저장하기 위한 데이터 구조를 포함한다. 생성 함수는 본 명세서에서 키블로브(514)라고 하는 데이터 구조를 생성하기 위해 로직(소프트웨어 또는 하드웨어로 구현됨)을 포함한다. 키블로브(514)는 적어도 3개의 데이터 아이템들을

포함한다. 유일 다이렉트 증명 개인 키(DPpri)는 서명을 위해 디바이스에 의해 사용될 수도 있는 암호 키를 포함한다. DP 개인 다이제스트(516; DPpri Digest)는 SHA-1과 같은 안전한 메시지 다이제스트를 생성하는 임의의 공지된 방법에 따라 DPpri의 메시지 다이제스트를 포함한다. 몇몇 실시예들은 호환을 위해 키블로브의 일부로서 비트 스트림을 포함하는 유사 랜덤 초기화 벡터(IV)(518)를 포함할 수도 있다. 암호화를 위해 스트림 암호(stream cipher)가 사용되면, 스트림 암호의 IV를 사용하는 공지된 방법으로 IV가 사용된다. 블록 암호가 암호화를 위해 사용되면, 암호화될 메시지의 일부로서 IV가 사용되어서, 암호의 각각의 인스턴스가 상이하게 된다.

<41> 본 발명의 실시예들에서, 제조 보호 시스템은 하나 이상의 키블로브들(상세히 후술됨)을 생성하고 CD(522)에 키블로브 데이터베이스(520)의 그룹 레코드들(515)에 키블로브들을 저장한다. 한 실시예에서, 각각의 그룹 레코드에는 다수의 키블로브들이 있을 수도 있으며, 임의의 결합에서, 싱글 CD에 다수의 그룹 레코드들이 있을 수 있는데, 한가지 제한 사항은 CD의 물리적 스토리지 한계이다. 따라서, 각각의 그룹 레코드는 다수의 키블로브들을 포함한다. CD는 그 후 전형적인 물리 채널들을 통해 컴퓨터 시스템 제조자, 컴퓨터 분배원, 클라이언트 컴퓨터 시스템 소비자 등으로 분배된다. CD가 본 명세서에서 기억 매체로 기술되었지만, 임의의 적합한 이동식 기억 매체가 사용될 수도 있다(예를 들어, DVD(digital versatile disk) 또는 다른 매체).

<42> CD가 클라이언트 컴퓨터 시스템의 CDROM 드라이브(도시되지 않음)에 삽입될 때, 시스템(504) 내에 포함된 디바이스(506)와의 통신 세션의 인증 및 키 교환을 위해 다이렉트 증명 프로토콜을 사용하기를 희망하는 클라이언트 컴퓨터 시스템(504)은 CD의 키블로브 데이터베이스(520)에서 선택된 그룹 레코드(515)를 판독할 수도 있다. 키블로브 데이터는 그룹 레코드로부터 획득되어서, 다이렉트 증명 프로토콜을 구현하는데 사용되는 국부화 키블로브(524)(후술됨)를 생성하기 위해 디바이스에 의해 사용될 수도 있다. 본 발명의 실시예들에서, 다수의 키블로브들을 포함하는 총 그룹 레코드가 동시에 디바이스에 의해 처리되며, 침해자는 암호화 국부 키블로브를 생성하기 위해 어떤 특정 키블로브가 실제로 사용중인지를 결정할 수 없다. 디바이스 드라이버 소프트웨어(526)는 디바이스(506)를 초기화 및 제어하기 위해 클라이언트 컴퓨터 시스템에 의해 실행된다.

<43> 본 발명의 실시예들에서, 4개의 개별 동작 단계들이 있을 수도 있다. 도 6은 본 발명의 한 실시예에 따른 다이렉트 증명 키들을 분배하는 방법의 단계들을 도시하는 플로우챠트(600)이다. 본 발명의 실시예들에 따라, 특정 액션들이 각각의 단계에서 실행될 수도 있다. 디바이스 제조자 사이트에는, 적어도 두개의 단계들: 셋업 단계(602) 및 제조 생성 단계(604)가 있다. 셋업 단계는 도 7을 참조해서 본 명세서에 기술된다. 제조 생성 단계는 도 8을 참조해서 본 명세서에서 기술된다. 클라이언트 컴퓨터 시스템을 갖는 소비자 사이트에는, 적어도 두개의 단계들: 셋업 단계(606) 및 사용 단계(608)가 있다. 클라이언트 컴퓨터 시스템 셋업 단계는 도 9를 참조해서 본 명세서에 기술된다. 클라이언트 컴퓨터 시스템 사용 단계는 도 10을 참조해서 본 명세서에 기술된다.

<44> 도 7 및 도 8은 본 발명의 한 실시예에 따른 디바이스 제조 셋업 프로세싱을 도시하는 플로우챠트들(700 및 800)이다. 한 실시예에서, 디바이스 제조자는 제조 보호 시스템(502)을 사용해서 상기 액션들을 실행할 수도 있다. 블록(701)에서, 디바이스 제조자가 제조될 디바이스의 각각의 클래스에 대해 다이렉트 증명 패밀리 키 쌍(Fpub 및 Fpri)을 생성한다. DPpri을 사용해서 생성된 서명이 Fpub에 의해 검증될 수도 있도록 각각의 유일 디바이스는 대응 DPpri 키를 갖는다. 디바이스들의 클래스는 버전 번호 또는 디바이스의 다른 특징들을 근거로 생성 라인의 부집합 또는 선택된 생성 라인(즉, 디바이스의 타입)과 같은 디바이스의 임의의 집합 또는 부집합을 포함할 수도 있다. 패밀리 키 쌍은 생성 목적인 디바이스의 클래스에 의해 사용된다.

<45> 블록(702)에서, 디바이스 제조자는 그룹 레코드를 서명 및 검증하는데 사용되는 RSA 키 쌍(Gpri, Gpub)을 생성한다. 다른 실시예들에서, 임의의 보안 디지털 서명 시스템이 RSA 대신 사용될 수도 있다. 상기 키 쌍은 블록(701)에서 생성된 패밀리 키 쌍과 독립적이고, 디바이스 제조자에 의해 생성된 모든 디바이스 그룹들을 위해 사용될 수도 있다. 블록(703)에서, 디바이스 제조자는 희망 그룹 크기를 선택한다. 그룹 크기는 함께 그룹화될 패밀리의 디바이스들의 수일 수도 있다. 그룹 크기는 개별디바이스가 그룹 내에서 "숨겨질(hide)" 수 있을 만큼 충분히 크도록 선택되지만, 디바이스에 의한 키블로브 추출 프로세싱 중에 과도한 시간을 소비할만큼 크지는 않다. 한 실시예에서, 그룹 크기는 5,000 디바이스들이 되도록 선택될 수도 있다. 다른 실시예들에서, 다른 크기들이 사용될 수도 있다.

