(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월29일
(11) 등록번호 10-2233356
(24) 등록일자 2021년03월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/53 (2013.01) *G06F 21/57* (2013.01)
G06F 21/62 (2013.01) *H04W 12/08* (2021.01)
H04W 4/00 (2018.01) *H04W 88/06* (2009.01)
(52) CPC특허분류
G06F 21/53 (2013.01)
G06F 21/575 (2013.01)
(21) 출원번호 10-2016-7009199
(22) 출원일자(국제) 2014년07월01일
심사청구일자 2019년06월27일
(85) 번역문제출일자 2016년04월07일
(65) 공개번호 10-2016-0054556
(43) 공개일자 2016년05월16일
(86) 국제출원번호 PCT/US2014/045042
(87) 국제공개번호 WO 2015/038221
국제공개일자 2015년03월19일
(30) 우선권주장
14/025,608 2013년09월12일 미국(US)
(56) 선행기술조사문헌
KR1020090087865 A*
KR1020110049230 A*
US20100023743 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
더 보잉 컴파니
미국, 일리노이스 60606, 시카고, 100 노스 리버사이드 플라자
(72) 발명자
슈테른, 알론 제이.
미국 22153 버지니아 스프링필드 보스톤 블러바드 7700 메일 코드: 7920-1001
(74) 대리인
특허법인 남앤남

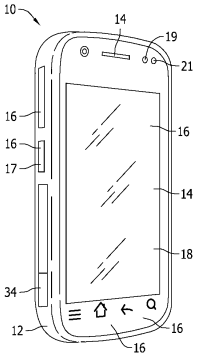
전체 청구항 수 : 총 15 항 심사관 : 정성훈

(54) 발명의 명칭 **모바일 통신 디바이스 및 그 작동 방법**

(57) 요 약

모바일 통신 디바이스가 제공된다. 모바일 통신 디바이스는 하우징 그리고 하우징과 동작 가능한 입력 디바이스를 포함한다. 입력 디바이스를 작동시키는 것은 사용자가 모바일 통신 디바이스의 동작 상태를 변경하는 것과 검증하는 것 중 적어도 하나를 할 수 있게 한다. 모바일 통신 디바이스는 상기 입력 디바이스와 연결되어 통신하며 모바일 통신 디바이스의 동작 상태를 기초로 사용자에게 피드백을 제공하도록 구성되는 표시자를 또한 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/6218 (2013.01)
H04W 12/08 (2021.01)
H04W 4/50 (2018.02)
H04W 88/06 (2013.01)

명 세 서

청구범위

청구항 1

복수의 동작 상태들을 갖는 모바일 통신 디바이스로서,

하우징;

프로세서;

상기 하우징에 연결된 단일 하드웨어 버튼; 및

상기 단일 하드웨어 버튼과 연결되어 통신하는 표시자를 포함하고,

상기 프로세서는,

제 1 가상화 운영 시스템 및 제 1 신뢰할 수 있는 실행 환경을 포함하는 제 1 페르소나를 실행하고 - 제 1 신뢰할 수 있는 실행 환경은 제 1 하드웨어 신뢰 앵커 및 제 1 가입자 식별 모듈 카드에 직접 접근함 -;

제 2 가상화 운영 시스템 및 제 2 신뢰할 수 있는 실행 환경을 포함하는 제 2 페르소나를 실행하고 - 제 2 신뢰할 수 있는 실행 환경은 제 1 하드웨어 신뢰 앵커와 상이한 제 2 하드웨어 신뢰 앵커 및 제 1 가입자 식별 모듈 카드와 상이한 제 2 가입자 식별 모듈 카드에 직접 접근함 -; 그리고

상기 모바일 통신 디바이스의 포커스를 상기 제 1 페르소나 및 상기 제 2 페르소나 중 하나와 연관시키도록 구성되고 - 연관된 페르소나는 활성 페르소나이고, 사용자는 상기 모바일 통신 디바이스 상에서 상기 활성 페르소나와 상호 작용할 수 있고 연관된 가입자 식별 모듈 카드를 통하여 통신할 수 있음 -,

상기 단일 하드웨어 버튼은 상기 제 1 페르소나와 상기 제 2 페르소나 사이에서 상기 모바일 통신 디바이스의 포커스를 트랜지션(transition)하도록 구성되고,

상기 표시자는 상기 모바일 통신 디바이스의 포커스를 기초로 상기 사용자에게 지속적인 피드백을 제공하도록 구성되는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 2

제 1 항에 있어서,

상기 제 1 가상화 운영 시스템 및 상기 제 2 가상화 운영 시스템은 상기 모바일 통신 디바이스에 의하여 실행되는 제 3 운영 시스템과 연결되어 통신하고, 상기 제 3 운영 시스템은 보안 정책들을 저장 및 실행하는 보안 수퍼바이저인,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 3

제 1 항에 있어서,

상기 단일 하드웨어 버튼을 작동시키는 것은, 상기 프로세서로 하여금 상기 모바일 통신 디바이스가 신뢰할 수 있는 상태임을 확인하기 위한 신뢰 루트 정보를 디스플레이하도록 하는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 4

제 3 항에 있어서,

상기 신뢰 루트 정보는 상기 모바일 통신 디바이스 및 상기 모바일 통신 디바이스 상에서 작동하는 페르소나 중 적어도 하나에 대한 신뢰 루트 정보를 포함하는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 5

제 1 항에 있어서,

상기 표시자는 상기 하우징에 연결된 제 1 LED 표시자 및 제 2 LED 표시자를 더 포함하고, 상기 제 1 LED 표시자는 상기 제 1 페르소나에 포커스가 맞춰지면 활성화되도록 구성되고, 상기 제 2 LED 표시자는 상기 제 2 페르소나에 포커스가 맞춰지면 활성화되도록 구성되는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 6

제 1 항에 있어서,

인증되지 않은 하드웨어 가속 암호 기법을 가능하게 하는 제 1 신뢰할 수 있는 플랫폼 모듈을 더 포함하는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 7

제 1 항에 있어서,

상기 제 1 신뢰할 수 있는 실행 환경은 상기 제 1 가상화 운영 시스템을 평문 키에 노출시키지 않으면서 상기 제 1 가상화 운영 시스템 대신 암호화 서비스들에 접근하는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 8

제 1 항에 있어서,

상기 제 1 하드웨어 신뢰 앵커는 암호화 인증서를 사용하여 디지털 자산들에 서명하는 신뢰할 수 있는 플랫폼 모듈을 포함하는,

복수의 동작 상태들을 갖는 모바일 통신 디바이스.

청구항 9

복수의 동작 상태들을 가지며 하우징 및 상기 하우징에 연결된 단일 하드웨어 버튼을 포함하는 모바일 통신 디바이스를 작동시키는 방법으로서,

제 1 가상화 운영 시스템 및 제 1 신뢰할 수 있는 실행 환경을 포함하는 제 1 페르소나를 실행하는 단계 – 제 1 신뢰할 수 있는 실행 환경은 제 1 하드웨어 신뢰 앵커 및 제 1 가입자 식별 모듈 카드에 직접 접근함 –;

제 2 가상화 운영 시스템 및 제 2 신뢰할 수 있는 실행 환경을 포함하는 제 2 페르소나를 실행하는 단계 – 제 2 신뢰할 수 있는 실행 환경은 제 1 하드웨어 신뢰 앵커와 상이한 제 2 하드웨어 신뢰 앵커 및 제 1 가입자 식별 모듈 카드와 상이한 제 2 가입자 식별 모듈 카드에 직접 접근함 –;

상기 모바일 통신 디바이스의 포커스를 상기 제 1 페르소나 및 상기 제 2 페르소나 중 하나와 연관시키는 단계 – 연관된 페르소나는 활성 페르소나이고, 사용자는 상기 모바일 통신 디바이스 상에서 상기 활성 페르소나와 상호 작용할 수 있고 연관된 가입자 식별 모듈 카드를 통하여 통신할 수 있음 –;

사용자에 의한 상기 단일 하드웨어 버튼의 작동 표시를 수신하는 단계;

상기 제 1 페르소나와 상기 제 2 페르소나 사이에서 상기 포커스를 트랜지션하는 단계; 및

상기 모바일 통신 디바이스에 의해, 시각적 표시자를 통하여 상기 모바일 통신 디바이스의 포커스를 나타내는 지속적인 피드백을 제공하는 단계를 포함하는,

모바일 통신 디바이스를 작동시키는 방법.

청구항 10

제 9 항에 있어서,

상기 제 1 가상화 운영 시스템 및 상기 제 2 가상화 운영 시스템과 연결되어 통신하는 제 3 운영 시스템을 실행하는 단계를 더 포함하고,

상기 제 3 운영 시스템은 보안 정책들을 저장 및 실행하는 보안 수퍼바이저인,

모바일 통신 디바이스를 작동시키는 방법.

청구항 11

제 9 항에 있어서,

상기 작동 표시의 수신시 상기 모바일 통신 디바이스에 대해 사용자의 물리적 존재를 증명하는 단계를 더 포함하는,

모바일 통신 디바이스를 작동시키는 방법.

청구항 12

제 9 항에 있어서,

사용자에게 피드백을 제공하는 단계는, 제 1 페르소나에 포커스가 맞춰지면 제 1 시각적 LED 표시자를 활성화하고, 제 2 페르소나에 포커스가 맞춰지면 제 2 시각적 LED 표시자를 활성화하는 단계를 포함하는,

모바일 통신 디바이스를 작동시키는 방법.

청구항 13

제 9 항에 있어서,

상기 모바일 통신 디바이스에 크리덴셜들을 입력하도록 사용자에게 요청하는 단계 – 상기 작동 표시는 사용자에게 프롬프트(prompt)한 후 수신됨 –; 및

상기 작동 표시의 수신시 신뢰 루트 정보를 디스플레이하는 단계를 더 포함하는,

모바일 통신 디바이스를 작동시키는 방법.

청구항 14

제 9 항에 있어서,

상기 모바일 통신 디바이스에 크리덴셜들을 입력하도록 사용자에게 요청하는 단계 – 상기 작동 표시는 사용자에게 프롬프트한 후 수신됨 –; 및

상기 작동 표시의 수신시 적어도 하나의 시각적 LED 표시자를 미리 결정된 구성으로 활성화하는 단계를 더 포함하는,

모바일 통신 디바이스를 작동시키는 방법.

청구항 15

제 9 항에 있어서,

상기 단일 하드웨어 버튼 및 상기 시각적 표시자는, 상기 모바일 통신 디바이스 상에서 작동하는 신뢰할 수 없는 코드로부터 상기 단일 하드웨어 버튼 및 상기 시각적 표시자가 접근 불가능하도록 하드웨어가 격리되는,

모바일 통신 디바이스를 작동시키는 방법.

