(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0056199
(43) 공개일자 2013년05월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(21) 출원번호 10-2012-0132502
(22) 출원일자 2012년11월21일
심사청구일자 2012년11월21일
(30) 우선권주장
13/523,801 2012년06월14일 미국(US)
61/562,050 2011년11월21일 미국(US)

(71) 출원인
브로드콤 코포레이션
미합중국, 92617 캘리포니아 어빈, 캘리포니아 애비뉴 5300
(72) 발명자
뷰어, 마크
미국 애리조나 85541 페이슨 에이취씨2 박스 98에프
첸, 키
미국 캘리포니아 95014 쿠퍼티노 오크리프 피아이. 10079
(74) 대리인
특허법인에이아이피

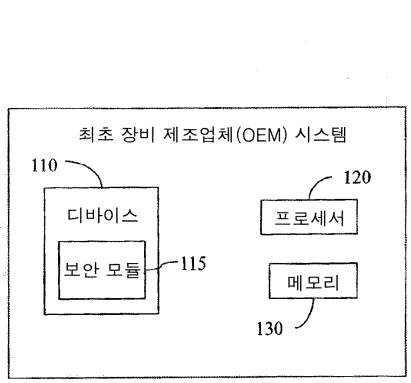
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **보안 키 생성**

(57) 요 약

보안 키 생성을 위한 방법들 및 시스템들이 제공된다. 실시예들에서, 제조 프로세스 동안에, 디바이스는 디바이스를 위한 주 시드를 생성하고 시드를 디바이스 내에 저장한다. 디바이스는 디바이스 주 키를 보안 제조업체 서버에 엑스포트(export) 한다. 보안 제조업체 서버는 디바이스를 위한 공개/사설 루트 키를 생성하고, 디바이스의 공개 루트 키를 위한 증명서를 인증 기관으로부터 요청한다. 저장된 주 시드를 갖는 디바이스는 최종-사용자 시스템 내로 통합된다. 조건의 발생 후에, 최종-사용자 시스템으로 통합 후의 디바이스는 필드에서 공개/사설 루트 키를 생성한다. 또한, 시스템은 공개 루트 키를 위한 증명서를 수신 및 설치한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

보안 키 생성을 위한 장치로서,

보안 모듈을 갖는 디바이스; 및

상기 디바이스에 결합된 메모리를 포함하고,

상기 보안 모듈은,

주 시드(primary seed)를 저장하는 비휘발성 메모리,

상기 장치 내에서 조건의 발생 후에 상기 주 시드로부터 디바이스 루트 키(device root key)를 생성하도록 구성된 프로세서를 포함하는, 보안 키 생성을 위한 장치.

청구항 2

청구항 1에 있어서,

상기 보안 모듈의 상기 프로세서는 또 하나의 암호 디바이스 키를 이용하여 상기 디바이스 루트 키를 암호화하도록 더 구성되는, 보안 키 생성을 위한 장치.

청구항 3

청구항 1에 있어서,

상기 디바이스 루트 키는 공개 디바이스 루트 키(public device root key) 및 사설 디바이스 루트 키(private device root key)를 포함하는, 보안 키 생성을 위한 장치.

청구항 4

청구항 3에 있어서,

상기 보안 모듈의 상기 프로세서는 또 하나의 암호 디바이스 키를 이용하여 상기 사설 디바이스 루트 키를 암호화하도록 더 구성되는, 보안 키 생성을 위한 장치.

청구항 5

청구항 2에 있어서,

상기 메모리는 상기 암호화된 디바이스 루트 키를 저장하도록 구성되는, 보안 키 생성을 위한 장치.

청구항 6

청구항 4에 있어서,

상기 메모리는 상기 암호화된 사설 디바이스 루트 키를 저장하도록 구성되는, 보안 키 생성을 위한 장치.

청구항 7

청구항 3에 있어서,

상기 디바이스 루트 키를 위한 증명서를 수신하기 위한 인터페이스를 더 포함하고, 상기 증명서는 상기 공개 디바이스 루트 키와, 상기 증명서를 발행하였던 인증 기관의 서명을 포함하는, 보안 키 생성을 위한 장치.

청구항 8

청구항 7에 있어서,

상기 메모리는 RSA 디바이스 루트 키를 위한 증명서를 저장하도록 더 구성되는, 보안 키 생성을 위한 장치.

청구항 9

청구항 1에 있어서,

상기 조건은 키의 생성을 요청하는 명령인, 보안 키 생성을 위한 장치.

청구항 10

청구항 1에 있어서,

상기 조건은 상기 장치의 초기 시동인, 보안 키 생성을 위한 장치.

청구항 11

청구항 1에 있어서,

상기 조건은 상기 보안 모듈의 초기 액세스인, 보안 키 생성을 위한 장치.

청구항 12

청구항 1에 있어서,

상기 디바이스 루트는 RSA 디바이스 루트 키인, 보안 키 생성을 위한 장치.

청구항 13

보안 모듈 및 메모리를 갖는 디바이스를 포함하는 최종-사용자 장치에 의한 보안 키 생성을 위한 방법으로서,

공개 디바이스 루트 키를 위한 증명서를 수신하는 단계로서, 상기 증명서는 상기 공개 디바이스 루트 키와, 상기 증명서를 발행하였던 인증 기관의 디지털 서명을 포함하는, 상기 증명서를 수신하는 단계;

상기 증명서를 검증하는 단계;

상기 최종-사용자 장치 내에서 조건의 발생 후에 상기 보안 모듈 내의 메모리에 저장된 사전-연산된 주 시드를 이용하여 사설 디바이스 루트 키를 생성하는 단계; 및

상기 증명서 및 상기 사설 디바이스 루트 키를 상기 장치의 상기 메모리에 저장하는 단계를 포함하는, 보안 키 생성을 위한 방법.

청구항 14

청구항 13에 있어서,

상기 조건은 키의 생성을 요청하는 명령인, 보안 키 생성을 위한 방법.

청구항 15

디바이스 제조업체 서버에서의 보안 키 생성을 위한 방법으로서,

디바이스를 위한 주 시드를 수신하는 단계로서, 상기 주 시드는 제조업체 키로 암호화되는, 상기 주 시드를 수신하는 단계;

상기 디바이스 제조업체 서버에서, 상기 디바이스의 상기 주 시드를 복호화하는 단계;

상기 디바이스 제조업체 서버의 보안 모듈에서, 상기 디바이스를 위한 상기 수신된 주 시드를 이용하여 상기 디바이스를 공개 및 사설 RSA 루트 키를 생성하는 단계;

상기 생성된 공개 디바이스 루트 키를 위한 증명서를 인증 기관으로부터 요청하는 단계;

상기 인증 기관으로부터 상기 생성된 공개 디바이스 루트 키를 위한 상기 증명서를 수신하는 단계;

상기 증명서를 상기 디바이스를 통합하는 시스템에 제공하는 단계; 및

상기 디바이스 제조업체 서버로부터 상기 사설 루트 키를 삭제하는 단계를 포함하는, 보안 키 생성을 위한 방법.

명 세 서

기 술 분 야

[0001] **관련 출원들에 대한 상호 참조**

[0002] 본 출원은 그 전체가 참조를 위해 여기에 병합되는, "Secure Key Generation"이라는 명칭으로 2011년 11월 21일자로 출원된, 미국 특허 가출원 제 61/562,050호의 이익을 주장한다.

[0003] **발명의 분야**

[0004] 본 출원은 일반적으로 데이터 통신 보안에 관한 것으로, 더욱 구체적으로, 암호 키 관리(cryptographic key management)에 관한 것이다.

배 경 기 술

[0005] 컴퓨터 시스템들은 널리 다양한 보안 위협들의 목표물들이 되는 일이 증가하고 있다. 다수의 컴퓨터 아키텍처(computer architecture)들은 애플리케이션들을 위한 하드웨어 지원을 제공하기 위하여 보안 서브-모듈(security sub-module) 또는 별개의 자립형 보안 프로세서(stand alone secure processor)를 갖는 디바이스를 통합한다. 이 보안 서브-모듈 또는 보안 프로세서는 종종 전체 시스템의 보안 토대가 되고 있다. 이들 시스템들에서는, 디바이스가 디바이스-고유 루트 키(device-unique root key)를 소유하는 것이 바람직하다. 종종, 디바이스-특정 루트 키(device-specific root key)는 사설 키 부분(private key portion) 및 공개 키 부분(public key portion)을 가지는 비대칭 키(asymmetric key)이다.

[0006] 디바이스-고유 루트 키의 공개 부분은 증명서(certificate)를 통해 인증 기관(CA : certificate authority)에 의해 증명될 수 있다. 증명서는 신뢰 기관(상기 CA)의 디지털 서명을 이용하여 디바이스-고유 루트 키의 공개 부분을 개인 또는 법인과 같은 엔티티(entity)에 바인딩(binding)한다. 전형적으로, 디지털 서명은 CA의 사설 키로 암호화되는 적어도 디바이스 공개 키의 해시(hash)이다. 디바이스 루트 키의 증명서를 제공함으로써, 상기 디바이스를 통합하는 시스템은 그 피어(peer)들 또는 네트워크 계층으로 하이 레벨(high level)의 신뢰도를 수립할 수 있다. 직접적으로 또는 간접적으로, 디바이스 루트 키는 시스템의 진실성을 수립하거나, 시스템 상태 정보를 증명하거나, 양방향 통신을 보장하기 위해 이용될 수 있다.