<46> 디바이스 제조자는 그룹 크기에 의해 지정된 수의 디바이스 키들을 생성할 수도 있다. 그룹 크기에 의해 지정된 수의 디바이스들을 갖는 각각의 그룹은 그룹 번호로 지명될 수도 있다. 소정의 그룹으로 제조되는 각각의 디바이스에 있어서, 생성 함수(512) 또는 제조 보호 시스템(502)의 다른 모듈들은 도 7의 블록(704) 내지 도 8의 블록(802)을 실행할 수도 있다. 먼저, 블록(704)에서, 생성 함수는 유일한 유사 랜덤 값(RAND; 508)을 생성한다. 한 실시예에서, RAND의 길이는 128 비트이다. 다른 실시예들에서, 값들의 다른 크기들이 사용될 수도

있다. 한 실시예에서, 다수의 디바이스들에 대한 유사 랜덤 값들은 미리 생성될 수도 있다. 블록(706)에서, 디바이스에 의해 지원되는 원웨이 함수, f를 사용해서, 생성 함수는 유일 RAND 값으로부터 대칭 암호화 키 SKEY를 생성한다(SKEY = f(RAND)). 원웨이 함수는 상기 목적에 적합한 임의의 공지된 알고리즘일 수도 있다(예를 들어, SHA-1, MGF1, DES(Data Encryption Standard), 트리플 DES 등). 블록(708)에서, 한 실시예에서, 생성 함수는 "널 엔트리"(예를 들어, 소수의 제로 바이트들)를 암호화하기 위해 SKEY를 사용함으로써, 배포 CD(522)에서 상기 디바이스의 키블로브(514)를 참조하는데 사용될 식별자(ID) 레이블을 생성한다(device ID = Encrypt(0..0), SKEY 이용). 다른 실시예들에서, 디바이스 ID를 생성하는 다른 방법들이 사용될 수도 있거나, 다른 값들이 SKEY에 의해 암호화될 수도 있다.

<47> 그 후, 블록(710)에서, 생성 함수는 디바이스의 패밀리 공개 키(Fpub)에 상관된 DP 개인 서명 키 DPpri를 생성한다. 블록(712)에서, 생성 함수는 공지된 방법들(예를 들어, SHA-1 또는 다른 해시 알고리즘 이용)을 사용해서 DPpri 다이제스트를 생성하도록 DPpri를 해시한다. 블록(714)에서, 생성 함수는 디바이스에 대한 키블로브 데이터 구조를 생성한다. 키블로브는 적어도 DPpri 및 DPpri 다이제스트를 포함한다. 한 실시예에서, 키블로브는 다수의 유사 랜덤 생성 비트들을 갖는 랜덤 초기화 벡터(IV)를 포함한다. 상기 값들은 암호화 키블로브(514)를 생성하도록 SKEY를 사용해서 암호화될 수도 있다. 블록(716)에서, 블록(708)에서 생성된 디바이스 ID 및 블록(714)에서 생성된 암호화 키블로브(514)는 배포 CD(522)에서 공개되는 키블로브 데이터베이스(520)의 레코드로 저장될 수도 있다. 한 실시예에서, 키블로브 데이터베이스의 레코드는 디바이스 ID로 표시될 수도 있다.

<48> 프로세싱은 도 8의 블록(801)으로 계속된다. 블록(801)에서, 디바이스가 속한 그룹의 현 그룹 번호 및 현 RAND 값은 보호 데이터베이스(510)에 저장될 수도 있다. 블록(802)에서, SKEY 및 DPpri는 본 분야의 디바이스에 의해 재생되기 때문에 삭제될 수도 있다. 그룹 번호는 제조중인 디바이스들의 각각의 연속 그룹에 대해 증가될 수도 있다. DPpri의 콘텐츠가 SKEY의 소유를 갖지 않은 임의의 엔티티에 의해 결정될 수 없고 SKEY의 소유를 갖는 엔티티에 의한 차후 검출 없이 KeyBlob의 콘텐츠가 SKEY의 소유를 갖지 않은 엔티티에 의해 변경될 수 없도록 DPpri 다이제스트의 생성 및 SKEY에 의한 다음 암호화가 설계된다. 다른 실시예들에서, 상기 비밀 및 완전성 보호를 제공하기 위한 다른 방법들이 사용될 수 있다. 몇몇 실시예들에서, 완전성 보호는 요구되지 않을 수도 있으며, 단지 비밀을 제공하는 방법이 사용될 수 있다. 이러한 경우, DPpri 다이제스트의 값은 필요하지 않다.

<49> 키블로브의 전체 데이터 집합이 디바이스 그룹에 대해 생성되었을 때, 적어도 그룹의 키블로브 데이터베이스(520)가 서명되고 공통 배포 CD에 부담을 주어, 각각의 디바이스와 함께 배포된다(한 실시예에서, 장치 ID 필드에 의해 인덱스되는 대로, 하나의 키블로브 데이터베이스 엔트리는 각각의 디바이스에 대해 사용될 수도 있음). 따라서, 블록(804)에서, 디바이스 제조자는 그룹 레코드(515)를 생성한다. 그룹 레코드는 그룹 번호, 그룹의 공개 키 Gpub, 그룹 크기 및 전체 그룹의 키블로브 레코드들(<Group Number, Gpub, Group Size, <Device ID1, Encrypted Keyblob1>, <Device ID2, Encrypted Keyblob2>, ...>)을 포함한다. 블록(806)에서, 디바이스 제조자는 그룹 개인 키 Gpri를 사용해서 그룹 레코드에 서명하고, 디지털 서명을 그룹 레코드에 첨부한다. 블록(808)에서, 서명 그룹 레코드는 배포 CD에서 키블로브 데이터베이스에 추가될 수도 있다. 한 실시예에서, 배포 CD는 클라이언트 컴퓨터 시스템에서의 차후 프로세싱을 위해 키 검색 유틸리티 소프트웨어 모듈을 포함하는데, 그 용도는 상세히 후술된다.

<50> 블록(802) 후의 임의의 시간에, 블록(810)에서, RAND 및 그룹 번호 값 쌍들의 보호 데이터베이스는 제조 프로세스 중에 디바이스에 RAND 및 그룹 번호 값들을 저장하는 제조 생성 시스템(503)에 안전하게 업로드될 수도 있다. 상기 업로드가 검증되면, RAND 값들은 제조 보호 시스템(502)으로부터 안전하게 삭제될 수 있다.

<51> 도 9는 본 발명의 한 실시예에 따른 디바이스 제조 생성 프로세싱을 도시하는 플로우챠트(900)이다. 디바이스가 생성 라인에서 제조중이므로, 블록(902)에서, 제조 보호 시스템은 보호 데이터베이스로부터 미사용 RAND 및 그룹 번호 값 쌍을 선택한다. 선택된 RAND 및 그룹 번호 값은 그 후 디바이스의 비휘발성 스토리지에 저장될 수도 있다. 한 실시예에서, 비휘발성 스토리지는 TPM을 포함한다. 블록(904)에서, 그룹 공개 키 Gpub의 해시는 디바이스의 비휘발성 스토리지에 저장될 수도 있다. 블록(906)에서, RAND 값이 성공적으로 디바이스에 저장되면, 제조 생성 시스템은 보호 데이터베이스에서 디바이스의 RAND 값의 임의의 레코드를 파괴한다. 이 때에, RAND 값의 단독 복사본이 디바이스에 저장된다.