발명의 설명

기 술 분 야

[0001] [1] 본 개시의 분야는 일반적으로 모바일 통신 디바이스들에 관한 것으로, 보다 구체적으로는 모바일 통신 디바이스 상에서 작동하는 하나 또는 그보다 많은 격리된 가상화 운영 시스템들의 신뢰할 수 있는 동작을 가능

하게 하는 모바일 통신 디바이스에 관한 것이다.

배 경 기 술

[0002] [2] 스마트폰들, 셀룰러폰들 및 개인용 디지털 보조기기(PDA: personal digital assistant)들과 같은 모바일 통신 디바이스들은 다양한 서로 다른 타입들의 사용자들 사이에서 사용 및 인기가 증가해 왔다. 적어도 일부 알려진 디바이스들은 하나의 디바이스 상에서 다수의 운영 시스템(OS: operating system)들을 동시에 실행하도록 가상화될 수 있는 중앙 처리 유닛(CPU: central processing unit)을 포함한다. 예를 들어, 하이퍼바이저로서 알려진 소프트웨어 프로그램이 컴퓨터 시스템에 포함된 하드웨어 디바이스들과 OS들 사이에 송신되는 입력/출력(I/O: input/output) 접근 동작들을 관리함으로써 서로 다른 OS들을 구별하는 데 사용될 수 있다. 보다 구체적으로, 하이퍼바이저는 CPU 및 연관된 주변 장치들(예를 들어, 디스플레이 디바이스들, 터치 스크린들 및 통신 인터페이스들)과 같은 기본 하드웨어를 하드웨어 상에서 작동하는 OS들과 구별하는 것을 가능하게 한다.

[0003] [3] 디바이스 가상화는 알려진 컴퓨팅 디바이스들 상에서 한 세트의 소프트웨어를 다른 세트의 소프트웨어와 구별하는 것을 가능하게 할 수도 있지만, 기본 플랫폼이 다양한 보안 취약성들에 영향을 받기 쉬울 수도 있다. 이 때문에, 알려진 컴퓨팅 디바이스들의 보안을 강화하는 것이 컴퓨터 산업의 당업자들에게 점점 더 중요해져 왔다. 이에 따라, 디바이스 가상화 아키텍처에 강화된 보안을 포함시키는 것이 바람직할 수도 있다.

발명의 내용

[0004] [4] 한 양상에서, 모바일 통신 디바이스가 제공된다. 모바일 통신 디바이스는 복수의 동작 상태들을 가지며 하우징 그리고 하우징에 연결된 입력 디바이스를 포함한다. 입력 디바이스를 작동시키는 것은 사용자가 모바일 통신 디바이스의 동작 상태를 변경하는 것과 검증하는 것 중 적어도 하나를 할 수 있게 한다. 모바일 통신 디바이스는 상기 입력 디바이스와 연결되어 통신하며 모바일 통신 디바이스의 동작 상태를 기초로 사용자에게 피드백을 제공하도록 구성되는 표시자를 또한 포함한다.

[0005] [5] 다른 양상에서, 복수의 동작 상태들을 가지며 하우징 그리고 하우징에 연결된 입력 디바이스를 포함하는 모바일 통신 디바이스를 작동시키는 방법이 제공된다. 이 방법은 사용자에 의한 입력 디바이스의 작동 표시를 수신하는 단계, 작동 표시의 수신시 모바일 통신 디바이스의 동작 상태를 변경하는 것과 검증하는 것 중 적어도 하나를 하는 단계, 및 모바일 통신 디바이스에 의해 모바일 통신 디바이스의 동작 상태를 표시하는 피드백을 제공하는 단계를 포함한다.

[0006] [6] 또 다른 양상에서, 모바일 통신 디바이스를 작동시키기 위한 컴퓨터 실행 가능 명령들을 저장하는 비-일시적 컴퓨터 판독 가능 매체가 제공된다. 모바일 통신 디바이스는 복수의 동작 상태들을 가지며 하우징 그리고 하우징에 연결된 입력 디바이스를 포함한다. 컴퓨터 실행 가능 명령들은 프로세서로 하여금, 입력 디바이스가 작동될 때 모바일 통신 디바이스의 동작 상태를 변경하는 것과 검증하는 것 중 적어도 하나를 하게 하고 그리고 모바일 통신 디바이스의 동작 상태를 기초로 사용자에게 피드백을 제공하도록 표시자를 활성화하게 한다.

도면의 간단한 설명

[0007] [7] 도 1은 예시적인 모바일 통신 디바이스의 정면 사시도이다.

[8] 도 2는 도 1에 도시된 모바일 통신 디바이스의 뒷면 사시도이다.

[9] 도 3은 도 1에 도시된 모바일 통신 디바이스에 사용될 수 있는 예시적인 하드웨어 아키텍처의 개략도이다.

[10] 도 4는 도 1에 도시된 모바일 통신 디바이스에 사용될 수 있는 예시적인 소프트웨어 아키텍처의 개략도이다.

[11] 도 5는 도 1에 도시된 모바일 통신 디바이스에 사용될 수 있는 페르소나의 소유권을 주장하는 예시적인 방법의 흐름도이다.

[12] 도 6은 도 1에 도시된 모바일 통신 디바이스 상에서 수행될 동작을 인가하는 데 사용하기 위한 예시적인 시스템의 개략도이다.

[13] 도 7은 도 1에 도시된 모바일 통신 디바이스에 사용될 수 있는 페르소나 소프트웨어를 업데이트하는 예시적인 방법의 흐름도이다.

[14] 도 8은 도 1에 도시된 모바일 통신 디바이스에 사용될 수 있는 페르소나의 소유권을 트랜지션하는 예시적인 방법의 흐름도이다.

[15] 도 9는 도 1에 도시된 모바일 통신 디바이스에 사용될 수 있는 새로운 페르소나를 로딩하는 예시적인 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0008] [16] 본 명세서에서 설명되는 시스템들 및 방법들은 모바일 통신 디바이스를 작동시키는 데 사용될 수 있다. 예시적인 구현에서, 모바일 통신 디바이스는 이 디바이스 상에서 작동하는 운영 시스템들을 안전하게 하는 것을 가능하게 하기 위해 공개 및 개인 키들을 기반으로 하는 암호 기법과 같은 암호 기법을 사용하는 하드웨어 및 소프트웨어 아키텍처에 의해 관리된다. 보다 구체적으로, 모바일 통신 디바이스는 디바이스 상에서 동시에 작동하며 각각이 개별 신뢰 루트들을 갖는 다수의 가상화 운영 시스템들을 지원한다. 이에 따라, 디바이스 상의 하드웨어에 대한 가상화 운영 시스템들의 접근은 디바이스의 신뢰할 수 있는 동작을 가능하게 하도록 미리 결정된 보안 정책들에 의해 시행된다.

[0009] [17] 도 1과 도 2는 예시적 모바일 통신 디바이스(10)를 나타낸다. 예시적인 구현에서, 모바일 통신 디바이스(10)는 다른 모바일 통신 디바이스와 같은 다른 디바이스와의 음성 통신을 지원하기 위해 제공된다. 더욱이, 모바일 통신 디바이스(10)는 네트워크 액세스, SMS 메시징, 하나 또는 그보다 많은 애플리케이션들의 호스팅, 데이터 처리, 암호화 및/또는 다른 기능들을 비롯한 다양한 다른 기능들을 포함할 수도 있다. 모바일 통신 디바이스(10)는 하나 또는 그보다 많은 셀룰러 네트워크들을 통해 통신하도록 구성된 스마트폰일 수도 있다. 대안적인 구현에서, 모바일 통신 디바이스(10)는 WiFi 및/또는 위성 네트워크와 같은 비-셀룰러 네트워크 상에서 배타적으로 작동할 수도 있다.

[0010] [18] 도시된 바와 같이, 모바일 통신 디바이스(10)는 하우징(12) 그리고 하우징(12) 내에 적어도 부분적으로 배치된 다수의 표현 디바이스들(14)을 포함한다. 표현 디바이스(14)는 모바일 통신 디바이스(10)의 동작과 관련된 데이터, 커맨드들, 요청된 데이터, 메시지들, (가상 키보드와 같은) 하나 또는 그보다 많은 입력 디바이스들, 및/또는 임의의 다른 타입의 데이터와 같은, 그러나 이에 한정된 것은 아닌 정보를 사용자에게 출력한다. 여러 예들에서, 표현 디바이스(14)는 예를 들어, 액정 디스플레이(LCD: liquid crystal display), 발광 다이오드(LED: light-emitting diode) 디스플레이, 발광 다이오드(LED), 카메라 플래시, 유기 LED(OLED: organic LED) 디스플레이 및/또는 "전자 잉크" 디스플레이를 포함할 수 있다. 일부 구현들에서는, 사용자에게 데이터를 시각적으로 그리고/또는 청각적으로 제시하기 위해 다수의 표현 디바이스들(14)이 포함될 수도 있다. 예시적인 구현에서, 표현 디바이스(14)는 음성 통신에서 사용할 오디오 출력을 포함한다.

[0011] [19] 모바일 통신 디바이스(10)는 하우징(12) 내에 적어도 부분적으로 배치된 다수의 입력 디바이스들(16)을 더 포함한다. 각각의 입력 디바이스(16)는 본 명세서에서 설명되는 방법들 및/또는 프로세스들 중 하나 이상에 따라, 선택들, 요청들, 커맨드들, 정보, 데이터 및/또는 임의의 다른 타입의 입력들을 수신하도록 구성될 수도 있다. 입력 디바이스들(16)은 예를 들어, 버튼들, 키보드, 마이크로폰, 바이브(vibe), 포인팅 디바이스, 스타일러스, 터치 감지 패널(예를 들어, 터치 패드 또는 터치 스크린), 자이로스코프, 가속도계, 디지털 나침반, 포지션 검출기, 카메라, 제2 카메라, 주변광 센서 및/또는 오디오 입력 인터페이스를 포함할 수 있다. 예시적인 구현에서는, 터치 스크린(18)과 같은 단일 컴포넌트가 표현 디바이스(14)와 입력 디바이스(16) 둘 다로서 기능을 한다.