[0007] 디바이스 루트 키를 생성하고, 디바이스를 포함하는 시스템에 디바이스 루트 키를 위한 증명서를 발행하는 것은 실행적으로 그리고 기술적으로 디바이스 제조 프로세스에 거대한 과제를 제공한다. RSA 루트 키들의 생성은 극도로 시간 소비적이므로, 대량 생산을 위해서는 실현 가능하지 않다. 부가적으로, 그 대신에 키들이 디바이스 내로 주입되는 경우, 보안 평가들에 있어서의 보증은 키들을 주입하는 장비 및 디바이스들 사이의 보안 통신을 요구한다.

[0008] 그러므로, 필요한 것은 필드(field)에서 디바이스 루트 키들을 보안성 있게 생성하고 디바이스 루트 키 증명서들을 발행하기 위한 시스템들 및 방법들이다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 보안 키 생성을 위한 장치 및 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0010] 일 측면에 따르면, 보안 키 생성을 위한 장치는,

[0011] 보안 모듈을 갖는 디바이스; 및

[0012] 상기 디바이스에 결합된 메모리를 포함하고,

[0013] 상기 보안 모듈은,

[0014] 주 시드(primary seed)를 저장하는 비휘발성 메모리,

[0015] 상기 장치 내에서 조건의 발생 후에 상기 주 시드로부터 디바이스 루트 키(device root key)를 생성하도록 구성

된 프로세서를 포함한다.

[0016] 바람직하게는, 상기 보안 모듈의 상기 프로세서는 또 하나의 암호 디바이스 키를 이용하여 상기 디바이스 루트 키를 암호화하도록 더 구성된다.

[0017] 바람직하게는, 상기 디바이스 루트 키는 공개 디바이스 루트 키(public device root key) 및 사설 디바이스 루트 키(private device root key)를 포함한다.

[0018] 바람직하게는, 상기 보안 모듈의 상기 프로세서는 또 하나의 암호 디바이스 키를 이용하여 상기 사설 디바이스 루트 키를 암호화하도록 더 구성된다.

[0019] 바람직하게는, 상기 메모리는 상기 암호화된 디바이스 루트 키를 저장하도록 구성된다.

[0020] 바람직하게는, 상기 메모리는 상기 암호화된 사설 디바이스 루트 키를 저장하도록 구성된다.

[0021] 바람직하게는, 상기 디바이스 루트 키를 위한 증명서를 수신하기 위한 인터페이스를 더 포함하고, 상기 증명서는 상기 공개 디바이스 루트 키와, 상기 증명서를 발행하였던 인증 기관의 서명을 포함한다.

[0022] 바람직하게는, 상기 메모리는 RSA 디바이스 루트 키를 위한 증명서를 저장하도록 더 구성된다.

[0023] 바람직하게는, 상기 조건은 키의 생성을 요청하는 명령이다.

[0024] 바람직하게는, 상기 조건은 상기 장치의 초기 시동이다.

[0025] 바람직하게는, 상기 조건은 상기 보안 모듈의 초기 액세스이다.

[0026] 바람직하게는, 상기 디바이스 루트는 RSA 디바이스 루트 키이다.

[0027] 일 측면에 따르면, 보안 모듈 및 메모리를 갖는 디바이스를 포함하는 최종-사용자 장치에 의한 보안 키 생성을 위한 방법이 제공되고, 상기 방법은,

[0028] 공개 디바이스 루트 키를 위한 증명서를 수신하는 단계로서, 상기 증명서는 상기 공개 디바이스 루트 키와, 상기 증명서를 발행하였던 인증 기관의 디지털 서명을 포함하는, 상기 증명서를 수신하는 단계;

[0029] 상기 증명서를 검증하는 단계;

[0030] 상기 최종-사용자 장치 내에서 조건의 발생 후에 상기 보안 모듈 내의 메모리에 저장된 사전-연산된 주 시드를 이용하여 사설 디바이스 루트 키를 생성하는 단계; 및

[0031] 상기 증명서 및 상기 사설 디바이스 루트 키를 상기 장치의 상기 메모리에 저장하는 단계를 포함한다.

[0032] 바람직하게는, 상기 조건은 키의 생성을 요청하는 명령이다.

[0033] 바람직하게는, 상기 조건은 상기 장치의 초기 시동이다.

[0034] 바람직하게는, 상기 조건은 상기 보안 모듈의 초기 액세스이다.

[0035] 바람직하게는, 상기 방법은,

[0036] 상기 디바이스를 인증하기 위하여 상기 증명서를 제 2 장치에 제공하는 단계를 더 포함한다.

[0037] 일 측면에 따르면, 디바이스 제조업체 서버에서의 보안 키 생성을 위한 방법은,

[0038] 디바이스를 위한 주 시드를 수신하는 단계로서, 상기 주 시드는 제조업체 키로 암호화되는, 상기 주 시드를 수신하는 단계;

[0039] 상기 디바이스 제조업체 서버에서, 상기 디바이스의 상기 주 시드를 복호화하는 단계;

[0040] 상기 디바이스 제조업체 서버의 보안 모듈에서, 상기 디바이스를 위한 상기 수신된 주 시드를 이용하여 상기 디바이스를 공개 및 사설 RSA 루트 키를 생성하는 단계;

[0041] 상기 생성된 공개 디바이스 루트 키를 위한 증명서를 인증 기관으로부터 요청하는 단계;

[0042] 상기 인증 기관으로부터 상기 생성된 공개 디바이스 루트 키를 위한 상기 증명서를 수신하는 단계;

[0043] 상기 증명서를 상기 디바이스를 통합하는 시스템에 제공하는 단계; 및

[0044] 상기 디바이스 제조업체 서버로부터 상기 사설 루트 키를 삭제하는 단계를 포함한다.

[0045] 바람직하게는, 상기 방법은 상기 공개 디바이스 루트 키를 디바이스 루트 키 명칭과 연관시키는 단계를 더 포함한다.

[0046] 바람직하게는, 상기 디바이스 루트 키 명칭은 상기 디바이스를 위한 일련 번호(sequence number) 및 상기 디바이스를 위한 상기 주 시드를 이용하여 생성된다.

[0047] 바람직하게는, 상기 일련 번호는 다수의 디바이스들 내의 상기 디바이스에 대해 고유하다.

[0048] 바람직하게는, 상기 방법은,

[0049] 상기 디바이스 루트 키 명칭 및 상기 공개 디바이스 루트 키를 제조업체 데이터베이스에 저장하는 단계를 더 포함한다.

발명의 효과

[0050] 본 발명에 따르면, 보안 키 생성을 위한 장치 및 방법을 구현할 수 있다.

도면의 간단한 설명

[0051] 여기에 병합되어 명세서의 일부를 구성하는 첨부 도면들은 본 발명을 예시하고, 그 설명과 함께, 발명의 원리들을 설명하고, 관련 기술의 당업자가 발명을 제조 및 이용하도록 작용한다.

도 1은 본 발명의 실시예들을 병합하는 시스템의 하이-레벨 블록 다이어그램이다.

도 2는 발명의 실시예에 따른 예시적인 보안 모듈의 블록 다이어그램이다.

도 3은 본 발명의 실시예들을 통합하는 예시적인 동작 환경을 도시한다.

도 4는 본 발명의 실시예들에 따라, 디바이스 루트 키들의 주문형 필드 생성(on-demand field generation)을 위한 방법의 순서도를 도시한다.

도 5는 본 발명의 실시예들에 따라, OEM에 의한 디바이스 루트 키들의 디바이스로의 주입을 위한 방법의 순서도를 도시한다.

도 6은 본 발명의 실시예들에 따라, 디바이스 루트 키들의 제조업체 주입을 위한 방법의 순서도를 도시한다.

도 7은 본 발명의 실시예들에 따라, RSA 디바이스 키들의 시드-기반 필드내 유도(seed-based in-field derivation)를 위한 방법의 순서도를 도시한다.

본 발명은 첨부 도면들을 참조하여 설명될 것이다. 구성요소가 처음 나타나는 도면은 대응하는 참조 번호에서 가장 좌측 숫자(들)에 의해 전형적으로 표시된다.

발명을 실시하기 위한 구체적인 내용

[0052] 다음의 설명에서, 다수의 특정한 상세 사항들은 발명의 철저한 이해를 제공하기 위해 설명된다. 그러나, 구조들, 시스템들, 및 방법들을 포함하는 발명은 이들 특정한 상세 사항들 없이 실시될 수 있다는 것이 당업자들에게 명백할 것이다. 여기에서의 설명 및 표현은 그 작업의 실체를 당 업계의 다른 사람들에게 가장 효과적으로 전달하기 위하여 당 업계의 숙련자들 또는 당업자들에 의해 이용되는 통상적인 수단이다. 다른 사례들에서는, 발명의 측면들을 불필요하게 모호하게 하는 것을 회피하기 위하여, 잘 알려진 방법들, 절차들, 부품들, 및 회로는 구체적으로 설명되지 않았다.