<52> 다른 실시예에서, RAND 값은 디바이스 제조 중에 생성될 수 있으며, 그 후, 키블로브의 계산을 위해 제조 보호 시스템에 송신될 수 있다.

<53> 다른 실시예에서, RAND 값은 디바이스에서 생성될 수 있으며, 디바이스 및 제조 보호 시스템은 디바이스 외부에서 DPpri 키를 공개하지 않는 방법을 사용해서 DPpri 키를 생성하는 프로토콜에 참여할 수 있다. 그 후, 디바이스는 디바이스 ID, SKEY 및 키블로브를 생성할 수 있다. 디바이스는 디바이스 ID 및 키블로브를 보호 데이터베이스(510)에 저장되도록 제조 시스템에 전달한다. 이러한 방법으로, 제조 시스템은 보호 데이터베이스의 동일한 정보(디바이스 ID, 키블로브)로 종료하며, RAND 값 또는 DPpri 값을 알지 못한다.

<54> 도 10 및 도 11은 본 발명의 한 실시예에 따른 클라이언트 컴퓨터 시스템 셋업 프로세싱을 도시하는 플로우챠트들(1000 및 1100)이다. 클라이언트 컴퓨터 시스템은 시스템의 부팅업의 일부로서 상기 액션들을 실행할 수도 있다. 블록(1002)에서, 클라이언트 컴퓨터 시스템은 정상 방식으로 부팅될 수도 있으며, 디바이스용 디바이스 드라이버(526)는 메인 메모리에 로드될 수도 있다. 디바이스 드라이버가 초기화되고 실행을 개시할 때, 디바이스 드라이버는 블록(1004)에서 이미 암호화 국부화 키블로브(524)가 디바이스(506)의 대용량 기억 장치(308)에 저장되어 있는지를 결정한다. 저장되어 있으면, 차후 셋업 프로세싱이 실행될 필요가 없으며, 셋업 프로세싱은 블록(1006)에서 종료한다. 저장되어 있지 않으면, 프로세싱은 블록(1008)으로 계속된다. 블록(1008)에서, 디바이스 드라이버는 배포 CD(522)의 삽입을 요청하는 메시지를 클라이언트 컴퓨터 시스템의 사용자에게 디스플레이한다. CD가 컴퓨터 시스템에 의해 판독되면, 디바이스 드라이버는 CD에 저장된 키 검색 유틸리티 소프트웨어 모듈(도 5에 도시되지 않음)을 론칭한다. 키 검색 유틸리티는 디바이스에게 그룹 공개 키 Gpub의 해시 및 그룹 번호(509)일 수도 있는 그룹 ID를 요청한다. 디바이스가 상기 값들을 리턴하고, 유틸리티는 상기 값들을 사용해서 CD의 키블로브 데이터베이스로부터 적합한 서명 그룹 레코드의 위치를 찾는다. 상기 유틸리티는 디바이스의 DP 개인 키 획득 프로세스를 개시하도록 획득 키 커맨드를 디바이스(506)에 발행한다.

<55> 응답으로, 블록(1010)에서, 디바이스는 원웨이 함수 f를 사용해서 내장된 RAND 값(508)으로부터 대칭 키 SKEY(해독에 사용됨)를 재생한다(SKEY = f(RAND)). 블록(1012)에서, 디바이스는 SKEY를 사용해서 "널 엔트리"(예를 들어, 소수의 제로 바이트들)를 암호화함으로써, 유일 디바이스 ID 레이블을 생성한다(Device ID = Encrypt(0..0), SKEY 사용). 본 발명의 한 실시예에서, 상기 값들은 디바이스 외부에 공개되지 않을 수도 있다. 디바이스는 준비성에 대한 신호를 준다.

<56> 블록(1014)에서, 키 검색 유틸리티는 매칭 그룹 번호를 포함하는 그룹 레코드에 대해 CD의 키블로브 데이터베이스(520)를 탐색하고, 그룹 레코드를 추출하며, 전체 그룹 레코드를 디바이스에 전송한다.

<57> 블록(1016)에서, 디바이스는 전체 공급 그룹 레코드를 분석하지만, 그룹 번호, 그룹 레코드의 해시, 그룹 공개 키 Gpub, 및 디바이스 자신의 디바이스 ID(블록(1012)에서 생성됨)와 매치하는 제1 <Device ID, Encrypted Keyblob> 필드만을 유지한다. 블록(1018)에서, 디바이스는 그룹 레코드를 검증한다. 한 실시예에서, 디바이스는 디바이스에 포함된 그룹 번호와 추출된 그룹 번호 필드를 비교한다. 그들이 매치하지 않으면, 키 획득 프로세스는 종료될 수도 있다. 그렇지 않으면, 디바이스는 추출된 Gpub 필드를 해시하고 디바이스에 포함된 Gpub 해시와 비교한다. 해시들이 매치하지 않으면, 키 획득 프로세스는 종료될 수도 있다. 그렇지 않으면, 디바이스는 그룹 레코드의 해시에서 공급된 서명을 검증하기 위해 타당성 검사된 Gpub 키를 사용한다. 서명이 검증되면, 그룹 레코드는 검증되고, 프로세스는 도 11의 블록(1120)으로 진행한다.

<58> 한 실시예에서, 디바이스가 키블로브를 가진 후에 사기 소프트웨어가 획득 키 커맨드를 디바이스에 송신하고자 하면, 디바이스는 사기 소프트웨어에 그룹 번호로 응답하지 않는다. 대신, 디바이스는 에러 표시자를 리턴한다. 실제적으로, 디바이스가 국부화 키블로브에 액세스하면, 획득 키 커맨드의 기능은 억제된다. 이러한 방법으로, 디바이스는 키블로브를 갖지 않을 때를 제외하고 그룹 번호를 공개하지 않는다.

<59> 블록(1120)에서, 디바이스는 대칭 키 SKEY를 사용해서 암호화 키블로브를 해독하고, DPpri 및 DPpri 다이제스트를 산출하고, 상기 값들을 비휘발성 스토리지에 저장한다(Decrypted Keyblob = Decrypt (IV, DPpri, DPpri Digest), SKEY 사용). 초기화 벡터(IV)는 폐기될 수도 있다. 블록(1122)에서, 디바이스는 DPpri를 해시하고 결과를 DPpri 다이제스트와 비교함으로써, DPpri의 완전성을 체크한다. 비교가 양호하면, 디바이스는 유효 키로서 DPpri를 수용한다. 디바이스는 키 획득 플래그를 참으로 설정해서, DP 개인 키가 성공적으로 획득되었음을 나타낼 수도 있다. 블록(1124)에서, 디바이스는 새로운 IV를 선택하고, 새로운 IV를 사용해서 새로운 암호화 국부화 키블로브를 생성한다(Localized Keyblob = Encrypt (IV2, DPpri, DPpri Digest), SKEY 사용). 새로운 암호화 국부화 키블로브는 키 검색 유틸리티에 리턴될 수도 있다. 블록(1126)에서, 키 검색 유틸리티는 클라이언트 컴퓨터 시스템 내의 스토리지(예를 들어, 대용량 기억 장치(308))에 암호화, 국부화 키블로브를 저장한다. 디바이스의 DPpri는 클라이언트 컴퓨터 시스템에 새롭게 안전하게 저장된다.