[0012] [20] 한 구현에서, 모바일 통신 디바이스(10)는 모바일 통신 디바이스(10)의 보안 동작을 가능하게 하는 보안 특징들을 포함한다. 모바일 통신 디바이스(10)는 입력 디바이스(16)와 연결되어 통신하며 모바일 통신 디바이스의 동작 상태를 기초로 사용자에게 피드백을 제공하도록 구성되는 표시자를 포함할 수도 있다. 보안 특징들은 보안 버튼(17)과 같은 입력 디바이스(16) 및 복수의 LED들과 같은 표현 디바이스(14)를 포함한다. 보다 구체적으로, 모바일 통신 디바이스(10)는 제 1 LED(19) 및 제 2 LED(21)를 포함한다. 아래 더 상세히 설명되는 바와 같이, 보안 특징들은 모바일 통신 디바이스(10)의 신뢰할 수 있는 동작 상태를 변경 및/또는 검증하는 데 사용될 수도 있다. 대안적인 구현에서, 모바일 통신 디바이스(10)는 보안 특징들이 본 명세서에서 설명되는 바와 같이 기능할 수 있게 하는 임의의 타입 및/또는 임의의 개수의 표현 디바이스들을 포함할 수도 있다.

[0013] [21] 모바일 통신 디바이스(10)는 하우징(12)과 맞물린 뒷판(20)을 포함한다. 뒷판(20)이 하우징(12)과 실질적으로 일치하는 단면을 한정함으로써, 하우징(12)에 결합될 때 하우징(12)과 실질적으로 일체형 유닛을 형성한다. 뒷판(20)은 모바일 통신 디바이스(10)의 하나 또는 그보다 많은 양상들에 대한 접근을 제공하도록 모바

일 통신 디바이스(10)로부터 탈착 가능하다.

[0014] [22] 도 3은 (도 1에 도시된) 모바일 통신 디바이스(10)에 사용될 수 있는 예시적인 하드웨어 아키텍처의 개략도이다. 예시적인 구현에서, 모바일 통신 디바이스(10)는 메모리(22) 그리고 메모리(22)에 연결되어 프로그래밍된 명령들을 실행하기 위한 프로세서(24)를 포함한다. 프로세서(24)는 하나 또는 그보다 많은 처리 유닛들을 (예를 들어, 멀티코어 구성으로) 포함할 수도 있고 그리고/또는 (도시되지 않은) 암호화 가속기를 포함할 수도 있다. 모바일 통신 디바이스(10)는 메모리(22) 및/또는 프로세서(24)를 프로그래밍함으로써 본 명세서에서 설명되는 하나 또는 그보다 많은 동작들을 수행하도록 프로그래밍 가능하다. 예를 들어, 프로세서(24)는 실행 가능 명령들로서 동작을 인코딩하고 실행 가능 명령들을 메모리(22)에 제공함으로써 프로그래밍될 수도 있다.

[0015] [23] 프로세서(24)는, 범용 중앙 처리 유닛(CPU), 마이크로컨트롤러, 축소 명령 집합 컴퓨터(RISC: reduced instruction set computer) 프로세서, 오픈 미디어 애플리케이션 플랫폼(OMAP: open media application platform), 주문형 집적 회로(ASIC: application specific integrated circuit), 프로그래밍 가능 로직 회로(PLC: programmable logic circuit), 및/또는 본 명세서에서 설명되는 기능들을 실행할 수 있는 임의의 다른 회로 또는 프로세서를 포함할 수도 있지만 이에 한정된 것은 아니다. 본 명세서에서 설명되는 방법들은 한정 없이, 저장 디바이스 및/또는 메모리 디바이스를 포함하는 컴퓨터 판독 가능 매체에 포함된 실행 가능 명령들로서 인코딩될 수도 있다. 이러한 명령들은 프로세서(24)에 의해 실행될 때 프로세서(24)로 하여금, 본 명세서에서 설명되는 기능들의 적어도 일부를 수행하게 한다. 상기 예들은 단지 예시일 뿐이며, 따라서 프로세서라는 용어의 정의 및/또는 의미를 어떤 식으로도 한정하는 것으로 의도되지 않는다.

[0016] [24] 본 명세서에서 설명되는 것과 같은 메모리(22)는 실행 가능 명령들 및/또는 다른 데이터와 같은 정보가 저장 및 리트리브될 수 있게 하는 하나 또는 그보다 많은 디바이스들이다. 메모리(22)는 한정 없이, 동적 랜덤 액세스 메모리(DRAM: dynamic random access memory), 동기식 동적 랜덤 액세스 메모리(SDRAM: synchronous dynamic random access memory), 정적 랜덤 액세스 메모리(SRAM: static random access memory), 솔리드 스테이트 디스크, 및/또는 하드 디스크와 같은 하나 또는 그보다 많은 컴퓨터 판독 가능 매체를 포함할 수도 있다. 메모리(22)는 한정 없이, 실행 가능 명령들, 운영 시스템들, 애플리케이션들, 자원들, 설치 스크립트들 및/또는 본 명세서에서 설명되는 방법들 및 시스템들에 사용하기에 적합한 임의의 다른 타입의 데이터를 저장하도록 구성될 수도 있다.

[0017] [25] 운영 시스템들 및 애플리케이션들에 대한 명령들은 본 명세서에서 설명되는 프로세스들 중 하나 또는 그보다 많은 프로세스를 수행하도록 프로세서(24)에 의한 실행을 위해 비-일시적 메모리(22) 상에 함수 형태로 로케이팅된다. 서로 다른 구현들에서 이러한 명령들은 서로 다른 물리적 또는 유형의 컴퓨터 판독 가능 매체, 예컨대 메모리(22) 또는 한정 없이, 플래시 드라이브 및/또는 썸(thumb) 드라이브를 포함할 수도 있는 다른 메모리, 예컨대 컴퓨터 판독 가능 매체(26) 상에 포함될 수도 있다. 또한, 명령들은 한정 없이, 스마트 미디어(SM: smart-media) 메모리, 콤팩트 플래시(CF: compact flash) 메모리, 보안 디지털(SD: secure digital) 메모리, 메모리 스틱(MS: memory stick) 메모리, 멀티미디어 카드(MMC: multimedia card) 메모리, 임베디드 멀티미디어 카드(e-MMC: embedded-multimedia card) 및 마이크로 드라이브 메모리를 포함할 수도 있는 비-일시적 컴퓨터 판독 가능 매체(26) 상에 함수 형태로 로케이팅된다. 컴퓨터 판독 가능 매체(26)는 프로세서(24)에 의한 접근 및/또는 실행을 허용하도록 모바일 통신 디바이스(10)로부터 선택적으로 삽입 가능 및/또는 탈착 가능할 수도 있다. 일부 구현들에서, 컴퓨터 판독 가능 매체(26)는 탈착 가능하지 않다.

[0018] [26] 다시 도 3을 참조하면, 모바일 통신 디바이스(10)는 프로세서(24)에 위치 데이터를 제공하도록 구성되는 GPS 컴포넌트(30)를 포함할 수도 있다. 위치 데이터는 프로세서(24)가 모바일 통신 디바이스(10)의 위치를 결정하고 그리고/또는 예를 들어, 내비게이션 기능과 같은, 모바일 통신 디바이스(10)의 위치에 의존한 기능을 제공하는 것을 가능하게 한다. 대안적인 구현에서는, 인근 802.11 및/또는 블루투스 기지국들 또는 디바이스들, 및/또는 이들의 결합을 식별함으로써 셀룰러 네트워크를 사용하여 모바일 통신 디바이스(10)에 대한 위치 데이터가 얻어질 수도 있다.

[0019] [27] 일부 구현들에서, 모바일 통신 디바이스(10)는 추가로, 적어도 하나의 암호화 프로세서를 포함한다. 보다 구체적으로, 모바일 통신 디바이스(10)는 제 1 신뢰할 수 있는 플랫폼 모듈(TPM: trusted platform module)(60) 및 제 2 TPM(62)을 포함한다. TPM들은 모바일 통신 디바이스(10)로의/로부터의 통신을 위해 그리고/또는 모바일 통신 디바이스(10)로의 저장을 위해 프로세서(24)에 의해 접근되는 데이터의 적어도 일부를 암호화한다. 이에 따라, 일부 데이터는 모바일 통신 디바이스(10)의 다른 애플리케이션들 및/또는 동작들과 구별되고, 이러한 애플리케이션들/동작들보다 더 높은 수준의 보안이 유지될 수도 있다. 이에 따라, TPM들(60, 6

2)은 예를 들어, 신뢰할 수 있는 부팅, 신중한 부팅, 보안 부팅, 원격 증명 및 보호 키스토어를 작동시키는 것을 가능하게 한다.

[0020] [28] 또한, 모바일 통신 디바이스는 프로세서(24)에 연결된 보안 엘리먼트(64)를 포함한다. 보다 구체적으로, 보안 엘리먼트(64)는 범용 집적 회로 카드(UICC: Universal Integrated Circuit Card), 마이크로SD 카드, 그리고/또는 모바일 통신 디바이스(10) 내에 내장되는 것 중 적어도 하나로서 모바일 통신 디바이스(10)와 통합될 수도 있다. 보안 엘리먼트(64)는 키스토어 디바이스로서 그리고/또는 모바일 통신 디바이스(10) 상에서 작동하는 플랫폼에 대한 하드웨어 신뢰 앵커로서 사용될 수 있는 변조 방지(tamper-resistant) 저장 및 실행 환경이다. 보다 구체적으로, 보안 엘리먼트(64)는 데이터 암호 키들, 패스워드들 그리고 하드웨어 및 소프트웨어 구성 정보를 저장한다. 또한, 보안 엘리먼트(64)는 공개 키 쌍들을 생성하고 연관된 개인 키들의 내보내기의 제한을 가능하게 한다. 대안적인 구현에서, 보안 엘리먼트(64)는 TPM으로 구현될 수도 있다.

[0021] [29] 모바일 통신 디바이스(10)는 또한 보안 수퍼바이저 메모리(66)를 포함한다. 보안 수퍼바이저 메모리(66)는 복수의 키들을 포함할 수도 있고 보안 엘리먼트(64) 및/또는 제 1 TPM(60) 또는 제 2 TPM(62) 내에서 데이터를 랩핑(wrap)하는 데 사용될 수 있는 변조 반응(tamper-reactive) 데이터를 저장한다. 동작시, 변조 반응 데이터는 변조 사건의 검출시 랩핑된 데이터가 복구될 수 없게 클리어될 수 있다. 보안 수퍼바이저 메모리(66)는 모바일 통신 디바이스(10)가 본 명세서에서 설명되는 바와 같이 기능할 수 있게 하는 임의의 양의 변조 반응 데이터를 보유할 수 있다.