[0053] "하나의 실시예", "실시예", "일 예의 실시예" 등에 대한 명세서에서의 참조들은 설명된 실시예가 특별한 특징, 구조, 또는 특성을 포함할 수 있지만, 모든 실시예가 반드시 그 특별한 특징, 구조, 또는 특성을 포함하지 않을 수도 있음을 표시한다. 또한, 이러한 어구들은 반드시 동일한 실시예를 참조하는 것이 아니다. 또한, 특별한 특징, 구조, 또는 특성이 실시예와 관련하여 설명될 때, 명시적으로 설명되어 있든 그렇지 않든 간에 다른 실시예들과 관련하여 이러한 특징, 구조, 또는 특성에 영향을 주는 것은 당업자의 지식 범위 내에 있다고 사료된다.

[0054] **보안 키 생성을 위한 시스템**

[0055] 이동 디바이스, 컴퓨터, 또는 다른 전자 기기와 같은 최종-사용자(end-user) 시스템은 다수의 제조업체들로부터

의 디바이스들을 통합한다. 예를 들어, 이동 핸드셋(mobile handset)은 다른 부품들 중에서도, 기저대역 프로세서(baseband processor), 트랜시버(transceiver), GPS 수신기, 및/또는 블루투스(Bluetooth) 디바이스를 포함할 수 있다. 시스템을 위한 필요한 디바이스들은 최종-사용자 시스템의 조립을 위해 다양한 디바이스 제조업체들에 의해, 최초 장비 제조업체라고 통상적으로 지칭되는 시스템 제조업체에게 제공된다.

[0056] 도 1은 본 발명의 실시예들을 병합하는 시스템(100)의 하이-레벨 블록 다이어그램이다. 시스템(100)은 데스크톱 컴퓨터(desktop computer), 무선 컴퓨터(wireless computer), 서버(server), 라우터(router), 무선 핸드셋(wireless handset) 또는 임의의 다른 형태의 전자 디바이스를 포함하지만 이것으로 한정되지는 않는 임의의 유형의 전자 기기(electronic appliance)일 수 있다. 시스템(100)은 최초 장비 제조업체(OEM : original equipment manufacturer)에 의해 만들어질 수 있다. 하이 레벨에서, 시스템(100)은 디바이스(110), 프로세서(120), 및 메모리(130)를 포함한다.

[0057] 실시예들에서, 디바이스(110)는 최초 장비 제조업체와는 상이한 제조업체에 의해 제조될 수 있다. 실시예들에서, 디바이스(110)는 보안 모듈(security module)(115)을 포함한다. 보안 모듈(115)은 보안 애플리케이션들을 위한 하드웨어 지원을 제공한다. 대안적인 실시예들에서, 디바이스(110)는 유니버설 보안 허브(USH : universal security hub)와 같은 자립형 보안 프로세서(stand-alone secure processor)일 수 있다. 디바이스(110)는 루트 암호 키(root cryptographic key)(여기에서는 "디바이스 루트 키(device root key)"라고 지칭됨)를 소유한다. 디바이스를 위한 루트 키는 추가적인 키들을 생성하는 것을 포함하지만 이것으로 한정되지는 않는 다수의 목적들을 위해 이용될 수 있는 마스터 키(master key)이다.

[0058] 디바이스(110)와 같은 디바이스들을 위한 루트 키들은 각각의 디바이스에 통계적으로 고유할 수 있고 그 디바이스에 바인딩되어야 한다. 본딩(bonding)을 보장하기 위하여, 디바이스 루트 키는 디바이스 상에서 생성되거나 외부적으로 생성되고, 디바이스 내로 보안성 있게 주입된다. 디바이스가 배치된 후, 디바이스 루트 키는 디바이스(110)의 비휘발성 메모리(non-volatile memory) 또는 암호 방식으로 디바이스에 바인딩되어 있는 외부의 비휘발성 메모리(예를 들어, 메모리(130)) 내에 저장된다.

[0059] 디바이스 루트 키들은 전형적으로, 취소할 수 없는 장기 키(long-term key)들이다. 디바이스 루트 키들은 다른 기관들과 신뢰를 수립하기 위해 사용되므로, 디바이스 루트 키들은 충분히 암호 방식에 있어서 강력하고 양호하게 보호되어야 한다. 공개 키 암호화에 기반한 비대칭 키들은 비밀(사설) 키들이 피어(peer)들 사이에서 공유되지 않으므로 강력하게 선호된다.

[0060] 디바이스 루트 키는 인증 기관(CA)에 의해 증명될 수 있다. 증명 프로세스 동안에, CA는 디바이스 루트 키를 위한 증명서를 생성한다. 증명서는 디바이스 루트 키의 공개 키 부분을 식별자(예를 들어, 디바이스의 제조업체)와 바인딩한다. 증명서는 다른 구성요소들 중에서도, 디바이스 루트 키(예를 들어, 공개 디바이스 루트 키), 디바이스 제조업체의 식별, CA의 식별, 및 CA를 위한 디지털 서명을 포함한다. CA를 위한 디지털 서명은 증명서 내의 정보를 해싱하고 해싱된 정보를 CA의 사설 키로 암호화함으로써 얻어진다. 디바이스 루트 키를 위한 증명서를 제공함으로써, 네트워크 환경 내의 다른 기관들과 추가적인 신뢰가 진전될 수 있다.

[0061] 디바이스 루트 키들 및 대응하는 루트 키 증명서들을 생성하기 위해서는 중요한 과제들이 존재한다. 예를 들어, 제조 도중에 디바이스 루트 키들을 생성하는 것은 제조 프로세스의 비용을 증가시킨다. 대량의 디바이스 제조 프로세스들에서는, 디바이스의 비용이 처리 비용뿐만 아니라 재료 비용(예를 들어, 웨이퍼, 마스크, 패키지 비용들)에 의해 결정된다. 처리 비용에 대한 주요한 기여자는 각각의 디바이스에 대해 소비된 처리 시간이다.

[0062] 이상적으로는, 온-칩 랜덤 엔트로피 소스(on-chip random entropy source)와, 제조 프로세스에서 테스트 프로그램을 갖는 다른 암호 기능들에 기반으로 하여 디바이스에 의해 디바이스 루트 키가 생성되어야 한다. 이 프로세스는 디바이스 루트 키의 사설 부분이 디바이스에만 알려지고 그 디바이스를 절대로 떠나지 않는다는 것을 보장한다. 그러나, 디바이스 루트 키가 RSA 키일 때, 디바이스에 의한 RSA 키의 생성은 과제들을 제공한다.

[0063] 현재, RSA는 보안 애플리케이션들에 의해 지원되는 지배적인 알고리즘이다. 그러므로, 디바이스 루트 키들의 대다수는 RSA 키들이다. RSA 보안은 큰 수를 인수분해하는 어려움으로부터 유래된다. RSA 공개/사설 키 쌍들을 생성하기 위하여, 2개의 무작위의 큰 소수(prime number)들, p 및 q가 먼저 선택된다. p 및 q의 선택은 온-칩 엔트로피 소스에 의해 생성되는 시드(seed)를 이용한 밀러-라빈(Miller-Rabin) 알고리즘에 기반하고 있다. 2048-비트 RSA 키에 대하여, 2개의 소수들은 각각 1024-비트들이다. 소수 선택 알고리즘은 극도로 시간 소모적이다. 프로세스의 지속기간은 대략 15초로부터 1분 이상까지 상당히 변동된다. RSA 루트 키가 제조 프로세스 동안에 디바이스에 의해 생성된다면, 디바이스의 비용은 소수 선택 프로세스에 의해 도입되는 증가된 처리 시간으로 인

해 상당히 증가할 것이다. 또한, 연산의 비-결정론적(non-deterministic) 특성은 대량 생산을 위해 테스트 프로그램을 설정하는 것을 어렵게 한다.

[0064] 부가적으로, 디바이스(110)와 같은 디바이스들은 제한된 온-칩 메모리를 가진다. RSA 사설 키는 중국인의 나머지 정리(Chinese remainder theorem)를 이용한 사설 키 동작들을 위한 퀸터플렛(quintuplet) {p, q, dp, dq, qinv}에 의해 표현된다. 2048-비트 RSA 디바이스 키에 대하여, 각각의 파라미터는 1024-비트이다. RSA 키가 온-칩에서 생성되는 경우, 사설 키는 안전하게 저장되어야 하고 디바이스에 바인딩되어야 한다. 제 1 방법에서, 디바이스(110)는 RSA 사설 키가 생성된 후에 디바이스 비휘발성 메모리로 프로그래밍되도록 하기 위하여, 디바이스(110)는 충분한 비휘발성 메모리 온-칩을 가진다. 제 2 방법에서, RSA 사설 키는 디바이스 고유 대칭 키(예를 들어, 256-비트 AES 키)로 암호화되고 엑스포트(export) 된다. 이 방법에서, 디바이스 고유 대칭 키는 디바이스 내에서 프로그래밍가능 비휘발성 메모리로 프로그래밍되어야 한다.

[0065] 진보된 CMOS 디지털 프로세스를 이용하여 제조된 디바이스들에 대하여, 내장된 플래시(embedded flash)와 같이, 온-칩 리-프로그래밍 가능한(re-programmable) 비휘발성 메모리 기술은 이용가능하지 않다. 이러한 큰 키를 저장하기 위하여 1회용 프로그래밍 가능한(OTP : one-time programmable) 비휘발성 메모리를 이용하는 것은 다이 크기(die size)를 상당히 증가시킬 것이다. 또한, OTP 저장장치는 어떤 애플리케이션을 위하여 루트 키를 취소하고 재수립(re-establish)하는 것을 불가능하게 한다. 그러므로, 제 1 방법은 이들 진보된 CMOS 디지털 프로세스들을 이용하여 제조된 디바이스들을 위해서는 실행가능하지 않다.