<60> 디바이스가 셋업 프로세싱 중에 DPpri를 획득하면, 디바이스는 DPpri를 사용할 수도 있다. 도 12는 본 발명의

한 실시예에 따른 클라이언트 컴퓨터 시스템 프로세싱을 도시하는 플로우챠트이다. 클라이언트 컴퓨터 시스템은 셋업이 완료된 후 임의의 시간에 상기 액션들을 실행할 수도 있다. 블록(1202)에서, 클라이언트 컴퓨터 시스템은 정상 방식으로 부팅될 수도 있으며, 디바이스용 디바이스 드라이버(526)는 메인 메모리에 로드될 수도 있다. 디바이스 드라이버가 초기화되고 실행을 개시할 때, 디바이스 드라이버는 이미 암호화 국부화 키블로브(524)가 디바이스(506)의 대용량 기억 장치(308)에 저장되어 있는지를 결정한다. 저장되어 있지 않으면, 도 10 및 도 11의 셋업 프로세싱이 실행된다. 디바이스에 유용한 암호화 국부화 키블로브가 있으면, 프로세싱은 블록(1206)으로 계속된다. 블록(1206)에서, 디바이스 드라이버는 암호화 국부화 키블로브를 검색하고, 키블로브를 디바이스에 전송한다. 한 실시예에서, 키블로브의 전송은 Load Keyblob 커맨드를 실행함으로써 달성될 수도 있다.

<61> 블록(1208)에서, 디바이스는 원웨이 함수 f를 사용해서 내장된 RAND 값(508)으로부터 대칭 키 SKEY(해독에 사용됨)를 재생한다(SKEY = f(RAND)). 블록(1210)에서, 디바이스는 대칭 키 SKEY를 사용해서 암호화 국부화 키블로브를 해독하고, DPpri 및 DPpri 다이제스트를 산출하고, 상기 값들을 비휘발성 스토리지에 저장한다(Decrypted Keyblob = Decrypt (IV2, DPpri, DPpri Digest), SKEY 사용). 제2 초기화 벡터(IV2)는 폐기될 수도 있다. 블록(1212)에서, 디바이스는 DPpri를 해시하고 결과를 DPpri 다이제스트와 비교함으로써, DPpri의 완전성을 체크한다. 비교가 양호하면(예를 들어, 다이제스트들이 매치하면), 디바이스는 보다 초기에 획득된 유효 키로서 DPpri를 수용하고, 사용이 가능하게 한다. 디바이스는 키 획득 플래그를 참으로 설정해서, DP 개인 키가 성공적으로 획득되었음을 나타낼 수도 있다. 블록(1214)에서, 디바이스는 또 다른 IV를 선택하고, 새로운 IV를 사용해서 새로운 암호화 국부화 키블로브를 생성한다(Localized Keyblob = Encrypt (IV3, DPpri, DPpri Digest), SKEY 사용). 새로운 암호화 국부화 키블로브는 키 검색 유틸리티에 리턴될 수도 있다. 블록(1216)에서, 키 검색 유틸리티는 클라이언트 컴퓨터 시스템 내의 스토리지(예를 들어, 대용량 기억 장치(308))에 암호화 국부화 키블로브를 저장한다. 디바이스의 DPpri는 클라이언트 컴퓨터 시스템에 새롭게 안전하게 다시 한번 저장된다.

<62> 본 발명의 한 실시예에서, 한번에 서명 그룹의 모든 디바이스 DP 개인 키들을 생성할 필요는 없다. 배포 CD가 정규적으로 갱신된다고 가정하면, 디바이스 DP 개인 키들은 필요한 경우 일괄적으로 생성될 수 있다. 배포 CD가 "번(burned)"될 때마다, 생성되었지만 디바이스에 아직 할당되지 않은 디바이스 키들을 포함해서, 지금까지 생성된 키블로브 데이터베이스용 서명 그룹들을 포함한다.

<63> 한 실시예에서, 도 10의 블록(1018)에서와 같이 전체 그룹 레코드를 처리할 때, 디바이스가 에러를 검출하면, 디바이스는 에러가 발생했음을 나타내는 플래그를 설정할 수도 있으며, 프로세싱을 계속한다. 시스템 셋업을 위한 모든 단계들이 완료될 때, 디바이스는 에러를 디바이스 드라이버에게 신호해 줄 수 있다. 이는 침해자가 에러 타입 및 로케이션으로부터 정보를 획득하는 것을 차단할 수 있다.

<64> 한 실시예에서, 본 명세서에서 기술된 방법들은 디바이스의 비휘발성 스토리지의 대략 40 바이트들을 사용할 수도 있다. 다른 실시예에서, 이는 Gpub 키 해시가 디바이스의 비휘발성 스토리지에 저장되는 대신 디바이스의 암호화 키블로브에 포함되면 대략 20 바이트들로 감소될 수도 있다. 이러한 경우, 디바이스가 암호화 키블로브를 해독할 때, 디바이스는 Gpub 해시를 검색하고, Gpub를 체크하기 위해 해시를 사용하고, Gpub 키를 사용해서 전체 그룹 레코드에 대한 서명을 체크할 수도 있다.

<65> 본 명세서에 기술된 오퍼레이션들이 순차 프로세스로서 기술될 수도 있지만, 몇몇 오퍼레이션들은 실제로 병렬로 또는 동시에 실행될 수도 있다. 또한, 몇몇 실시예들에서, 오퍼레이션들의 순서는 본 발명의 원리 내에서 재배열될 수도 있다.

<66> 본 명세서에 기술된 기술들은 임의의 특정 하드웨어 또는 소프트웨어 구성으로 제한되지 않는다; 임의의 계산 또는 프로세싱 환경에서의 응용성을 찾을 수도 있다. 기술들은 하드웨어, 소프트웨어 또는 그 두 결합으로 구현될 수도 있다. 기술들은 프로세서, 프로세서에 의해 판독 가능한 기억 매체(휘발성 및 비휘발성 메모리 및/또는 스토리지 소자들을 포함), 적어도 하나의 입력 장치 및 하나 이상의 출력 장치들을 각각 포함하는 이동 컴퓨터 또는 고정 컴퓨터, 퍼스널 디지털 어시스턴트, 셋탑 박스, 셀룰러 폰 및 페이저 및 다른 전자 장치들과 같은 프로그램 가능 기계들에서 실행되는 프로그램들로 구현될 수도 있다. 프로그램 코드는 기술된 기능들을 실행하고 출력 정보를 생성하기 위해 입력 장치를 사용해서 입력된 데이터에 적용된다. 출력 정보는 하나 이상의 출력 장치들에 적용될 수도 있다. 본 기술 분야에 숙련된 자들은 멀티프로세서 시스템, 미니컴퓨터, 메인프레임 컴퓨터 등을 포함하는 다양한 컴퓨터 시스템 구성들로 본 발명이 구현될 수 있음을 알 것이다. 본 발명은 또한 통신 네트워크를 통해 연결된 원격 프로세싱 디바이스들에 의해 태스크들이 실행될 수도 있는 분산 컴퓨팅 환경에서 구현될 수 있다.