[0022] [30] 모바일 통신 디바이스(10)는 추가로, 프로세서(24)에 연결된 셀룰러 제어기(31)를 포함한다. 셀룰러 제어기(31)는 모바일 통신 디바이스(10)가 (도시되지 않은) 하나 또는 그보다 많은 셀룰러 네트워크와 통신하여 셀룰러 네트워크와의 음성 및/또는 데이터 통신을 제공하도록 허용한다. 이 예에서, 모바일 통신 디바이스(10)는 셀룰러 제어기(31)에 연결된 2개의 가입자 식별 모듈(SIM: subscriber identity module) 카드 소켓들(33A, 33B)을 포함한다. 이런 식으로, 모바일 통신 디바이스(10)는 모바일 통신 디바이스(10)의 사용자에 의해 선택 가능한 2개의 서로 다른 셀룰러 계정들과 연관된 2개의 SIM 카드들을 수신할 수 있다. 예를 들어, 모바일 통신 디바이스(10)는 개인용 셀룰러 계정 및 업무용 셀룰러 계정에 접근하여, 사용자가 그 사이에서 개인적 사용과 업무적 사용을 구별하도록 선택하게 할 수도 있다. 다른 구현들에서는 다른 개수의 SIM 카드 소켓들이 포함될 수도 있다고 인식되어야 한다.

[0023] [31] 또한, 모바일 통신 디바이스(10)는 프로세서(24)에 연결된 USB 제어기(35)를 포함한다. 도 3에 도시된 바와 같이, USB 제어기(35)는 커넥터(37)를 통해 접근 가능하다. 이런 식으로, 하나 또는 그보다 많은 서로 다른 디바이스들이 모바일 통신 디바이스(10)와 통신할 수도 있다. 마찬가지로, 모바일 통신 디바이스(10)는 추가로, 프로세서(24)에 연결되어 커넥터(41)를 통해 접근 가능한 고화질 멀티미디어 인터페이스(HDMI: high-definition multimedia interface) 제어기(39)를 포함한다. 적어도 하나의 구현에서, 커넥터들(37 및/또는 41)은 모바일 통신 디바이스(10)에 대한 마이크로-USB 및/또는 마이크로-HDMI 접속들을 제공할 수도 있다.

[0024] [32] 추가로 또는 대안으로, 모바일 통신 디바이스(10)는 하나 또는 그보다 많은 무선 통신 채널들을 제공하기 위해 블루투스 제어기, 지그비(ZigBee) 제어기 및/또는 Wi-Fi 제어기 중 하나 이상을 포함할 수도 있다. GPS 컴포넌트(30), 제 1 TPM(60), 제 2 TPM(62) 및 셀룰러 제어기(31)는 적어도 부분적으로는 하드웨어로 제공되지만, 모바일 통신 디바이스(10)에 통합된 하나 또는 그보다 많은 컴포넌트들은 프로세서(24)와 연관된 소프트웨어 및/또는 펌웨어를 통해 제공될 수도 있다고 추가로 인식되어야 한다. 일례로, 프로세서(24)는 모바일 통신 디바이스(10)의 저수준 에어 인터페이스 프로토콜들을 분석하고 공인된 네트워크 아이덴티티들 및 특징들을 기초로 네트워크 송신들을 허가 또는 거부하도록 구성된 에어 인터페이스 방화벽을 제공한다. 이 예에서, 셀룰러 네트워크 아이덴티티들 및 특징들을 포함하는 셀룰러 제어기(31)로부터의 에어 인터페이스 프로토콜 데이터는 프로세서(24)에 제공되고 프로세서(24)에 의해 분석되어, 모바일 통신 디바이스(10)가 셀룰러 제어기(31)에 의해 식별된 셀룰러 네트워크들을 통해 네트워크 송신들을 수행하도록 허가되어야 하는지 여부가 결정된다. 이 예에서, 제공되는 분석 수준은 프로세서(24)가 셀룰러 제어기(31)의 표준 셀룰러 네트워크 프로토콜 인증 메커니즘들만을 사용하는 것 이상으로 셀룰러 제어기(31)의 네트워크 접속들을 추가 인증하게 함으로써 모바일 통신 디바이스(10)에 네트워크 보안을 부가한다. 예를 들어, 블루투스 제어기 및/또는 Wi-Fi 제어기와 같은 모바일 통신 디바이스(10)의 다른 에어 인터페이스 컴포넌트들은 또한 에어 인터페이스 방화벽에 의해 모니터링될 수도 있다는 점이 주목되어야 한다. 대안적인 구현에서, 제 1 TPM(60) 및 제 2 TPM(62)은 소프트웨어로 구현될 수도 있다.

[0025] [33] 다른 모바일 통신 디바이스 구현들은 프로세서(24)와 통합된 또는 프로세서(24) 외부의 더 많은 또는

더 적은 컴포넌트들을 포함할 수도 있다고 인식되어야 한다.

[0026] [34] 도 4는 (도 1에 도시된) 모바일 통신 디바이스(10)에 사용될 수 있는 예시적인 소프트웨어 아키텍처(100)의 개략도이다. 예시적인 구현에서, 소프트웨어 아키텍처(100)는 프로세서(24) 및 메모리(22)를 포함하는 하드웨어 플랫폼(102) 상에 설치된 운영 시스템(104)을 포함한다. 하드웨어 플랫폼(102)은 앞서 설명한 모바일 통신 디바이스(10)의 컴포넌트들을 포함한다. 소프트웨어 아키텍처(100)는 또한 가상화 소프트웨어 계층, 예컨대 운영 시스템(104) 위에서 작동하는 하이퍼바이저(106)(즉, 타입 2 하이퍼바이저) 및 하이퍼바이저(106)와 연결되어 통신하는 보안 수퍼바이저(108)를 포함한다. 대안적인 구현에서, 하이퍼바이저(106)는 하드웨어 플랫폼(102) 상에 설치되어 동작할 수도 있다(즉, 타입 1 하이퍼바이저). 하이퍼바이저(106)는 복수의 가상 머신들이 동시에 실체화되어 실행될 수 있도록 복수의 가상 머신 실행 공간들을 지원한다.

[0027] [35] 하이퍼바이저(106)는 하이퍼바이저(106) 위에서 실행되어 작동할 수 있는 제 1 페르소나(110) 및 제 2 페르소나(120)를 가상화한다. 제 1 페르소나(110)는 제 1 페르소나 운영 시스템(OS)(112) 및 제 1 신뢰할 수 있는 실행 환경(TEE: trusted execution environment)(114)을 포함하고, 제 2 페르소나(120)는 제 2 페르소나 운영 시스템(122) 및 제 2 신뢰할 수 있는 실행 환경(124)을 포함한다.

[0028] [36] 제 1 페르소나(110) 및 제 2 페르소나(120)는 각각, 신뢰성을 확인하고 각각의 페르소나에 의해 수행되는 동작들을 인가하는 데 사용될 수 있는 정해진 신뢰 앵커를 갖는다. 보다 구체적으로, 제 1 페르소나(110)는 제 1 신뢰 앵커를 갖고, 제 2 페르소나(120)는 제 1 신뢰 앵커와는 별개인 제 2 신뢰 앵커를 갖는다. 본 명세서에서 사용되는 바와 같이, "신뢰 앵커"라는 용어는 페르소나의 소유자를 정의하는 그리고 페르소나 자산들을 서명하는 데 사용될 수도 있는 하나 또는 그보다 많은 비밀 암호 키들(즉, 암호화 인증서)을 의미한다. 반대로, 본 명세서에서 사용되는 바와 같이, "소유자" 및/또는 "소유권"이라는 용어들은 신뢰 앵커를 보유함으로써 페르소나에 대한 관리 통제를 하는 사람 또는 엔티티를 의미한다. 일부 구현들에서는, 신뢰 앵커 루트 인증서가 페르소나 패키지의 자산들을 서명하는 중간 인증서 권한을 서명하는 데 사용될 수도 있다.

[0029] [37] 각각의 신뢰 앵커는 루트 인증서 권한을 역추적하는데, 이는 업체 기관일 수도 있고 그리고/또는 데스크톱 컴퓨터 상의 단일 사용자에 대해 가벼운 방식으로 정의될 수도 있다. 이에 따라, 제 1 페르소나(110)의 자원들은 제 2 페르소나(120)와 별개로 유지될 수도 있고, 각각의 신뢰 앵커에 대해 합의되어 그에 의해 서명된 접근 정책들이 시행될 수도 있다. 루트 인증서 권한은 오프라인으로 보안 위치에 저장될 수도 있다. 또한, 신뢰 앵커는 구체적으로 정의된 능력들을 갖는 복수의 중간 인증서 권한들을 포함할 수도 있다. 예시적인 능력들은 운영 시스템을 정할 권한, TEE를 정할 권한, 보안 정책들을 정할 권한, 다른 중간 인증서 권한들 및/또는 사용자 인증서들을 정할 권한, 백업 능력들, 백업 정책, 운영 시스템을 업데이트하는 능력, TEE를 업데이트하는 능력, 모바일 디바이스 관리(MDM: mobile device management) 기능, 및 키 가져오기 및/또는 내보내기를 포함하지만 이에 한정된 것은 아니다.

[0030] [38] 제 1 페르소나(110) 및 제 2 페르소나(120)의 신뢰할 수 있는 소프트웨어는 각각, 다른 하위 디폴트 상태들로부터 격리된 상황에서 작동한다. 보다 구체적으로는, 앞서 설명한 바와 같이, 하이퍼바이저(106)가 제 1 TEE(114)와 제 2 TEE(124)를 서로 구별하고 격리하는 것을 가능하게 한다. 이에 따라, 각각의 페르소나는 모바일 통신 디바이스(10) 상에서 작동하는 다른 운영 시스템들의 영향을 받지 않을 것이다. 또한, 제 1 페르소나(110) 및 제 2 페르소나(120)는 제 1 TEE(114)와 제 2 TEE(124) 사이에 상호 신뢰를 구축하도록 구성될 수도 있다. 이러한 상호 신뢰의 구축은 제 1 페르소나(110)와 제 2 페르소나(120) 사이에 신뢰할 수 있는 통신 경로가 형성될 수 있게 한다. 제 1 TEE(114)와 제 2 TEE(124) 사이의 통신은 제 1 페르소나(110) 및 제 2 페르소나(120)의 보안 정책들의 상호 합의에 의해서만 허용될 수도 있다. 또한, (도시되지 않은) 고 확실성 가드(high assurance guard)가 제 1 페르소나(110)와 제 2 페르소나(120) 간의 데이터 흐름의 제한을 가능하게 하도록 구현될 수도 있다. 예를 들어, 고 확실성 가드는 제 1 페르소나(110)와 제 2 페르소나(120) 간의 민감한 그리고/또는 분류된 데이터의 흐름을 제한하면서, 이들 사이의 분류되지 않은 데이터의 흐름은 허용하는 것을 가능하게 할 수도 있다.