[0066] 그러나, 제 2 방법은 실행적인 과제들을 겪는다. 예를 들어, 제 2 방법이 디바이스 제조 프로세스에서 적용될 때, 암호화된 사설 키 및 그 대응하는 공개 키는 수집되어 데이터베이스로 목록화되어야 한다. 암호화된 사설 키는 시스템(100)의 최초 장비 제조업체(OEM)에 의해 추후에 디바이스로 다시 주입되어야 한다. 대안적으로, 일단 외부적으로 부착된 플래시가 이용가능하면, 암호화된 키는 필드에서 디바이스로 주입될 수 있다. 이하에서 더욱 구체적으로 설명된 바와 같이, 필드에서의 루트 키의 주입은 보안 과제들을 제공한다.

[0067] 도 2는 발명의 실시예에 따른 예시적인 보안 모듈(210)의 블록 다이어그램이다. 보안 모듈(210)은 하나 이상의 보안 처리 유닛들(202), 난수 생성기(226), 공개 키 가속기(234), 비휘발성 메모리(222)를 포함한다. 난수 생성기(226)는 난수들을 생성하도록 구성된다. 예를 들어, 여기에 설명된 실시예들에서, 난수 생성기(226)는 RSA 공개/사설 키 쌍(pair)을 생성하기 위한 시드(seed)로서 난수를 생성하도록 구성된다. 공개 키 가속기(PKA : public key accelerator)(234)는 지원되는 공개 키 동작들에 특정된 처리를 취급하도록 구성된다. 예를 들어, 공개 키 가속기는 RSA 공개/사설 루트 키를 생성하도록 구성될 수 있다.

[0068] 보안 모듈(210)(또는 보안 프로세서)은 보안 모듈(또는 보안 프로세서)이 외부 디바이스들과 통신하는 것을 가능하게 하는 부품들을 포함할 수도 있다. 이 부품들은 직접 메모리 액세스(DMA : Direct Memory Access) 엔진, 주변 부품 상호접속(PCI : Peripheral Component Interconnect) 인터페이스, 범용 인터페이스, 유니버설 직렬 버스(USB : Universal Serial Bus) 인터페이스 및/또는 하나 이상의 버스들을 포함할 수 있다. 보안 모듈(210)은 키 관리자(204), 보안 보호 로직, 및 RAM과 같은 특정 실시예들에 의해 요구되는 바와 같이 추가적인 또는 대안적인 구성요소들을 더 포함할 수 있다.

[0069] 도 3은 본 발명의 실시예들을 통합하는 예시적인 동작 환경(390)을 도시한다. 환경(390)은 디바이스 제조업체, 최초 장비 제조업체(OEM), 인증 기관, 및 사용자를 포함한다. 디바이스 제조업체는 디바이스 제조업체 설비(340), 선택적인 키 서버(350), 및 키 관리 데이터베이스(355)를 가진다. 실시예에서, 키 서버(250) 및 데이터베이스(355)는 디바이스 제조업체 설비에 위치되지 않는다. 제조업체 설비(340)는 디바이스들(310)을 제조한다. 위에서 설명된 바와 같이, 각각의 디바이스(310)는 연관된 디바이스 루트 키를 가진다. 제조업체 설비(340)는 제조업체 키 서버(350)와 통신하도록 구성된 하나 이상의 컴퓨터들(345)을 더 포함한다. 제조업체 키 서버(350)는 제조업체 디바이스들(310)을 위한 키들 및 증명서들을 관리하는 것을 담당하고 있다. 제조업체 키 서버(350)는 보안 서버이다. 실시예들에서, 제조업체 키 서버(350)는 하드웨어 보안 모듈(HSM : hardware security module)을 포함한다.

[0070] 예시적인 실시예(390)는 인증 기관(360)을 더 포함할 수 있다. 인증 기관(360)은 제조업체 디바이스 공개 키들을 증명하고 디바이스 공개 키들을 위한 증명서들을 생성하도록 구성된다. 실시예에서, 인증 기관(360)은 제 3자에 의해 동작된다. 대안적인 실시예들에서, 인증 기관(360)은 제조업체에 의해 제공되거나 호스팅(hosting)될 수 있다. 또한, 환경(390)은 최조 장비 제조업체(OEM) 설비(370) 및 최종-사용자 설비(380)를 포함하고, OEM 설비(370)는 적어도 하나의 디바이스를 포함하는 부품들을 최조 사용자 시스템(300) 내로 조립한다. 도 3의 구성요소들은 네트워크(380)에 의해 함께 결합될 수 있다. 네트워크(380)는 인터넷, 하나 이상의 사설 데이터 통신

네트워크들, 또는 공개 및 사설 데이터 통신 네트워크들 둘 모두의 조합과 같은 하나 이상의 공개 데이터 통신 네트워크들일 수 있다.

[0071] 도 4는 본 발명의 실시예들에 따라, 디바이스 루트 키들의 주문형 필드 생성을 위한 방법의 순서도(400)를 도시한다. 도 4는 도 3의 예시적인 동작 환경을 참조하여 설명된다. 그러나, 도 4는 그 실시예에 한정되지 않는다.

[0072] 단계(410)에서, 디바이스(310)는 DSA 또는 타원형 곡선 DSA(ECDSA : elliptical curve DSA)와 같은 알고리즘을 이용하여 디바이스 공개/사설 키 쌍을 생성한다. 논의를 용이하게 하기 위하여, DSA 키들은 여기에서 공개 키 부분에 대해 Kdi-pub 그리고 사설 키 부분에 대해 Kdi-priv라고 지칭된다. 사설 DSA 디바이스 키는 디바이스 내의 메모리에 저장된다.

[0073] 단계(420)에서, 공개 DSA 디바이스 키, Kdi-pub는 제조업체 설비(340) 내의 컴퓨터(345)로 엑스포트(export)된다. 컴퓨터(345)는 제조업체 설비(340)에서 제조된 복수의 디바이스들(310)로부터 공개 DSA 디바이스 키를 수신한다.

[0074] 단계(430)에서, 컴퓨터(345)는 하나 이상의 공개 DSA 디바이스 키들을 제조업체 키 서버(350)로 통신한다. 제조업체 키 서버(350)로 통신되는 각각의 DSA 공개 디바이스 키, Kdi-pub는 디바이스를 위한 식별자와 연관된다. 제조업체 키 서버(350)는 디바이스(310)를 위한 Kdi-pub를 저장한다. 예를 들어, Kdi-pub는 제조업체 키 관리 데이터베이스(355)에 저장될 수 있다.

[0075] 단계(440)에서, 디바이스(310)는 컴퓨터 시스템(300)으로의 통합을 위해 OEM에 제공된다. 그 다음으로, OEM은 조립된 컴퓨터 시스템을 최종 사용자(예를 들어, 최종 사용자(380))에게 제공할 수 있다.

[0076] 단계(450)에서, 디바이스 RSA 루트 키는 필드에서 주문형으로 생성된다. 시스템이 최초로 시동될 때, 또는 보안 모듈/보안 프로세서가 초기에 액세스될 때, 또는 RSA 루트 키 생성을 위한 요청이 수신될 때, 디바이스 RSA 루트 키가 생성될 수 있다. 디바이스 루트 키는 OEM 설비에서 또는 대안적으로 최종 사용자 설비에서 생성될 수 있다. 논의를 용이하게 하기 위하여, 공개/사설(public/private) 디바이스 RSA 루트 키는 (공개 키 부분에 대해) EK-pub 및 (사설 키 부분에 대해) EK-priv이라고 지칭된다.

[0077] 단계(460)에서, 디바이스(310)는 디바이스(310)의 메모리에 저장된 사설 DSA 키, Kdi-priv를 이용하여, 공개 RSA 디바이스 루트 키, EK-pub를 서명한다.

[0078] 단계(470)에서, 서명된 공개 RSA 디바이스 루트 키는 제조업체 키 서버(350)로 통신된다. 서명된 공개 디바이스 RSA 루트 키는 디바이스(310)를 식별하는 정보와 함께 통신될 수도 있다.

[0079] 단계(475)에서, 제조업체 키 서버(350)는 저장된 공개 DSA 키, Kdi-pub를 이용하여 수신된 서명을 검증한다. 서명이 검증되는 경우, 동작은 단계(480)로 진행한다.

[0080] 단계(480)에서, RSA 디바이스 루트 키의 공개 부분(EK-pub)은 증명서 서명 요청에서 디바이스 제조업체에 의해 CA(360)로 제공된다.

[0081] 단계(485)에서, 인증 기관(360)은 공개 RSA 디바이스 루트 키를 포함하는 디바이스 증명서를 생성하고, 그 증명서를 제조업체 키 서버(350)에 제공한다. 위에서 설명된 바와 같이, 증명서는 인증 기관(360)에 의해 디지털 방식으로 설명된다.

[0082] 단계(490)에서, 디바이스 증명서는 OEM 또는 최종-사용자에게 제공된다. 그 다음으로, OEM 또는 최종-사용자는 제 3 자에게 그 디바이스를 인증하기 위하여 증명서를 이용할 수 있다.