<67> 각각의 프로그램은 프로세싱 시스템과 통신하기 위해 하이 레벨 절차 또는 객체 지향 프로그래밍 언어로 구현될 수도 있다. 그러나, 프로그램들은 희망하는 경우 어셈블리어 또는 기계어로 구현될 수도 있다. 임의의 경우에, 언어는 컴파일 또는 해석될 수도 있다.

<68> 프로그램 명령들은 명령들로 프로그램된 범용 또는 특별 목적 프로세싱 시스템이 본 명세서에 기술된 오퍼레이션들을 실행하게 하는데 사용될 수도 있다. 또한, 오퍼레이션들은 오퍼레이션들을 실행하기 위한 하드와이어 로직을 포함하는 특정 하드웨어 컴포넌트들에 의해 또는 프로그램 컴퓨터 컴포넌트들 및 커스텀 하드웨어 컴포넌트들의 임의의 결합에 의해 실행될 수도 있다. 본 명세서에 기술된 방법들은 방법들을 실행하도록 프로세싱 시스템 또는 다른 전자 장치를 프로그래밍하는데 사용될 수도 있는 명령들이 저장되어 있는 기계 판독 가능 매체를 포함할 수도 있는 컴퓨터 프로그램 제품으로서 제공될 수도 있다. 본 명세서에서 사용된 "기계 판독 가능 매체"라는 용어는 기계에 의한 실행을 위한 명령 시퀀스를 저장하거나 인코드할 수 있고 기계로 하여금 본 명세서에 기술된 방법들 중 임의의 방법을 실행하게 하는 임의의 매체를 포함한다. "기계 판독 가능 매체"라는 용어는 고체 상태 메모리, 광 자기 디스크 및 데이터 신호를 인코드하는 반송파를 포함하지만, 이들로만 제한되지는 않는다. 또한, 한 형태로 또는 액션을 취하거나 결과를 야기하는 다른 형태(예를 들어, 프로그램, 프로시져, 프로세스, 애플리케이션, 모듈, 로직 등)로 소프트웨어에 관하여 말하는 것이 일반적이다. 이러한 표현들은 단지 프로세싱 시스템에 의한 소프트웨어의 실행이 프로세서가 결과를 달성하는 액션을 실행하게 함을 나타내는 속기 방법이다.

<69> 본 발명이 일례의 실시예들을 참조해서 기술되었지만, 상기 기술은 제한의 의미로 해석되지 않는다. 본 기술분야에 숙련된 자들에게 명백한 일례의 실시예들 및 본 발명의 다른 실시예들의 다양한 변경들은 본 발명의 원리 및 범위 내에 속한 것으로 간주된다.

도면의 간단한 설명

<3> 본 발명의 특징들 및 장점들은 본 발명의 이하의 상세한 설명으로부터 명백해질 것이다:

<4> 도 1은 본 발명의 한 실시예에 따라 동작하는 TPM(Trusted Platform Module)로 구현된 플랫폼을 특징으로 하는 시스템을 도시한다.

<5> 도 2는 도 1의 TPM을 포함하는 플랫폼의 제1 실시예를 도시한다.

<6> 도 3은 도 1의 TPM을 포함하는 플랫폼의 제2 실시예를 도시한다.

<7> 도 4는 도 2의 TPM으로 구현된 컴퓨터 시스템의 일례의 실시예를 도시한다.

<8> 도 5는 본 발명의 한 실시예에 따른 서명 그룹의 다이렉트 증명 키들을 분배하는 시스템의 도면이다.

<9> 도 6은 본 발명의 한 실시예에 따른 서명 그룹의 다이렉트 증명 키들을 분배하는 방법의 단계들을 도시한 플로우챠트이다.

<10> 도 7 및 도 8은 본 발명의 한 실시예에 따른 디바이스 제조 셋업 프로세싱을 도시하는 플로우챠트들이다.

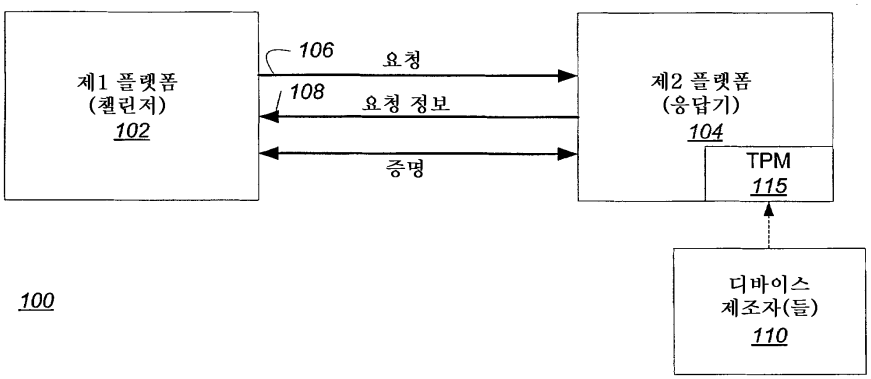
<11> 도 9는 본 발명의 한 실시예에 따른 디바이스 제조 생성 프로세싱을 도시하는 플로우챠트이다.

<12> 도 10 및 도 11은 본 발명의 한 실시예에 따른 클라이언트 컴퓨터 시스템 셋업 프로세싱을 도시하는 플로우챠트들이다.

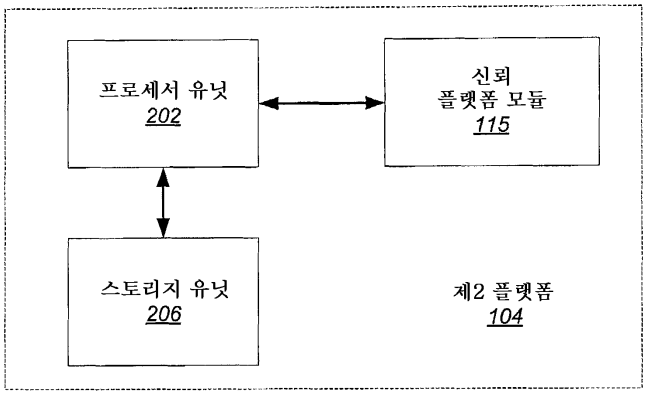
<13> 도 12는 본 발명의 한 실시예에 따른 클라이언트 컴퓨터 시스템 프로세싱을 도시하는 플로우챠트이다.