[0031] [39] 제 1 페르소나(110) 및 그 엘리먼트들은 아래 더 상세히 설명될 것이지만, 제 2 페르소나(120) 및 그 엘리먼트들에 동일한 설명이 적용될 수도 있다고 이해되어야 한다. 예시적인 구현에서, 제 1 페르소나 OS(112)는 전체 운영 시스템의 작동을 가능하게 하는 자원들 및 가상 디바이스 드라이버들을 갖는 실행 환경이다. 예시적인 전체 운영 시스템은 Android® 오픈 소스 프로젝트(AOSP: Open Source Project) 운영 시스템을 포함할 수도 있지만 이에 한정된 것은 아니다. 제 1 페르소나 OS(112)는 제 1 페르소나 OS(112)가 제 1 TEE(114)와 통신할 수 있게 하는 라이브러리를 포함할 수도 있다. 또한, 복수의 애플리케이션들(130)이 (도시되지 않은) 외

부 소스로부터 획득되어 제 1 페르소나 OS(112) 위에서 작동할 수도 있다.

[0032] [40] 제 1 TEE(114)는 제 1 페르소나 OS(112)와 별개이며 제 1 페르소나 OS(112)와 연결되어 통신하는 가벼운 실행 환경이다. 제 1 TEE(114)는 민감한 데이터를 저장하고 민감한 애플리케이션들을 작동시키는 데 사용될 수 있는 영역을 제공하는 보안 환경이다. 대안적인 구현들에서, 제 1 TEE(114)는 전체 운영 시스템의 작동을 가능하게 하는 자원들 및 가상 디바이스 드라이버들을 갖는 실행 환경일 수도 있고 그리고/또는 하드웨어의 개별 부분 상에서 작동될 수도 있다. 또한, 제 1 페르소나(110)는 하나를 초과하는 신뢰할 수 있는 실행 환경을 포함할 수도 있다.

[0033] [41] 제 1 TEE(114)는 ISO7816 가입자 식별 모듈(SIM) 인터페이스 및/또는 TPM에 직접 접근한다. 보다 구체적으로, (도 3에 도시된) 제 1 TPM(60)이 제 1 페르소나(110)에 할당되고, (도 3에 도시된) 제 2 TPM(62)이 제 2 페르소나(120)에 할당된다. 이에 따라, 제 1 TPM(60)이 제 1 페르소나(110)의 소유자에 대한 하드웨어 신뢰 앵커로서 사용될 수도 있고, 제 2 TPM(62)이 제 2 페르소나(120)의 소유자에 대한 하드웨어 신뢰 앵커로서 사용될 수도 있다. 또한, 제 1 TEE(114)는 제 1 TPM(60)에 그리고 예를 들어, 인증, 키스토어 접근, 가상 개인 네트워크(VPN: virtual private network) 구성, 및/또는 인터넷을 통한 음성 프로토콜(VoIP: voice over internet protocol) 소프트웨어와 같은 신뢰할 수 있는 실행 환경 서비스들에 직접 접근한다. 이러한 민감한 데이터 경로들을 제 1 TEE(114) 내에서 그리고 제 1 페르소나 OS(112)로부터 멀리 격리하는 것은 페르소나 소유자에 의한 TEE 서비스들의 제어를 유지하면서 모바일 통신 디바이스(10)의 신뢰할 수 있는 동작을 보장하는 것을 가능하게 한다. 또한, 제 1 TEE(114)가 제 1 TPM(60)을 제어하게 하는 것은, 정보가 더 안전하고 보호되는 환경에 있도록 제 1 페르소나 OS(112)로부터 민감한 정보를 격리하는 것을 가능하게 한다.

[0034] [42] 또한, 제 1 TEE(114)는 암호화 동작들이 이를 평문 키에 노출시키지 않으면서 제 1 페르소나 OS(112) 대신 수행될 수 있도록 암호화 서비스들에 접근할 수도 있다. 보다 구체적으로, 제 1 TEE(114)는 인증되지 않은 하드웨어 가속 암호 기법, 스위트(suite) B 및/또는 FIPS-140-2 인증된 암호화를 가능하게 하는 암호화 모듈들을 제 1 TPM(60)에서 사용할 수도 있다. 모바일 통신 디바이스(10)는 또한 VPN 모듈 및/또는 VoIP 모듈을 포함할 수도 있다. VPN 모듈은 제 1 페르소나(110)가 VPN을 인증하여 신뢰할 수 없는 코드에는 인증 또는 암호 키들이 보이지 않는 암호화로 통신할 수 있게 한다. 추가로, VoIP 모듈은 제 1 페르소나(110)가 VoIP 호를 설정하고 인증하여 신뢰할 수 없는 코드에는 인증 또는 암호 키들이 보이지 않는 암호화로 통신할 수 있게 한다.

[0035] [43] 제 1 페르소나 OS(112) 및 제 2 페르소나 OS(122)의 신뢰성은 플랫폼 하드웨어(102)에 의해 로딩되는 각각의 페르소나의 부트 이미지의 무결성으로 정의된다. 예를 들어, 제 1 TEE(114)의 신뢰성은 아래 더 상세히 설명되는 바와 같이 플랫폼 하드웨어(102)에 의해 로딩될 때 그 정적 이미지의 무결성으로 정의된다. 보다 구체적으로, 제 1 TEE(114)에 로딩되는 코드는 로딩 중에 신뢰 앵커와 비교하여 승인되고, 이미지는 일단 로딩되면 불변한다. 이미지는 불변하기 때문에, 제 1 TEE(114)는 제 1 TEE(114) 위로 새로운 서명된 이미지를 로딩하는 것에 의해서만 변경될 수도 있다. 또한, 제 1 페르소나 OS(112) 및 제 2 페르소나 OS(122)는 이들 자체의 실행 환경 밖의 자원들을 사용하여 이들의 무결성을 관리할 수도 있다. 예를 들어, 운영 시스템들의 로딩은 암호화되어 승인될 수도 있고, 하드웨어 자원들에 대한 운영 시스템들의 접근은 이들의 제어 밖의 구성들을 통해 제한 및 시행될 수도 있다.

[0036] [44] 소프트웨어 아키텍처(100)는 또한 운영 시스템(104)을 로딩하는 1차 부트로더(140), 제 1 페르소나 OS(112)를 로딩하는 첫 번째 2차 부트로더(142), 및 제 2 페르소나 OS(122)를 로딩하는 두 번째 2차 부트로더(144)를 포함한다. 예시적인 구현에서, 모바일 통신 디바이스(10)는 부팅 프로세스 동안 플랫폼 신뢰의 구축을 가능하게 하는 프로세서를 사용한다. 보다 구체적으로, 프로세서는 부트로더들의 서명 검증이 각각의 운영 시스템의 로딩 중에 신뢰의 구축을 가능하게 할 수 있게 한다. 예를 들어, 모바일 통신 디바이스(10)는 신뢰 체인이 하드웨어 플랫폼(102)에서 제 1 페르소나(110) 및 제 2 페르소나(120)로 확장될 때 신뢰 체인이 끊어지지 않고 유지되도록 고정된 해시 값들과 서명 검증의 결합을 사용한다.

[0037] [45] 동작시, 프로세서(24)는 디바이스 제조사의 신뢰 루트에 의해 디지털 서명된다면 1차 부트로더(140)를 로딩한다. 본 명세서에서 사용되는 바와 같이, "디바이스 제조사 신뢰 루트"라는 용어는 모바일 통신 디바이스(10) 상에 설치하게 된 자산들을 서명하기 위해 디바이스 제조사에 의해 사용되는 하나 또는 그보다 많은 비밀 암호 키들(즉, 암호화 인증서)을 의미한다. 신뢰 체인은 하이퍼바이저(106)를 통해 끊어지지 않고 계속되어, 격리된 실행 환경들의 구축, 모바일 통신 디바이스(10) 내에서 컴포넌트들의 승인, 및/또는 사용자 코드가 신뢰할 수 있는 상태에 대해 구속하도록 추후 사용하기 위해 신뢰할 수 있는 플랫폼 모듈들로의 측정들의 저장을 가능하게 한다.

[0038] [46] 제 1 페르소나(110) 및 제 2 페르소나(120)에 의해 TPM들(60, 62)의 신중한 부팅 양상들이 사용될 수 있도록, 제 1 TPM(60)의 제어는 제 1 페르소나(110)에 양도(transfer)되고, 제 2 TPM(62)의 제어는 제 2 페르소나(120)에 양도된다. 보다 구체적으로, TPM들(60, 62)은 모바일 통신 디바이스(10)의 신뢰할 수 있는 부팅 소프트웨어에 의해 초기화되고, 다음에 페르소나들이 로딩된 후 이들의 배타적 사용을 위해 각각의 페르소나에 제어가 양도된다. 페르소나가 신뢰할 수 있는 부팅을 위해 TPM을 사용한다면, 하드웨어 및/또는 소프트웨어 변경들은 페르소나가 전체 디바이스를 리셋하지 않고는 재부팅되지 못할 수도 있게 원래 구성들에 대해 구속된 키들의 리트리브 불능을 야기할 수도 있다.

[0039] [47] 부팅 프로세스 동안, TPM들은 모바일 통신 디바이스(10) 내에서 사용되는 중대한 소프트웨어 및 펌웨어 컴포넌트들을 측정(즉, 해시)한다. 예를 들어, 1차 부트로더(140), 운영 시스템(104), 하이퍼바이저(106), 보안 수퍼바이저(108), 부트로더(142) 및 제 1 페르소나 OS(112)에 대한 측정들이 제 1 TPM(60)으로 확장될 때 측정에 대한 신뢰 루트가 구축될 수도 있다. 측정들은 제 1 TPM(60)에 로케이팅된 플랫폼 구성 레지스터(PCR: platform configuration register)들 내에 저장될 수 있고, 부팅시 연관된 신뢰 앵커와 비교하여 운영 시스템의 이미지를 승인하는 데 사용될 수도 있다. 이에 따라, PCR들에 구속될 수도 있는 민감한 정보에 대한 접근을 허용하기 전에 시스템의 무결성이 검증될 수도 있다.

[0040] [48] 부트 로딩 중에 신뢰할 수 있는 디바이스 제조사로부터 제어가 트랜지션되면, 페르소나들이 이들 자체의 무결성에 책임이 있을 수 있다. 예를 들어, 제 1 페르소나 OS(112) 상에 설치되어 작동하는 애플리케이션들(130)을 승인하는 것은 제 1 페르소나 OS(112)의 책임이다. 이에 따라, (도시되지 않은) 사기(rogue) 애플리케이션이 모바일 통신 디바이스(10) 상에서 작동하는 게스트 운영 시스템의 무결성을 손상시키는 경우, 다른 게스트 운영 시스템들이 손상된 운영 시스템과 신뢰 관계를 갖지 않는다면 그 손상은 다른 게스트 운영 시스템들의 무결성에 영향을 주지 않을 것이다.