[0083] 도 4의 방법은 최종 사용자 또는 OEM이 증명서들을 위한 요청들을 행하도록 하기 위하여 디바이스 제조업체에 의해 증명서 발행 메커니즘이 수립될 것을 요청한다. 대량으로 생산되는 디바이스들에 대해서는, 이것은 설정 및 유지하기에 고가일 수 있다. 부가적으로, 최종-사용자는 증명서를 요청하고 설치하기 위하여 기술적으로 충분한 판단력을 가질 필요가 있을 것이다. 다수의 최종 사용자들은 이 교양을 결여하고 있다. 그러므로, 도 4의 방법을 위하여 추가적인 지원이 요구될 수 있다.

[0084] 도 5 및 도 6에서 설명된 실시예들은 RSA 디바이스 키들의 외부 생성과, 생성된 키들의 디바이스들 내로의 주입과 관련된다. 키 주입 장비 및 디바이스 사이의 보안이 중요하다. 이들 키 주입 실시예들에서는, 키 주입 장비와 키를 수신하는 디바이스 사이에 보안 통신이 수립될 수 있다. 부가적으로, 이들 실시예들에서, 키 주입 장비 및 디바이스의 상호 인증이 제공될 수 있다. 예를 들어, 키 주입 장비는 디바이스들을 진짜 디바이스들로서 인증할 수 있으므로, RSA 키들은 의도된 디바이스들 내로 주입되는 것이 보장된다. 또한, 디바이스들은 키 주입

장비를 인증할 수 있으므로, 이들은 신뢰된 소스(source)로부터 RSA 디바이스 키들을 수신하고 있다고 확인될 수 있다. 최종적으로, 키 주입 장비는 운영자(operator)들의 적당한 액세스 제어(물리적 및 논리적)에 의해 보안 환경에서 충분히 보호되어야 한다.

[0085] 도 5는 본 발명의 실시예들에 따라, OEM에 의한 디바이스 루트 키들의 디바이스로의 주입을 위한 방법의 순서도(500)를 도시한다. 도 5는 도 3의 예시적인 동작 환경을 참조하여 설명된다. 그러나, 도 5는 그 실시예에 한정되지 않는다. 도 5의 실시예에서, 디바이스를 위한 RSA 루트 키는 OEM에 의해 호스팅되는 보안 서버에 의해 외부에서 생성된다.

[0086] 단계(510)에서, 디바이스(310)는 Diffie Hellman(DH), 타원형 곡선 DH(ECDH : elliptical curve DH), DSA, 타원형 곡선 DSA(ECDSA : elliptical curve DSA) 또는 이와 유사한 것과 같은 알고리즘을 이용하여 키 자료(예를 들어, 공개/사설 키 쌍들)를 생성한다. 디바이스 키 자료는 디바이스(310)의 메모리 내에 저장될 수 있다.

[0087] 단계(520)에서, 예를 들어, 디바이스(310) 및 서버 사이의 Diffie Hellman 키 교환을 이용하여 공유 비밀(shared secret)이 수립된다.

[0088] 단계(530)에서, 디바이스(310)는 컴퓨터 시스템(300)으로의 통합을 위하여 OEM에 제공된다.

[0089] 단계(540)에서, RSA 디바이스 루트 키(EK-pub, EK-priv)는 OEM의 보안 서버에 의해 디바이스를 위해 생성된다.

[0090] 단계(550)에서, 보안 서버는 공유 비밀을 이용하여 생성된 대칭 키로 상기 생성된 사설 RSA 디바이스 루트 키(EK-priv)를 암호화한다.

[0091] 단계(560)에서, 암호화된 사설 RSA 디바이스 루트 키는 디바이스(310) 내로 주입된다. 위에서 설명된 바와 같이, 단계(560) 이전에, OEM의 키 주입 장비는 RSA 디바이스 키를 제공하기 전에 디바이스를 진짜 디바이스로서 인증할 수 있다. 부가적으로, 디바이스는 키 주입 장비를 인증하기 위한 능력을 포함할 수 있다.

[0092] 암호화를 통해, RSA 사설 키는 공유 비밀에 의해 보호된다. 그러므로, 암호화된 RSA 사설 키는 디바이스의 보안 모듈의 외부에 있는 메모리에 저장될 수 있다. 암호화된 사설 RSA 디바이스가 디바이스 내로 주입된 후, 보안 서버는 보안 서버로부터 RSA 키를 삭제한다.

[0093] 단계(570)에서, 공개 RSA 디바이스 루트 키는 증명서 서명 요청에서 인증 기관(360)에 통신된다. OEM은 디바이스 제조업체의 식별을 CA에 통신할 수도 있다.

[0094] 단계(580)에서, 인증 기관(360)은 공개 디바이스 RSA 루트 키 및 인증 기관의 서명을 포함하는 디바이스 공개 RSA 루트 키 증명서를 생성한다. 그 다음으로, CA는 증명서를 OEM의 보안 서버에 제공한다.

[0095] 단계(590)에서, 공개 디바이스 RSA 루트 키 증명서는 OEM에 제공되고, 다음으로, 이 OEM은 공개 디바이스 RSA 루트 키 증명서를, 디바이스를 통합하는 시스템(300)에 제공한다.

[0096] 도 6은 본 발명의 실시예들에 따라, 디바이스 루트 키들의 제조업체 주입을 위한 방법의 순서도(600)를 도시한다. 도 6은 도 3의 예시적인 동작 환경을 참조하여 설명된다. 그러나, 도 6은 그 실시예에 한정되지 않는다. 도 6의 실시예에서, RSA 키는 제조업체에 의해 호스팅되는 보안 서버에 의해 생성된다.

[0097] 단계(610)에서, 디바이스(310)는 Diffie Hellman(DH), 타원형 곡선 DH(ECDH), DSA, 타원형 곡선 DSA(ECDSA) 또는 이와 유사한 것과 같은 알고리즘을 이용하여 키 자료(예를 들어, 공개/사설 키 쌍들)를 생성한다. 디바이스 키 자료는 디바이스(310)의 메모리 내에 저장될 수 있다.

[0098] 단계(620)에서, 예를 들어, 디바이스(310) 및 서버 사이의 Diffie Hellman 키 교환을 이용하여 공유 비밀이 수립된다.

[0099] 단계(630)에서, 디바이스 RSA 루트 키(EK-pub, EK-priv)는 키 서버 설비에서 보안 서버에 의해 생성된다. 디바이스 제조업체의 보안 서버는 디바이스 제조 이전에 RSA 키들을 생성할 수 있다는 것에 주목해야 한다. 그 다음으로, 보안 서버는 생성된 RSA 디바이스 키를 디바이스에 할당할 수 있다.

[0100] 단계(640)에서, 사설 RSA 디바이스 루트 키, EK-priv는 공유 비밀로부터 생성된 대칭 키로 암호화된다.

[0101] 단계(650)에서, 인증 기관(360)은 증명서 서명 요청에서 공개 RSA 디바이스 루트 키, EK-pub를 수신한다. 그 다음으로, CA는 공개 RSA 디바이스 루트 키를 포함하는 디바이스 증명서를 생성하고, 그 증명서를 제조업체 키 서버에 제공한다. 위에서 설명된 바와 같이, 증명서는 인증 기관(360)에 의해 디지털 방식으로 서명된다.

[0102] 대안적인 실시예에서, CA에는 생성된 RSA 키들의 세트(set)가 제공된다. 이 실시예에서, 증명서들은 세트 내의 각각의 RSA 키를 위해 생성되고, 일괄로 보안 서버에 제공된다.

[0103] 단계(660)에서, 암호화된 사설 RSA 디바이스 루트 키 및 공개 디바이스 RSA 루트 키 증명서는 제조업체 설비에서 컴퓨터(345)에 통신된다. 암호화된 사설 RSA 디바이스 루트 키를 컴퓨터(345)에 통신한 후, 제조업체의 보안 서버는 사설 RSA 디바이스 루트 키를 삭제한다.

[0104] 단계(665)에서, 암호화된 사설 디바이스 RSA 루트 키 및 디바이스 RSA 루트 키 증명서는 OEM에 통신된다. 실시예들에서, 제조업체 및 OEM은 키 및 증명서 정보를 통신하기 이전에 보안 통신들을 수립한다. 당업자에 의해 인식되는 바와 같이, 통신은 SSL, TLS, 또는 IPSec와 같은 알려진 프로토콜에 따라 암호화될 수 있다. 대안적인 실시예에서, 암호화된 디바이스 RSA 루트 키 및 디바이스 RSA 루트 키 증명서는 컴퓨터(345) 대신에 디바이스 제조업체의 보안 서버(키 서버(350))에 의해 통신될 수 있다는 것에 주목해야 한다.

[0105] 단계(670)에서, 디바이스(310)는 시스템(300) 내로의 통합을 위하여 OEM에 제공된다.

[0106] 단계(680)에서, OEM은 디바이스를 위한 디바이스 RSA 루트 키 증명서 및 암호화된 사설 디바이스 RSA 루트 키를 획득한다. 그 다음으로, OEM은 사설 디바이스 RSA 루트 키를 디바이스 내로 주입하고 증명서를 설치한다.