도면

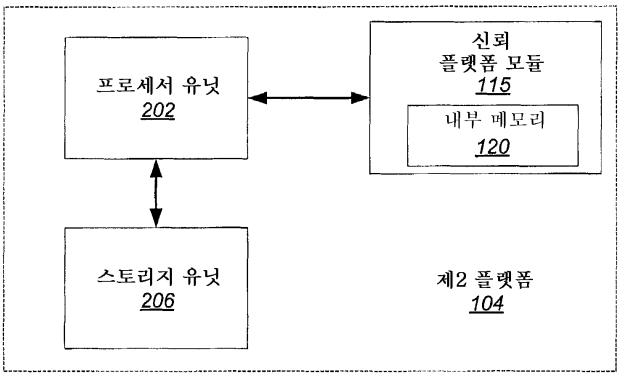
도면1



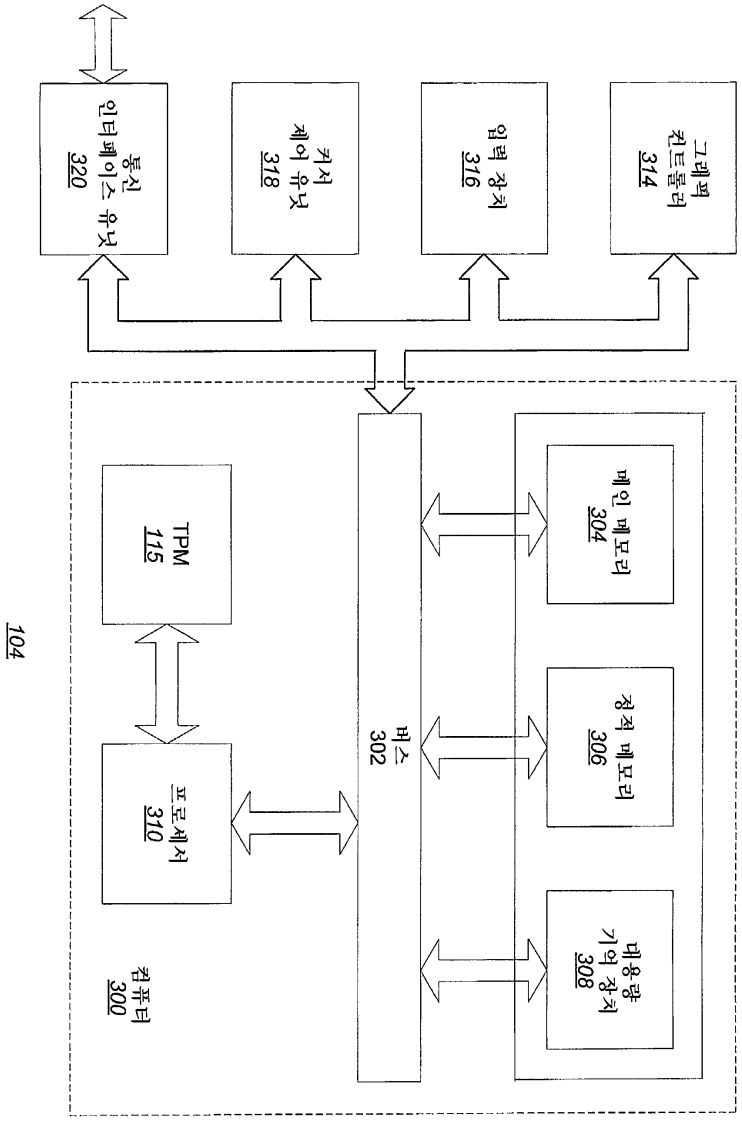
도면2



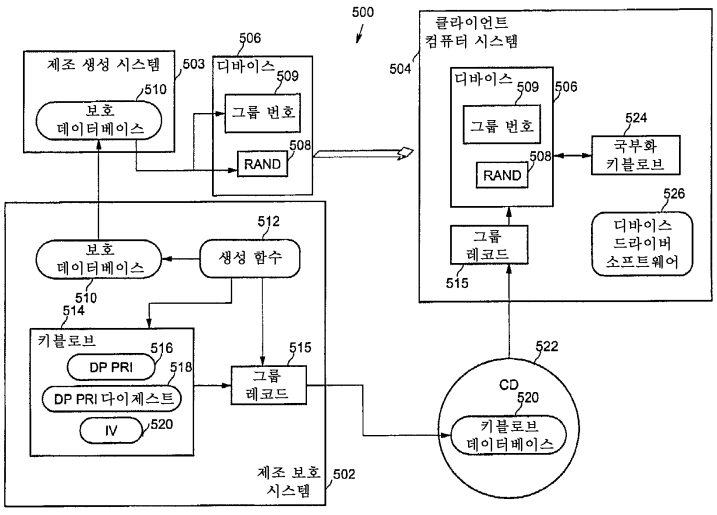
도면3



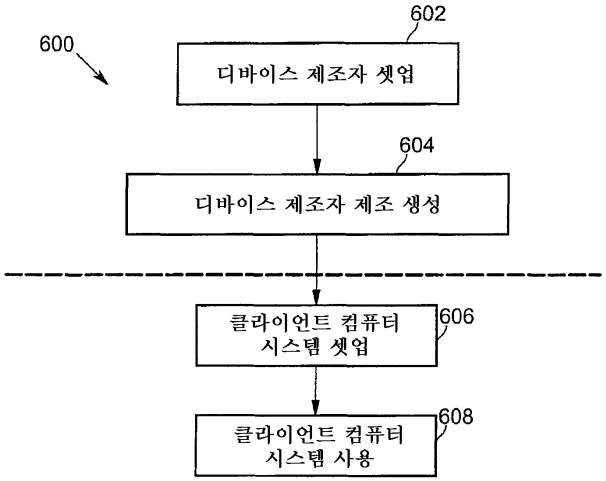
도면4


통신 인터페이스 유닛 320
커서 제어 유닛 318
입력 장치 316
그래픽 컨트롤러 314
TPM 115
메인 메모리 304
버스 302
정적 메모리 306
프로세서 310
대용량 기억 장치 308
컴퓨터 300
104