[0041] [49] 보안 수퍼바이저(108)가 제 1 및 제 2 페르소나 OS들(112, 122)과 연결되어 통신한다. 보안 수퍼바이저(108)는 모바일 통신 디바이스(10)의 동작에 사용할 보안 정책들의 저장 및 실행을 가능하게 하는 운영 시스템이다. 보안 수퍼바이저(108)는 격리된 환경에서 작동하며, 플랫폼 자원들, 추가 인터페이스들 및/또는 추가 능력들에 접근할 수도 있다. 일부 구현들에서, 페르소나 소유자가 그 페르소나 소유자에 의해 소유되지 않은 페르소나의 보안 정책을 구성할 수 없도록 제 1 페르소나(110) 및 제 2 페르소나(120)는 신뢰할 수 있는 메커니즘(즉, CPU 가상화)을 통해 구별된다. 예를 들어, 제 1 페르소나(110)의 보안 정책은 제 1 페르소나 소유자에 의해서만 구성될 수 있고, 제 2 페르소나(120)의 보안 정책은 제 2 페르소나 소유자에 의해서만 구성될 수 있다. 보다 구체적으로, 각각의 보안 정책은 페르소나 소유자의 개인 키로 서명될 수도 있고, 서명은 보안 수퍼바이저(108)가 연관된 페르소나에 보안 정책을 적용하기 전에 페르소나 소유자의 대응하는 공개 키를 사용하여 모바일 통신 디바이스(10)에 의해 검증될 수도 있다. 제 1 페르소나(110) 및 제 2 페르소나(120)에 대한 소유권 및 보안 정책들은 보안 수퍼바이저(108)에 의해 유지될 수도 있는 구성 파일에 저장된다. 또한, 소유권 및 보안 정책들은 암호화 인증서들에 의해 승인된다. 이에 따라, 각각의 페르소나 소유자는 각자 소유하는 페르소나에 대한 운영 시스템, 신뢰할 수 있는 실행 환경 및 보안 정책을 정의할 수 있다.

[0042] [50] 제 1 페르소나(110) 및 제 2 페르소나(120)의 보안 정책들은 페르소나 소유자들에 의해 정의될 수도 있고, 페르소나 코드와는 별개로 정의, 저장 및 시행될 수도 있다. 보안 정책들은 각각의 연관된 페르소나가 모바일 통신 디바이스(10) 상의 물리적 디바이스들에 어떻게 접근할 수 있는지를 정의한다. 예를 들어, 보안 정책들은 하나 또는 그보다 많은 물리적 디바이스들에 대한 페르소나의 접근을 제한하고, 하나 또는 그보다 많은 물리적 디바이스들에 대한 페르소나의 배타적 접근의 가이드라인들을 정의하고, 그리고/또는 제 1 페르소나(110) 및 제 2 페르소나(120)에 대한 공유 디바이스 접근의 가이드라인을 정의한다. 보다 구체적으로, 공유 디바이스에 대한 접근의 가이드라인들은 사용자 인터페이스를 제어하고 있는 페르소나만이 공유 디바이스에 접근하도록 디바이스를 공유하는 것을 가능하게 할 수도 있다. 또한, 공유 디바이스에 대한 접근에 관한 하나 또는 그보다 많은 보안 정책들에 명시된 규칙들은 배경에서 작동하는 페르소나가 여전히 공유 디바이스에 접근할 수 있도록 디바이스를 공유하는 것을 가능하게 할 수도 있다. 이에 따라, 보안 정책들에 의해 정의된 규칙들은 페르소나 소유자들이 이들의 요구들에 맞게 모바일 통신 디바이스(10)를 다양한 구성들로 맞출 수 있게 한다.

[0043] [51] 제 1 페르소나(110)의 기준 이미지 및/또는 파일시스템들이 암호화되어 내부 및/또는 탈착 가능 매체 상에 저장될 수도 있다. 또한, 제 1 페르소나(110)가 부팅하여 그에 저장된 민감한 데이터에 접근할 수 있기 전에 신뢰할 수 있는 부팅 프로세스로부터의 사전 부팅 인증이 요구될 수 있게 제 1 페르소나(110)의 부트 볼륨이 암호화될 수도 있다. 보다 구체적으로, 신뢰할 수 있는 부팅 프로세스 도중, 제 1 페르소나(110)가 부팅이 허용되기 전에 크리덴셜들을 입력하도록 사용자에게 프롬프트(prompt)될 수도 있다. 사용자는 자신의 크리덴셜

들을 입력하기 전에 모바일 통신 디바이스(10)의 상태를 검증하길 원할 수도 있다. 예를 들어, 사용자는 입력 화면이 인증된 것임을 확실하게 하기 위해 패스워드 및/또는 개인 식별 번호(PIN: personal identification number)를 입력하기 전에 모바일 통신 디바이스(10)가 신뢰할 수 있는 상태라는 검증을 요청할 수도 있다. 앞서 설명한 바와 같이, 모바일 통신 디바이스(10)는 보안 버튼(17) 및/또는 (도 1에 도시된) LED들(19, 21)과 같은 보안 특징들을 포함한다. 보안 특징들은 입력 화면이 인증된 것이라는 검증을 가능하게 하기 위해, 모바일 통신 디바이스(10) 상에서 작동하는 신뢰할 수 없는 코드로부터 접근 불가능한 하드웨어에 격리된다.

[0044] [52] 동작시, 사용자는 (도 1에 도시된) 터치 스크린(18) 상에 인증 다이얼로그가 나타나면 보안 버튼(17)을 작동시킬 수 있다. 보안 버튼(17)을 작동시키는 것은 모바일 통신 디바이스(10)에 대한 신뢰 루트 정보를 디스플레이하고 그리고/또는 인증 다이얼로그가 나타날 것을 요청하는 소프트웨어에 대한 신뢰 루트 정보를 디스플레이한다. 예를 들어, 신뢰 루트 정보는 모바일 통신 디바이스(10)에 대한 그리고/또는 모바일 통신 디바이스(10) 상에서 작동하는 페르소나에 대한 신뢰 루트 정보를 포함할 수도 있다. 이에 따라, 사용자는 신뢰 루트 정보를 검증하여 요청된 크리덴셜들을 안전하게 입력할 수 있다. 대안적인 구현에서는, LED들(19, 21)이 미리 결정된 구성으로 활성화될 때 인증 다이얼로그가 검증될 수도 있다.

[0045] [53] 한 구현에서, 사용자가 모바일 통신 디바이스의 동작 상태 변경을 원할 수도 있다. 보다 구체적으로, 사용자가 모바일 통신 디바이스(10) 상에서 작동하는 페르소나들 사이에서 모바일 통신 디바이스(10)의 포커스를 트랜지션하길 원할 수도 있다. 예를 들어, 보안 버튼(17)을 작동시키는 것은 제 1 페르소나(110)와 제 2 페르소나(120) 간의 포커스 트랜지션을 가능하게 한다. 더욱이, 제 1 LED(19)가 제 1 페르소나(110)에 할당되고, 제 2 LED(21)가 제 2 페르소나(120)에 할당된다. 제 1 페르소나(110)에 포커스가 맞춰지면 제 1 LED(19)는 활성화될 수 있고 제 2 LED(21)는 비활성화될 수 있으며, 제 2 페르소나(120)에 포커스가 맞춰지면 제 2 LED(21)는 활성화될 수 있고 제 1 LED(19)는 비활성화될 수 있다. 이에 따라, 제 1 LED(19) 및 제 2 LED(21)가 모바일 통신 디바이스(10)의 동작 상태를 기초로 사용자에게 시각적 피드백을 제공한다.

[0046] [54] TPM들(60, 62) 중 적어도 하나는 사용자에게 모바일 통신 디바이스(10)에 대한 그의 존재를 검증하도록 프롬프트하는 물리적 존재 특징을 갖는다. 예를 들어, 물리적 존재 특징은 모바일 통신 디바이스(10) 상에서 작동하고 있는 동작이 원격으로 수행되고 있지 않음을 검증하도록 구현될 수도 있다. 이에 따라, 보안 버튼(17)이 눌려 사용자의 물리적 존재가 검증될 수 있다.

[0047] [55] 도 5는 모바일 통신 디바이스(10)에 사용될 수 있는 페르소나의 소유권을 주장하는 예시적인 방법의 흐름도이다. 예시적인 구현에서, 모바일 통신 디바이스(10)는 암호 신뢰 루트들을 사용하여 제 1 페르소나(110) 및 제 2 페르소나(120)의 소유권을 정의한다. 예를 들어, 제 1 페르소나(110)는 하나의 엔티티에 의한 사용을 위해 구성될 수 있고, 제 2 페르소나(120)는 다른 엔티티에 의한 사용을 위해 구성될 수 있다. 모바일 통신 디바이스(10)의 발행인(즉, 기업)은 사용자(예를 들어, 고객 및/또는 피고용자)에게 하나 또는 그보다 많은 모바일 통신 디바이스들(10)을 지급할 수 있다. 이러한 구현에서, 제 1 페르소나(110)는 업무용으로 구성될 수도 있고, 제 2 페르소나(120)는 개인용으로 구성될 수도 있다. 대안적인 구현에서, 모바일 통신 디바이스(10)는 개별 SIM들, 개별 서비스들을 할당함으로써, 그리고/또는 제 1 페르소나(110) 및 제 2 페르소나(120)의 데이터, 운영 시스템들 및 셀룰러 통신들을 격리함으로써 페르소나들을 구별하도록 구성될 수도 있다.

[0048] [56] 암호 신뢰 루트들의 사용은 모바일 통신 디바이스(10)가 페르소나 구성의 무결성을 검증하고, 페르소나의 수정 권한들을 공인된 자들로 제한할 수 있게 한다. 예를 들어, 적어도 하나의 디폴트 페르소나(즉, 정해진 소유권이 없는 페르소나)가 설치된 모바일 통신 디바이스(10)가 최종 사용자에게 제공될 수 있다. 디폴트 페르소나는 제조사의 디폴트 신뢰 앵커로 서명되는데, 이는 페르소나가 수정되지 않으며 그에 할당된 디폴트 정책을 가짐을 표시한다. 그래서 최종 사용자는 디폴트 페르소나를 사용할 수 있지만, 신뢰 루트를 정의함으로써 먼저 소유권을 취득하지 않고서는 디폴트 페르소나를 커스터마이즈할 수 없다.