[0107] 위에서 설명된 바와 같이, 단계(680) 이전에, OEM의 키 주입 장비는 RSA 디바이스 키를 제공하기 전에, 디바이스를 진짜 디바이스로서 인증할 수 있다. 부가적으로, 디바이스는 키 주입 장비를 인증하기 위한 능력을 포함할 수 있다.

[0108] 도 7은 본 발명의 실시예들에 따라, RSA 디바이스 키들의 시드-기반 필드내 유도를 위한 방법의 순서도(700)를 도시한다. 도 7은 도 3의 예시적인 동작 환경을 참조하여 설명된다. 그러나, 도 7은 그 실시예에 한정되지 않는다. 도 7의 방법은 디바이스 제조 프로세스에 대한 비용 충격들을 최소화하고, 보안 위험들에 덜 취약하다. 또한, 도 7의 방법은 스케일 조정이 가능하다.

[0109] 도 7의 실시예에서, 디바이스는 타겟 시스템으로 통합된 후에, 필드에서 그 RSA 키를 생성한다. RSA 키 생성의 대기시간은 최종 사용자를 관여시키는 전형적인 상호작용 프로세스이므로, 필드에서 더 많이 용인될 수 있다. 또한, 이 실시예는 시스템에서 RSA 키를 생성하므로, 타겟 시스템에서의 연관된 메모리(예를 들어, 플래시 드라이브(flash drive))의 존재로 인해 저장장치 제약들은 전형적으로 제거된다.

[0110] 단계(710)에서, 주 시드(primary seed)는 온-칩 난수 생성기(on-chip random number generator)(226)를 이용하여 디바이스(310)에 의해 생성된다. 이 주 시드는 디바이스의 1회용 프로그래밍 가능한 비휘발성 메모리(222)로 프로그래밍된다. 2048-비트 RSA 키에 대하여, 주 시드의 크기는 112-비트인, 2048-비트 RSA 키의 보안 강도보다 클 필요가 있다. 이러한 이유로, 실시예들에서는, 256-비트 주 시드가 선택된다. 주 시드를 생성하는 것은 소수(prime number)의 선택을 요구하지 않으므로, 단계(710)는 합리적인 속도로 달성될 수 있다. DSA 사설 키는 256 비트 난수일 수도 있음에 주목해야 한다. DSA 키(kdi) 생성 프로세스를 약간 수정함으로써, 생성된 무작위의 시드는 RSA 루트 키 및 DSA 키의 둘 모두를 유도하기 위하여 공통적인 주 시드로서 이용될 수 있다.

[0111] 단계(715)에서, RSA 주 시드는 디바이스의 메모리 내로 프로그래밍된다. 예를 들어, RSA 주 시드는 보안 모듈 내의 1회용 프로그래밍 가능한 비휘발성 메모리에 저장될 수 있다. 따라서, 이 방법에서는, 디바이스가 제조될 때, 주 시드가 생성되고 온-칩에서 저장된다.

[0112] 단계(720)에서, RSA 주 시드는 제조업체 설비(340)에서 컴퓨터(345)로 엑스포트된다. 컴퓨터(345)는 제조업체 설비(340)에서 제조된 복수의 디바이스들(310)로부터 RSA 주 시드들을 수신한다. 이 단계는 선택적인 것임에 주목해야 한다. 존재하지 않는 경우, 시드는 디바이스 제조업체의 보안 서버로 엑스포트된다.

[0113] 단계(730)에서, 컴퓨터(345)는 RSA 주 시드를 제조업체의 공개 키(KM-pub)로 암호화하고, 암호화된 RSA 주 시드를 제조업체 내의 보안 서버로 엑스포트한다. 제조업체의 공개 키는 RSA 공개 키, DSA 공개 키, DH 공개 키, EC DSA 공개 키, 또는 EC DH 공개 키일 수 있다. 당업자에 의해 인식되는 바와 같이, 공개 제조업체 키의 다른 형태들은 본 발명과 함께 이용될 수 있다. 대응하는 사설 키는 제조업체의 보안 서버(예를 들어, 하드웨어 보안 모듈)에 의해 유지된다. 사설 제조업체 사설 키는 전형적으로 제조업체에 의해 비허가된 액세스(unauthorized access)로부터 물리적으로 그리고 논리적으로 안전하게 될 것이다.

[0114] 단계(740)에서, 제조업체 키 서버 설비 내의 보안 서버는 제조업체의 사설 키를 이용하여 RSA 주 시드를 복호화한다.

[0115] 단계(750)에서, 제조업체의 보안 서버는 RSA 공개/사설 루트 키 쌍을 생성하기 위하여 RSA 주 시드를 이용한다. 이 단계에서, 주 시드는 RSA 루트 키를 유도하기 위하여 알고리즘으로 공급된다. 이 단계는 소수 선택의 요건으로 인해 긴 연산을 요구한다. 상기 알고리즘은 일단 주 시드가 고정되고 고유하다면, 유도된 RSA 루트 키도 고유하다는 것을 보장한다. RSA 키 쌍의 생성 후에, 보안 서버는 보안 서버로부터 사설 RSA 키를 삭제한다.

[0116] 실시예들에서, RSA 주 시드가 생성되고 엑스포트된 후, 디바이스 루트 키의 일련 번호(sequence number) 및 명칭은 제조업체에 의해 생성될 수도 있다. 일련 번호 및/또는 명칭은 제조업체의 컴퓨터(345) 및/또는 보안 서버에 의해 생성될 수 있다. 일련 번호는 디바이스에 고유할 수 있고, 디바이스의 메모리 내로 프로그래밍될 수 있다. RSA 디바이스 루트 키 명칭은 디바이스 개정 번호(device revision number), 일련 번호, 및 주 시드와 같은 다수의 연결된 필드들을 암호 방식으로 해싱함으로써 생성될 수 있다. 당업자에 의해 인식되는 바와 같이, 키 명칭을 생성하기 위한 다른 기술들은 본 발명의 실시예들에서 이용될 수 있다. 일련 번호, 루트 키 명칭, 및 생성된 RSA 공개 키는 제조업체의 데이터베이스에 저장된다.

[0117] 단계(760)에서, 인증 기관(CA)(260)은 제조업체의 보안 서버로부터, 공개 RSA 디바이스 루트 키, EK-pub를 포함하는 제조업체로부터의 증명서 서명 요청을 수신한다. 그 다음으로, CA는 공개 RSA 디바이스 루트 키를 포함하는 RSA 공개 디바이스 루트 키 증명서를 생성하고, RSA 공개 디바이스 루트 키 증명서를 제조업체에게 제공한다. 증명서 서명 요청은 일련 번호 및 루트 키 명칭을 포함할 수도 있다. 이들이 CA(360)에 제공되는 경우, CA(360)는 발행된 증명서 내에 이 정보를 포함한다. 위에서 설명된 바와 같이, 증명서는 CA(360)에 의해 디지털 방식으로 서명된다.

[0118] 단계(770)에서, 제조업체의 보안 서버는 공개 RSA 루트 키 증명서를 컴퓨터(345)에 제공한다.

[0119] 단계(780)에서, 컴퓨터(345)는 공개 RSA 루트 키 증명서를 디바이스를 통합하는 최종 사용자 시스템(300)에 분배한다. 단계(780)는 선택적인 것임에 주목해야 한다. 실시예들에서, 제조업체의 보안 서버(또는 제조업체의 또 다른 플랫폼(platform))는 공개 RSA 키 증명서를, 디바이스를 통합하는 최종 사용자 시스템(300)에 분배하는 단계를 수행할 수 있다. 또한, 실시예들에서, 디바이스 제조업체는 이 정보를 OEM에 제공할 수 있고, 다음으로, OEM은 그 정보를 최종 사용자 시스템에 제공한다.

[0120] 단계(785)에서, 디바이스 공개 RSA 루트 키 증명서는 최종 사용자 시스템(300)으로 로딩되고 검증된다. 검증이 성공적인 경우, 동작은 단계(790)로 진행한다. 검증이 성공적이지 않은 경우, 최종 사용자 시스템(300)은 OEM 또는 디바이스 제조업체에 통지하고 새로운 증명서를 요청한다.

[0121] 단계(790)에서, 최종 사용자 시스템(300) 내의 디바이스(310)는 조건의 발생 후에 RSA 공개/사설 루트 키 쌍을 생성한다. 예를 들어, 디바이스 RSA 루트 키 쌍은 RSA 루트 키를 생성하기 위한 요청 또는 명령의 수신 후에 생성될 수 있다. 대안적으로, 디바이스 RSA 루트 키는 시스템의 초기 시동 후에, 또는 보안 모듈 또는 보안 프로세서가 처음에 액세스될 때에 생성될 수 있다.