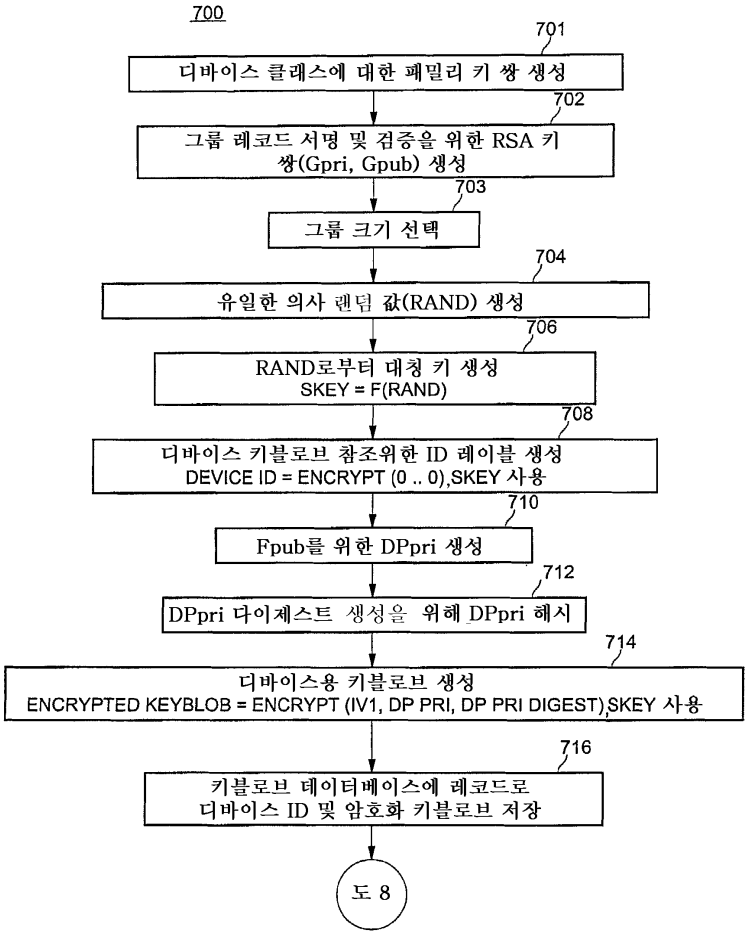
도면5


500
제조 생성 시스템
503
보호 데이터베이스
510
디바이스
506
509
그룹 번호
RAND
508
클라이언트 컴퓨터 시스템
504
디바이스
509
506
그룹 번호
RAND
508
524
국부화 키블로브
526
디바이스 드라이버 소프트웨어
그룹 레코드
515
512
보호 데이터베이스
510
생성 함수
514
키블로브
516
DP PRI
518
DP PRI 다이제스트
IV
520
515
그룹 레코드
522
CD
520
키블로브 데이터베이스
제조 보호 시스템
502

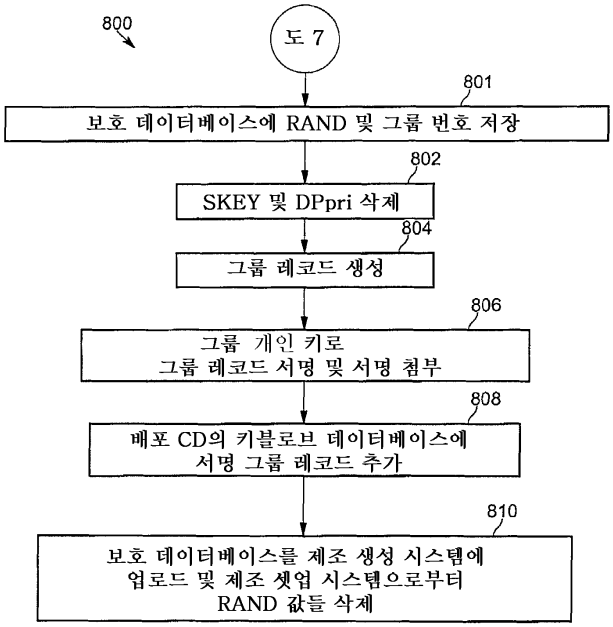
도면6


600
602
디바이스 제조자 셋업
604
디바이스 제조자 제조 생성
606
클라이언트 컴퓨터 시스템 셋업
608
클라이언트 컴퓨터 시스템 사용

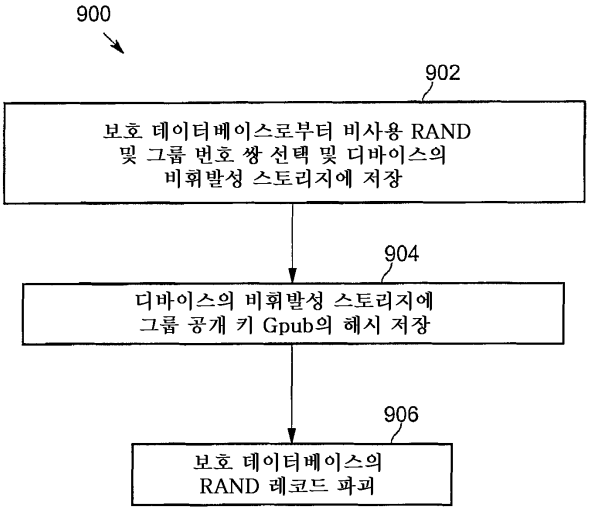
도면7


700
701
디바이스 클래스에 대한 패밀리 키 쌍 생성
702
그룹 레코드 서명 및 검증을 위한 RSA 키 쌍(Gpri, Gpub) 생성
703
그룹 크기 선택
704
유일한 의사 랜덤 값(RAND) 생성
706
RAND로부터 대칭 키 생성
SKEY = F(RAND)
708
디바이스 키블로브 참조위한 ID 레이블 생성
DEVICE ID = ENCRYPT (0 .. 0),SKEY 사용
710
Fpub를 위한 DPpri 생성
712
DPpri 다이제스트 생성을 위해 DPpri 해시
714
디바이스용 키블로브 생성
ENCRYPTED KEYBLOB = ENCRYPT (IV1, DP PRI, DP PRI DIGEST),SKEY 사용
716
키블로브 데이터베이스에 레코드로 디바이스 ID 및 암호화 키블로브 저장
도 8

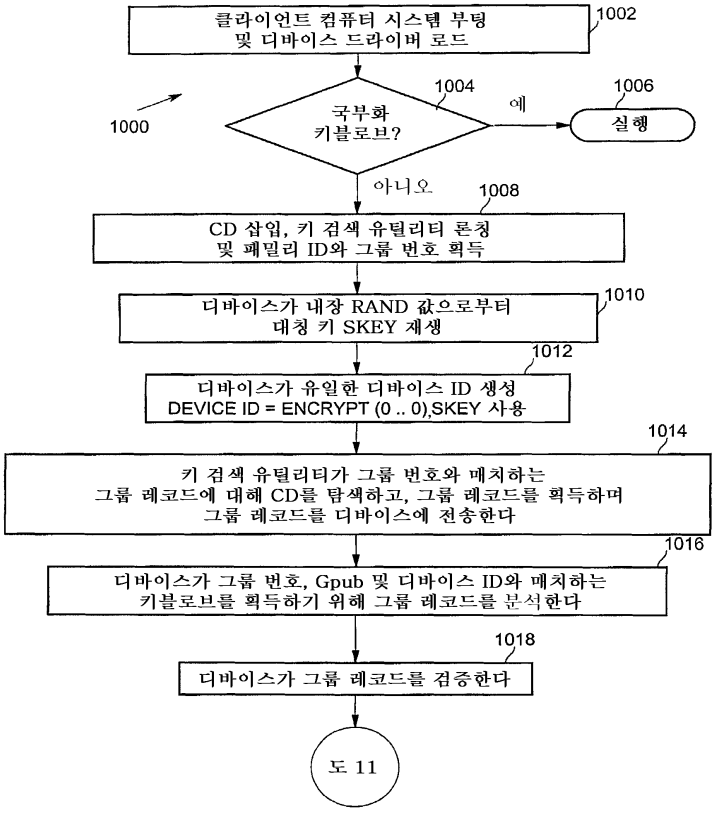
도면8


800
도 7
801
보호 데이터베이스에 RAND 및 그룹 번호 저장
802
SKEY 및 DPpri 삭제
804
그룹 레코드 생성
806
그룹 개인 키로
그룹 레코드 서명 및 서명 첨부
808
배포 CD의 키블로브 데이터베이스에
서명 그룹 레코드 추가
810
보호 데이터베이스를 제조 생성 시스템에
업로드 및 제조 셋업 시스템으로부터
RAND 값들 삭제