[0049] [57] 운영자(200)는 페르소나 매니저(PM: Persona Manager)(202)의 워크스테이션 상에 페르소나에 대한 신뢰 루트를 생성(212)함으로써 제 2 페르소나(120)와 같은 페르소나의 소유권을 주장한다. 일부 구현들에서, PM(202)은 또한, 운영자(200)가 페르소나에 대한 보안 정책을 편집 및/또는 정의하고 그리고/또는 페르소나의 이미지들 및/또는 제 2 TEE(124)와 같은 신뢰할 수 있는 실행 환경을 업데이트할 수 있게 할 수도 있다. 운영자(200)는 디폴트 신뢰 앵커로부터의 소유권을 생성된(212) 신뢰 루트에 양도하도록 디바이스 매니저(DM: Device Manager)(204)가 제 2 페르소나 OS(122)와 같은 운영 시스템을 주장하기 위한 주장 티켓을 생성(214)할 것을 요청한다. 다음에, 양도가 인가(216)되고 모바일 통신 디바이스(10)가 재부팅(218)된다.

[0050] [58] 재부팅(218) 동안, 운영자(200)는 DM(204)과 모바일 통신 디바이스(10) 사이에 범용 직렬 버스(USB:

Universal Serial Bus) 케이블을 연결하고, 모바일 통신 디바이스(10)는 USB 접속을 검출하여, 페르소나 운영 시스템들이 로딩하지 않도록 프로그래밍 모드에 진입한다. 운영자(200)는 다음에, DM(204)이 소프트웨어를 작동시켜 페르소나를 새로운 소유자에게 양도할 것을 워크스테이션으로부터 요청(220)한다. 요청은 보안 수퍼바이저(206) 쪽으로 전달(222)되고 새로운 페르소나 신뢰 앵커를 정의할 수도 있다. 다음에, 보안 수퍼바이저(206)는 생성된(214) 주장 티켓을 사용하여 자신의 아이덴티티를 검증하기 위한 운영자(200)로부터의 인가를 요청(224)하고, 운영자(200)는 인가 요청(224)에 응답하여 미리 결정된 디바이스 패스워드를 입력(226)한다. 요청(224)은 또한 생성된(212) 신뢰 루트로 서명될 수도 있다.

[0051] [59] 모바일 통신 디바이스(10)는 다음에, 사용자들의 크리덴셜들을 입력하여 보안 엘리먼트(208)를 언로크하도록 보안 수퍼바이저(206)로부터의 인증 요청(228)을 사용자에게 제시한다. 디폴트 신뢰 앵커에 의해 페르소나가 소유자 없는 것으로 확인된다면, 구(old) 페르소나 자산 해시들 및 서명들이 DM(204)으로 양도(234)된다. DM(204)은 서명들을 검증하고, 관련 자산들을 서명하도록 인가되는 새로운 페르소나 서명 키로 해시들을 다시 서명한다. 또한, 페르소나 미디어 키들에 대한 접근을 허용하는 페르소나 키가 변경된다. 다음에, 대체 서명들이 DM(204)에서 모바일 통신 디바이스(10)로 양도(236)되고, 모바일 통신 디바이스(10)는 서명들을 승인하고 페르소나 자산들에 대한 구 서명들을 새로운 서명들로 대체한다.

[0052] [60] 다음에, 페르소나 트랜지션 파일이 생성(238)되고, 페르소나에 대한 구성 파일이 유효성에 관해 체크되며 이미 모바일 통신 디바이스(10) 상에 있는 다른 구성 파일들과 충돌한다. 구성 파일이 승인된다면 프로세스가 진행되고, 구성 파일들 간에 충돌이 있다면 소프트웨어 업데이트가 중단된다. 인가시 사용자 페르소나 인증이 업데이트(240)되어, 미디어 키들이 새로운 신뢰 루트에 의해 접근되고 DM(204)으로 리턴(242)될 수 있게 진행한다.

[0053] [61] DM(204)은 업데이트되고 있는 자산들을 서명하고, 서명된 해시들을 리턴한다. 예를 들어, 업데이트되고 있는 자산들은 다시 서명된 해시들로 업데이트되는 서명들을 가질 수도 있고 그리고/또는 새로운 서명들로 업데이트(246)될 수도 있다. 각각의 업데이트 이후 페르소나 트랜지션 파일이 체크포인트(244)되어 프로세스가 중단된 업데이트에서부터 재시작될 수 있게 한다. 업데이트가 완료된 후, 버퍼 데이터가 플래시(210)로 플러시(flush)(248)되고, 페르소나 트랜지션 파일이 삭제(250)되며, 모바일 통신 디바이스(10)가 재부팅(252)된다.

[0054] [62] 도 6은 모바일 통신 디바이스(10) 상에서 수행될 동작을 인가하는 데 사용하기 위한 예시적인 시스템(300)의 개략도이다. 예시적인 구현에서, 엔티티는 모바일 통신 디바이스(10)와 같은 타깃이 되는 컴퓨팅 디바이스 상에 설치된 소프트웨어를 수정하도록 허가를 받기 전에 인가될 필요가 있을 수도 있다. 예를 들어, 모바일 통신 디바이스(10) 상에 페르소나가 로딩되었다면, 디바이스 보유자는 그 페르소나를 제거 및/또는 교체할 권한을 보유하지만, 페르소나 소유자는 페르소나를 수정할 권한을 갖는다. 이에 따라, 페르소나 소유자를 대행하는 엔티티는 페르소나를 수정하도록 페르소나 소유자에 의해 그 엔티티에 그랜트된 미리 결정된 허가들을 받은 것으로서 인가될 필요가 있을 수도 있다. 본 명세서에서 사용되는 바와 같이, "디바이스 보유자"라는 용어는 디폴트 페르소나를 사용하여 모바일 통신 디바이스(10)를 작동시키는 엔티티를 의미한다.

[0055] [63] 디바이스 매니저(DM)(302)와 같은 관리자 컴퓨터가 모바일 통신 디바이스(10) 상에서 동작을 수행하기 위한 인가에 대한 요청을 생성하여 인가 서버(304)에 송신할 수 있다. 요청은 모바일 통신 디바이스(10) 상에서 수행될 동작에 대한 파라미터들을 특정하는 파일이다. 예시적인 파라미터들은 타깃이 되는 컴퓨팅 디바이스(예를 들어, 모바일 통신 디바이스(10))의 식별, 타깃이 되는 컴퓨팅 디바이스 상에서 수행될 동작, 동작이 수행될 시간 기간, 및 타깃이 되는 컴퓨팅 디바이스의 지리적 위치를 포함하지만 이에 한정된 것은 아니다. 더욱이, 요청은 관리자에게 할당된 제 1 개인, 공개 키 쌍의 개인 키로 서명된다. 일부 구현들에서, 요청은 (도시되지 않은) 탈착 가능 매체를 통해 송신될 수도 있다.

[0056] [64] 인가 서버(304)는 DM(302)으로부터의 요청을 수신하고 제 1 개인, 공개 키 쌍의 공개 키로 DM(302)의 서명을 검증한다. 인가 서버(304)는 또한, 수행될 동작에 대한 파라미터들이 모바일 통신 디바이스(10)에 대한 보안 정책에 맞춰 조정되는지 여부를 결정한다. 인가된 파라미터들은 인가 서버(304)에 의해 접근 가능한 인가 데이터베이스(306)에 저장될 수 있다. 다음에, 인가 서버(304)는 요청이 인가되었다면 인가 응답을 생성한다. 인가 응답은 DM(302)으로부터의 요청 및 인가 서버(304)에 의해 생성된 인가 토큰을 포함할 수도 있다. 인가 토큰은 요청된 동작을 인가하는 데 사용될 수도 있다. 일부 실시예들에서, 인가 토큰은 미리 결정된 수명을 가질 수도 있고, 특정 타깃이 되는 컴퓨팅 디바이스에 대한 인가의 그랜트로 제한될 수도 있고, 그리고/또는 모바일 통신 디바이스(10) 상에서 단일 또는 다수의 동작들의 수행을 인가할 수도 있다. 단지 예로서, 인가 토큰은 미리 결정된 타깃이 되는 컴퓨팅 디바이스 상에서 동작을 수행하기 위한 인가, 및/또는 타깃이 되는 컴퓨팅 디

바이스 상에서 미리 결정된 동작을 수행하기 위한 인가를 포함할 수도 있다. 더욱이, 인가 토큰은 모바일 통신 디바이스(10) 상에서 동작을 수행하기 위한 요청을 수신하기 전에 그리고 모바일 통신 디바이스(10) 상에서 동작을 수행하기 위한 요청의 검증에 응답하여 중 적어도 하나에 따라 생성될 수도 있다. 다음에, 인가 응답은 인가 서버 컴퓨터와 연관된 제 2 개인, 공개 키 쌍의 개인 키로 서명되어 관리자 컴퓨터에 송신될 수도 있다. 대안적인 구현에서, 인가 응답은 인증 운영자에 의해 서명될 수도 있다. 예를 들어, 요청은 대기 열이 이루어져 인증 운영자에 의해 서명되거나, 그랜트되거나 또는 거부될 수도 있다. 일부 구현들에서, 인가 응답은 (도시되지 않은) 탈착 가능 매체를 통해 송신될 수도 있다.

[0057] [65] DM(302)은 인가 응답을 수신하고 인가 토큰이 요청된 동작을 인가하는지 여부를 결정한다. 예를 들어, DM(302)은 제 2 개인, 공개 키 쌍의 공개 키로 인가 응답을 검증할 수도 있으며, 여기서 인가 응답은 제 2 개인, 공개 키 쌍의 개인 키로 서명된다. DM(302)은 다음에, 인가 응답 파일을 모바일 통신 디바이스(10)에 송신하여, 요청이 인가되었다면 수행될 동작을 요청한다. 인가 응답의 송신은 제 1 개인, 공개 키 쌍의 개인 키로 인가 응답을 서명하는 것을 포함할 수도 있다. 모바일 통신 디바이스(10)는 인가 응답을 수신하고 관리자 컴퓨터와 연관된 제 1 개인, 공개 키 쌍의 공개 키로 서명들을 검증하며, 인가 응답에 명시된 파라미터들이 모바일 통신 디바이스(10)에 대한 보안 정책에 맞춰 조정되는지 여부를 결정한다. 모바일 통신 디바이스(10)는 서명들이 검증되고 파라미터들이 조정된다면 요청된 동작이 진행되게 한다. 다음에, 모바일 통신 디바이스(10) 상에서 특권 동작이 수행될 수도 있다. 대안적인 구현에서, 인가 응답은 인가 신뢰 루트에 대한 인증서 체인을 포함할 수도 있다. 또한, 대안적인 구현에서, 인가 토큰이 생성되어 스니커넷을 통해 송신될 수도 있다.