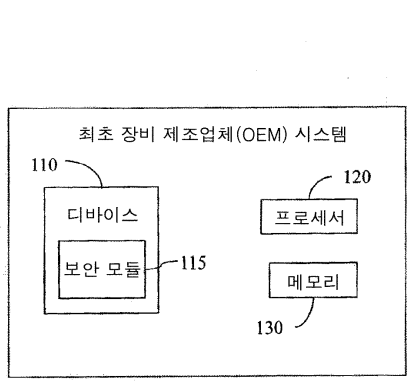
[0122] 이 단계에서, 저장된 주 시드는 RSA 루트 키를 유도하기 위하여 알고리즘으로 공급된다. 이 단계는 소수 선택의 요건으로 인해 긴 연산을 요구한다. 따라서, 그것은 디바이스가 배치된 후에 필드에서 수행된다. 알고리즘은 일단 주 시드가 고정되고 고유하다면, 유도된 RSA 루트 키도 고유하다는 것을 보장한다. 또한, 이 단계는 필드 내에서 수행되므로, RSA 루트 키(전체 루트 키 또는 사설 RSA 루트 키)는 디바이스에 의해 암호 방식으로 포장(예를 들어, 암호화)될 수 있고, 임의의 소프트웨어 개입 없이 부착된 플래시 디바이스 내에 투명하게 저장될 수 있다.

[0123] 발명의 상기 설명된 실시예들은 하드웨어, 펌웨어, 소프트웨어, 또는 그 임의의 조합으로 구현될 수 있다는 것을 인식할 것이다. 발명의 실시예들은 하나 이상의 프로세서들에 의해 판독 및 실행될 수 있는 기계-판독가능 매체(machine-readable medium) 상에 저장된 명령들로서 구현될 수도 있다. 기계-판독가능 매체는 기계(예를 들어, 컴퓨팅 디바이스)에 의해 판독가능한 형태로 정보를 저장하거나 송신하기 위한 임의의 메커니즘을 포함할 수 있다. 예를 들어, 기계-판독가능 매체는 판독전용 메모리(ROM : read only memory); 랜덤 액세스 메모리(RAM); 자기 디스크 저장 매체; 광학적 저장 매체; 플래시 메모리 디바이스들; 전기, 광, 음향 또는 다른 형태들의 전파되는 신호들을 포함할 수 있다.

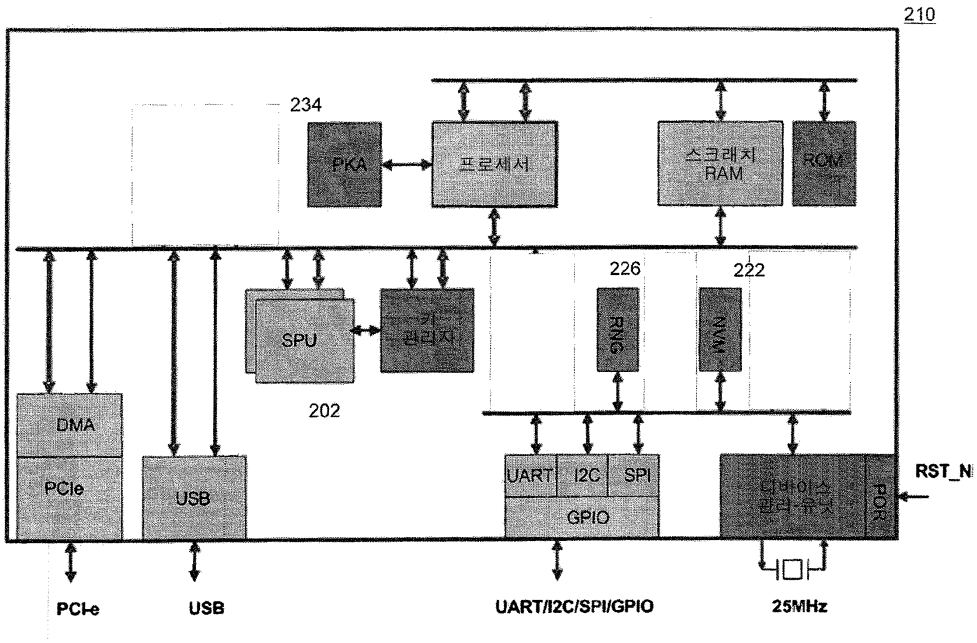
[0124] 본 발명은 특정된 기능들 및 그 관계들의 구현을 예시하는 기능적 구성 블록들의 도움으로 위에서 설명되었다. 이 기능적 구성 블록들의 경계들은 설명의 편의를 위하여 여기에서 임의로 정의되었다. 특정된 기능들 및 그 관계들이 적절하게 수행되기만 하면, 대안적인 경계들이 정의될 수 있다.

도면

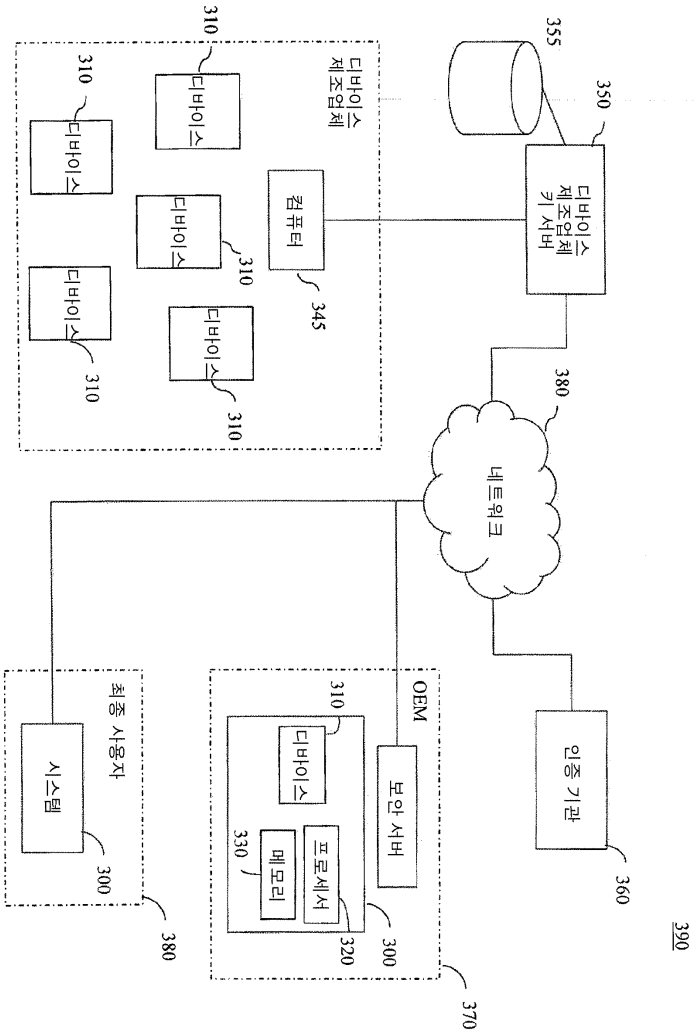
도면1


100
최초 장비 제조업체(OEM) 시스템
110
디바이스
보안 모듈
115
120
프로세서
메모리
130

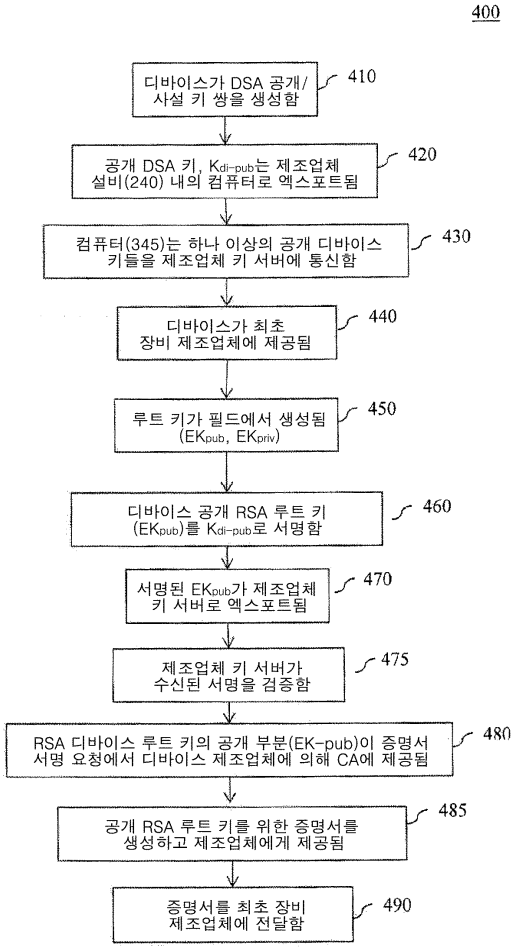
도면2


210
234
PKA
프로세서
스크래치 RAM
ROM
226
222
SPU
202
RNG
NVM
DMA
PCIe
USB
UART
I2C
SPI
GPIO
RST_N
POR
PCIe
USB
UART/I2C/SPI/GPIO
25MHz