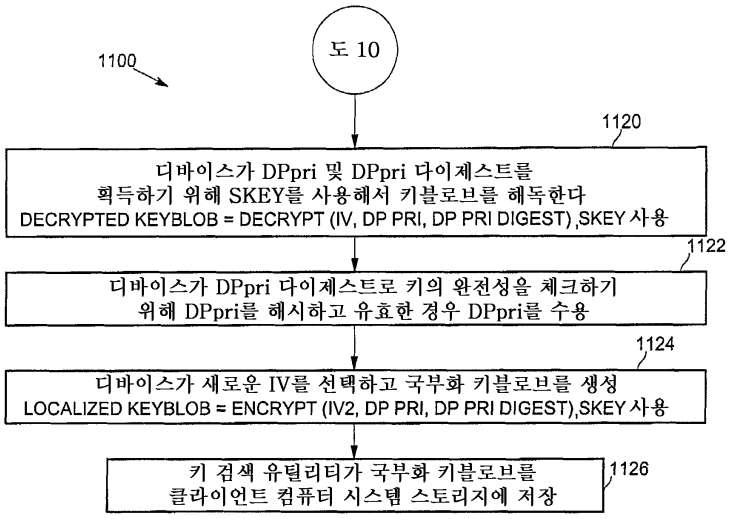
도면9


900
902
보호 데이터베이스로부터 비사용 RAND
및 그룹 번호 쌍 선택 및 디바이스의
비휘발성 스토리지에 저장
904
디바이스의 비휘발성 스토리지에
그룹 공개 키 Gpub의 해시 저장
906
보호 데이터베이스의
RAND 레코드 파괴

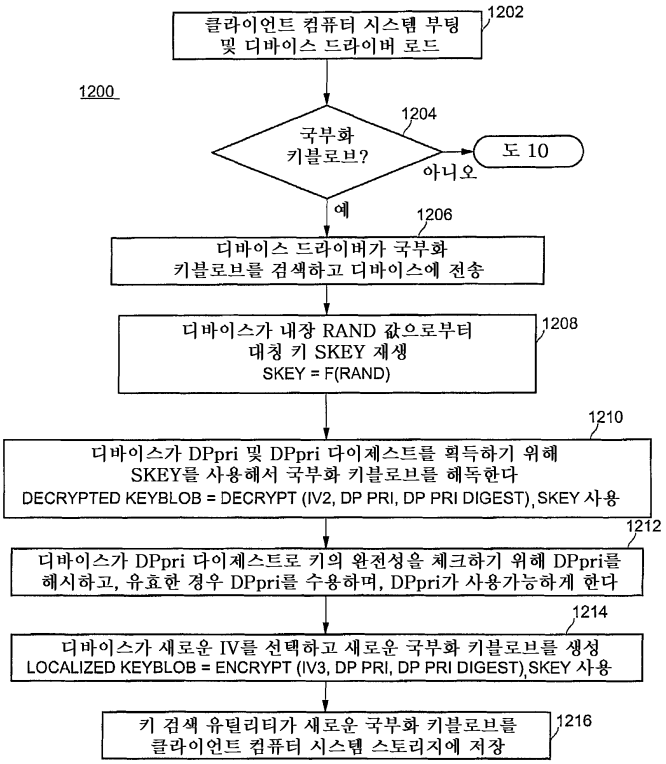
도면10


클라이언트 컴퓨터 시스템 부팅
및 디바이스 드라이버 로드
1002
1000
국부화
키블로브?
1004
예
1006
실행
아니오
1008
CD 삽입, 키 검색 유틸리티 론칭
및 패밀리 ID와 그룹 번호 획득
디바이스가 내장 RAND 값으로부터
대칭 키 SKEY 재생
1010
디바이스가 유일한 디바이스 ID 생성
DEVICE ID = ENCRYPT (0 .. 0),SKEY 사용
1012
키 검색 유틸리티가 그룹 번호와 매치하는
그룹 레코드에 대해 CD를 탐색하고, 그룹 레코드를 획득하며
그룹 레코드를 디바이스에 전송한다
1014
디바이스가 그룹 번호, Gpub 및 디바이스 ID와 매치하는
키블로브를 획득하기 위해 그룹 레코드를 분석한다
1016
디바이스가 그룹 레코드를 검증한다
1018
도 11

도면11


도 10
1100
디바이스가 DPpri 및 DPpri 다이제스트를
획득하기 위해 SKEY를 사용해서 키블로브를 해독한다
DECRYPTED KEYBLOB = DECRYPT (IV, DP PRI, DP PRI DIGEST) ,SKEY 사용
1120
디바이스가 DPpri 다이제스트로 키의 완전성을 체크하기
위해 DPpri를 해시하고 유효한 경우 DPpri를 수용
1122
디바이스가 새로운 IV를 선택하고 국부화 키블로브를 생성
LOCALIZED KEYBLOB = ENCRYPT (IV2, DP PRI, DP PRI DIGEST),SKEY 사용
1124
키 검색 유틸리티가 국부화 키블로브를
클라이언트 컴퓨터 시스템 스토리지에 저장
1126

도면12


1200
클라이언트 컴퓨터 시스템 부팅
및 디바이스 드라이버 로드
1202
국부화
키블로브?
1204
도 10
아니오
예
디바이스 드라이버가 국부화
키블로브를 검색하고 디바이스에 전송
1206
디바이스가 내장 RAND 값으로부터
대칭 키 SKEY 재생
SKEY = F(RAND)
1208
디바이스가 DPpri 및 DPpri 다이제스트를 획득하기 위해
SKEY를 사용해서 국부화 키블로브를 해독한다
DECRYPTED KEYBLOB = DECRYPT (IV2, DP PRI, DP PRI DIGEST), SKEY 사용
1210
디바이스가 DPpri 다이제스트로 키의 완전성을 체크하기 위해 DPpri를
해시하고, 유효한 경우 DPpri를 수용하며, DPpri가 사용가능하게 한다
1212
디바이스가 새로운 IV를 선택하고 새로운 국부화 키블로브를 생성
LOCALIZED KEYBLOB = ENCRYPT (IV3, DP PRI, DP PRI DIGEST), SKEY 사용
1214
키 검색 유틸리티가 새로운 국부화 키블로브를
클라이언트 컴퓨터 시스템 스토리지에 저장
1216