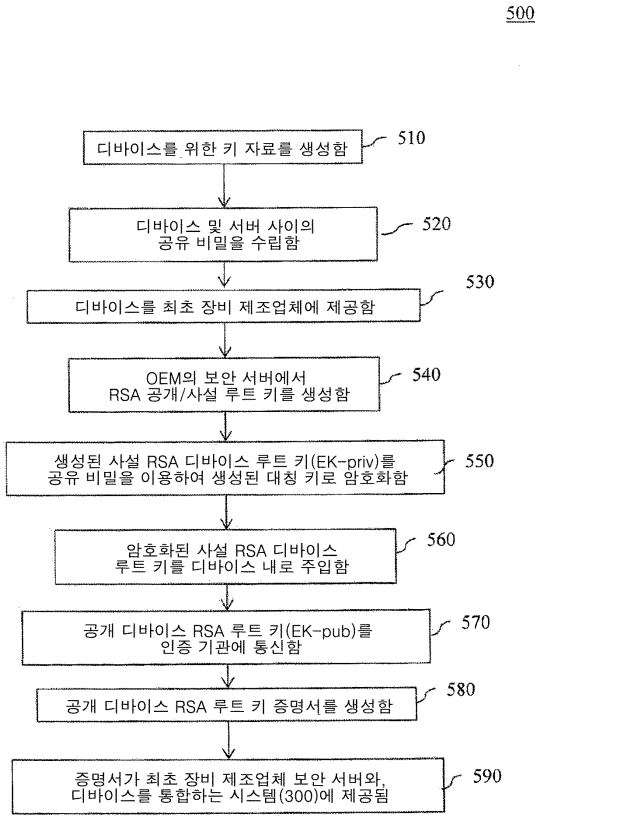
도면3


310
디바이스
310
디바이스
디바이스 제조업체
310
디바이스
310
디바이스
310
디바이스
컴퓨터
345
355
350
디바이스 제조업체 키 서버
380
네트워크
최종 사용자
시스템
300
380
OEM
310
디바이스
330
메모리
프로세서
320
300
보안 서버
370
인증 기관
360
390

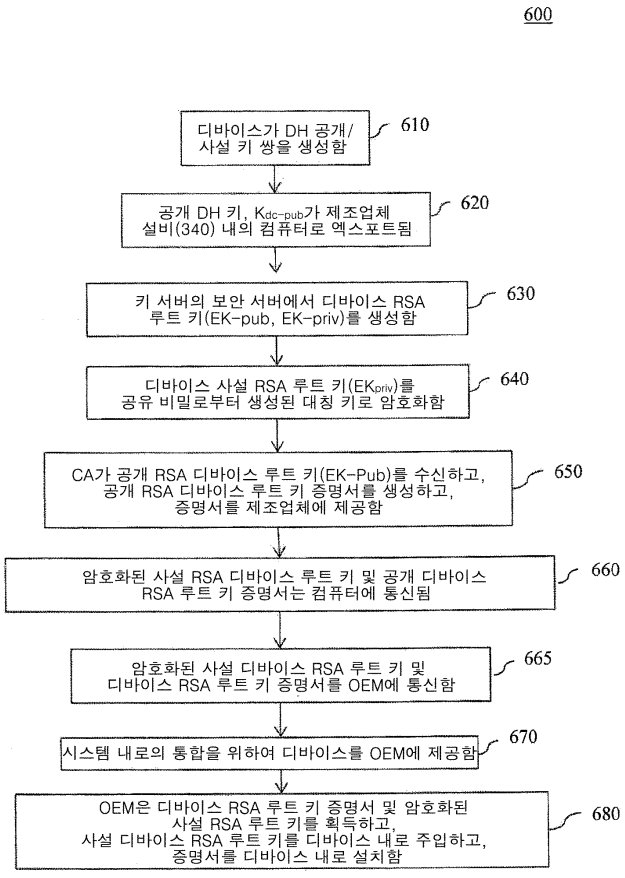
도면4


400
디바이스가 DSA 공개/사설 키 쌍을 생성함
410
공개 DSA 키, K_{di-pub}는 제조업체 설비(240) 내의 컴퓨터로 엑스포트됨
420
컴퓨터(345)는 하나 이상의 공개 디바이스 키들을 제조업체 키 서버에 통신함
430
디바이스가 최초 장비 제조업체에 제공됨
440
루트 키가 필드에서 생성됨 (EK_{pub}, EK_{priv})
450
디바이스 공개 RSA 루트 키 (EK_{pub})를 K_{di-pub}로 서명함
460
서명된 EK_{pub}가 제조업체 키 서버로 엑스포트됨
470
제조업체 키 서버가 수신된 서명을 검증함
475
RSA 디바이스 루트 키의 공개 부분(EK-pub)이 증명서 서명 요청에서 디바이스 제조업체에 의해 CA에 제공됨
480
공개 RSA 루트 키를 위한 증명서를 생성하고 제조업체에게 제공됨
485
증명서를 최초 장비 제조업체에 전달함
490

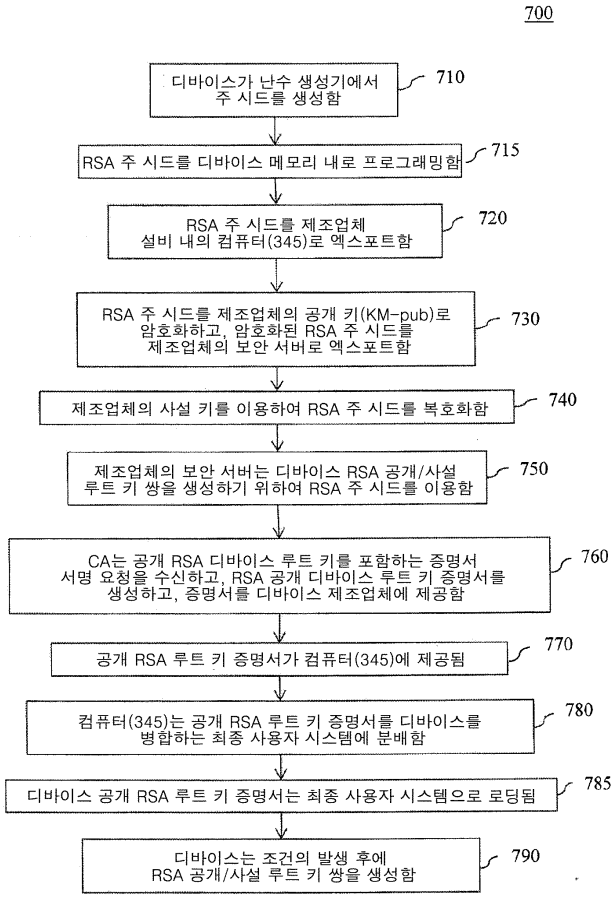
도면5


500
디바이스를 위한 키 자료를 생성함
510
디바이스 및 서버 사이의 공유 비밀을 수립함
520
디바이스를 최초 장비 제조업체에 제공함
530
OEM의 보안 서버에서 RSA 공개/사설 루트 키를 생성함
540
생성된 사설 RSA 디바이스 루트 키(EK-priv)를 공유 비밀을 이용하여 생성된 대칭 키로 암호화함
550
암호화된 사설 RSA 디바이스 루트 키를 디바이스 내로 주입함
560
공개 디바이스 RSA 루트 키(EK-pub)를 인증 기관에 통신함
570
공개 디바이스 RSA 루트 키 증명서를 생성함
580
증명서가 최초 장비 제조업체 보안 서버와, 디바이스를 통합하는 시스템(300)에 제공됨
590

도면6


600
디바이스가 DH 공개/사설 키 쌍을 생성함
610
공개 DH 키, Kdc-pub가 제조업체 설비(340) 내의 컴퓨터로 엑스포트됨
620
키 서버의 보안 서버에서 디바이스 RSA 루트 키(EK-pub, EK-priv)를 생성함
630
디바이스 사설 RSA 루트 키(EKpriv)를 공유 비밀로부터 생성된 대칭 키로 암호화함
640
CA가 공개 RSA 디바이스 루트 키(EK-Pub)를 수신하고, 공개 RSA 디바이스 루트 키 증명서를 생성하고, 증명서를 제조업체에 제공함
650
암호화된 사설 RSA 디바이스 루트 키 및 공개 디바이스 RSA 루트 키 증명서는 컴퓨터에 통신됨
660
암호화된 사설 디바이스 RSA 루트 키 및 디바이스 RSA 루트 키 증명서를 OEM에 통신함
665
시스템 내로의 통합을 위하여 디바이스를 OEM에 제공함
670
OEM은 디바이스 RSA 루트 키 증명서 및 암호화된 사설 RSA 루트 키를 획득하고, 사설 디바이스 RSA 루트 키를 디바이스 내로 주입하고, 증명서를 디바이스 내로 설치함
680

도면7


700
디바이스가 난수 생성기에서 주 시드를 생성함
710
RSA 주 시드를 디바이스 메모리 내로 프로그래밍함
715
RSA 주 시드를 제조업체 설비 내의 컴퓨터(345)로 엑스포트함
720
RSA 주 시드를 제조업체의 공개 키(KM-pub)로 암호화하고, 암호화된 RSA 주 시드를 제조업체의 보안 서버로 엑스포트함
730
제조업체의 사설 키를 이용하여 RSA 주 시드를 복호화함
740
제조업체의 보안 서버는 디바이스 RSA 공개/사설 루트 키 쌍을 생성하기 위하여 RSA 주 시드를 이용함
750
CA는 공개 RSA 디바이스 루트 키를 포함하는 증명서 서명 요청을 수신하고, RSA 공개 디바이스 루트 키 증명서를 생성하고, 증명서를 디바이스 제조업체에 제공함
760
공개 RSA 루트 키 증명서가 컴퓨터(345)에 제공됨
770
컴퓨터(345)는 공개 RSA 루트 키 증명서를 디바이스를 병합하는 최종 사용자 시스템에 분배함
780
디바이스 공개 RSA 루트 키 증명서는 최종 사용자 시스템으로 로딩됨
785
디바이스는 조건의 발생 후에 RSA 공개/사설 루트 키 쌍을 생성함
790