[0058] [66] 도 7은 모바일 통신 디바이스(10)에 사용될 수 있는 페르소나 소프트웨어를 업데이트하는 예시적인 방법의 흐름도이다. 예시적인 구현에서, 운영자(400)는 디바이스 매니저(DM) 워크스테이션(402)에서부터 모바일 통신 디바이스(10)까지 USB 케이블을 연결함으로써 제 2 페르소나(120)와 같은 기존의 페르소나 OS를 업데이트할 수도 있다. 디바이스 관리 소프트웨어가 실행되고, 운영자(400)는 모바일 통신 디바이스(10)에 재부팅(410)을 지시한다. 재부팅(410) 동안, 모바일 통신 디바이스(10)는 USB 접속을 검출하여, 페르소나 운영 시스템들이 로딩하지 않도록 프로그래밍 모드에 진입한다. 운영자(400)는 다음에, 모바일 통신 디바이스(10) 상의 페르소나 OS에 대한 업데이트를 요청(414)하도록 DM 소프트웨어에 지시(412)한다. DM 워크스테이션(402)이 인가 서버에 접촉하여 인가 토큰을 획득한다. 인가 토큰은 캐시될 수도 있고 그리고/또는 오프라인 소스로부터 로딩될 수도 있다. 다음에, 보안 수퍼바이저(404)가 요청(414)을 인가(416)할 수 있으며, 페르소나 업데이트(418)가 진행될 수 있다. 일부 구현들에서, DM 소프트웨어는 유효 인가 토큰이 존재하지 않는다면 운영자(400)에게 경고하고 업데이트 프로세스의 수행을 거부할 것이다.

[0059] [67] DM 워크스테이션(402)은 보안 엘리먼트(406)를 언로크하는 데 사용될 수 있는 공유 비밀 키를 포함한다. 공유 비밀 키에 의해 제공된 인증을 사용하여, 인가된 페르소나와 관련된 저장소 암호 키들만이 보안 엘리먼트(406)로부터 리트리브될 수도 있다. 다음에, 모바일 통신 디바이스(10)는 인가 토큰을 확인하여 운영자(400)가 요청된 동작을 수행할 특권들을 가짐을 검증한다. 보안 엘리먼트(406)에 의해 사용자가 인증(420)되고, 운영자(400)가 적절한 크리덴셜들을 갖지 않는다면 동작이 중단된다.

[0060] [68] DM 소프트웨어는 다음에, 모바일 통신 디바이스(10)로부터의 페르소나의 디바이스 지오메트리 데이터를 요청(422)한다. 디바이스 지오메트리 데이터는 페르소나의 OS 및 TEE 컴포넌트들의 크기를 포함할 수도 있지만, 이에 한정되는 것은 아니다. 페르소나 지오메트리가 디바이스 지오메트리와 매칭한다면 소프트웨어 업데이트가 진행되고, 미스매칭이 있다면 소프트웨어 업데이트가 중단되고 에러가 표시된다. 대안적인 구현에서, 페르소나 소유자가 업데이트의 호환성을 검증할 수 있도록 개정 번호의 페르소나 소유 패키지들이 또한 제공될 수도 있다.

[0061] [69] DM 소프트웨어는 업데이트될 소프트웨어를 모바일 통신 디바이스(10)에 송신(424)함으로써 로딩 프로세스를 시작한다. 한 구현에서, 페르소나의 구성이 업데이트에 포함된다면 페르소나의 구성을 송신(426)함으로써 소프트웨어 업데이트가 시작된다. 다음에, 보안 수퍼바이저(404)가 구성 파일의 지오메트리, 신뢰 루트 및 서명을 검사하고 평가하여 모바일 통신 디바이스(10) 상에 이미 로딩된 다른 구성 파일들과 충돌이 발생할지 여부를 결정한다. 구성 파일이 승인(428)된다면 그리고/또는 구성 파일이 업데이트되고 있지 않다면 소프트웨어 업데이트가 진행되고, 구성 파일들 간에 충돌이 있다면 소프트웨어 업데이트가 중단된다. 또한, 업데이트된 운영 시스템 및/또는 신뢰할 수 있는 실행 환경이 모바일 통신 디바이스(10)에 로딩(430, 432)될 수도 있다.

[0062] [70] 송신된 소프트웨어 업데이트들은 플래시 메모리(408) 상에 저장되고 신뢰 앵커와 비교하여 승인된다. 다음에, 페르소나 트랜지션 파일이 생성(434)되어 어떤 소프트웨어가 업데이트될지를 표시하고, 소프트웨어가

플래시(408)에 작성되고, 각각의 업데이트 이후 트랜지션 파일에 체크포인트가 생성된다. 예를 들어, 플래시(408)에 새로운 구성 파일이 작성(436)되고 트랜지션 파일이 체크포인트(438)되며, 새로운 페르소나 OS 파일시스템이 플래시(408)에 작성(440)되고 트랜지션 파일이 체크포인트(442)되며, 새로운 페르소나 TEE 파일시스템이 플래시(408)에 작성(444)되고 트랜지션 파일이 체크포인트(446)된다. 예시적인 구현에서, 타깃 플래시 파일시스템들은 이전에 저장된 메모리 콘텐츠로부터 프로그래밍되고, 구성 파일로부터의 저장소 키들을 사용하여 양도 중에 암호화된다. 업데이트가 완료된 후, 버퍼 데이터가 플래시(408)에 플러시(448)되고, 페르소나 트랜지션 파일이 삭제(450)되며, 모바일 통신 디바이스(10)가 재부팅(452)된다.

[0063] [71] 도 8은 모바일 통신 디바이스(10)에 사용될 수 있는 페르소나의 소유권을 트랜지션하는 예시적인 방법의 흐름도이다. 모바일 통신 디바이스(10) 상에 로딩된 페르소나의 소유권은 페르소나 데이터를 업데이트하지 않고 새로운 소유자에게 트랜지션될 수도 있다. 예시적인 구현에서, 새로운 소유자가 디바이스 매니저(DM)(새로운 RoT)(502) 내에 양도 티켓을 생성(510)한다. 양도 티켓은 트랜지션될 특정 디바이스 및 예상되는 현재 신뢰 루트를 상술하는 데이터의 블록일 수도 있다. 다음에, 데이터의 블록이 현재 페르소나 소유자에게 전송되고, 현재 페르소나 소유자는 현재 페르소나 소유자 DM(새로운 RoT) (502) 내의 정보를 검증한다.

[0064] [72] 다음에, 현재 페르소나 소유자를 대리하는 운영자(500)는, 페르소나를 양도하도록 DM(구 RoT)(503)에 의해 운영자 및 현재 페르소나 소유자가 인가(512, 514)되는지 여부를 표시하는 인가 토큰을 획득한다. 다음에, 인가 토큰이 양도 티켓에 첨부되어 양도 티켓을 서명하고, 서명된 양도 티켓이 플래시(508)로 양도되어 저장(516)된다. 서명된 양도 티켓은 또한 보안 엘리먼트(506) 내의 페르소나 슬롯에 대한 인증 키와 함께 장래의 새로운 페르소나 소유자에게 리턴될 수도 있다. 이러한 구현에서, 인증 키는 양도 티켓에 부착되는 새로운 페르소나 소유자의 DM 운영자 공개 키를 사용하여 랩핑될 수도 있다. 다음에, 새로운 페르소나 소유자를 대리하는 운영자가 랩핑된 양도 티켓을 사용하여 양도 프로세스를 시작할 수 있다. 보다 구체적으로, 모바일 통신 디바이스(10)는 새로운 페르소나 소유자의 크리덴셜들을 검증하고 양도를 인가할 수 있다.

[0065] [73] 다음에, 운영자(500)는 DM(새로운 RoT)(502)의 워크스테이션에서부터 모바일 통신 디바이스(10)까지 USB 케이블을 연결한다. 디바이스 관리 소프트웨어가 실행되고, 운영자(500)는 모바일 통신 디바이스(10)에 재부팅(518)을 지시한다. 재부팅(518) 동안, 모바일 통신 디바이스(10)는 USB 접속을 검출하여 페르소나 운영 시스템들이 로딩하지 않도록 프로그래밍 모드에 진입한다. 다음에, 운영자(500)는 현재 페르소나 소유자에 의해 소유된 페르소나를 새로운 페르소나 소유자로 트랜지션하도록 DM 소프트웨어에 명령한다. 양도 티켓은 인가에 필요한 정보, 및 트랜지션된 페르소나의 이전 소유자에 대한 신뢰 루트로 서명된 요청을 인증하는 역할을 하는 운영자(500)의 공개 키 기반구조(PKI: public key infrastructure) 인증서를 포함한다.

[0066] [74] DM 소프트웨어는 운영자(500)의 비밀 키를 사용하여 양도 티켓으로부터의 인증 키를 언랩핑한다. 다음에, 인증 키가 사용(520)되어 페르소나 양도를 요청(522)하고, 모바일 통신 디바이스(10) 상의 보안 엘리먼트(506)를 언로크하도록 운영자를 인증(524)할 수도 있다. 이러한 구현에서, 인증(524)은 단지 인가된 페르소나와 관련된 저장소 암호 키들만이 보안 엘리먼트(506)로부터 리트리브될 수 있게 한다.

[0067] [75] 트랜지션은 추가로, 구 페르소나 자산 해시들을 DM(502)에 양도(530)하는 것을 포함한다. DM(502)은 서명들을 검증하고, 관련 자산들을 서명하도록 인가되는 새로운 페르소나 서명 키로 해시들을 다시 서명한다. 또한, 페르소나 미디어 키들에 대한 접근을 허용하는 페르소나 키가 변경되고, 새로운 값이 DM(502)으로 양도된다. 다음에, 대체 서명들이 DM(502)에서 모바일 통신 디바이스(10)로 양도(532)되고, 모바일 통신 디바이스(10)는 서명들을 승인하고 페르소나 자산들에 대한 구 서명들을 새로운 서명들로 대체한다.

[0068] [76] 다음에, 페르소나 트랜지션 파일이 생성(534)되고, 페르소나에 대한 구성 파일이 유효성에 관해 체크되며 이미 모바일 통신 디바이스(10) 상에 로딩된 다른 구성 파일들과 충돌한다. 구성 파일이 승인된다면 프로세스가 진행되고, 구성 파일들 간에 충돌이 있다면 소프트웨어 업데이트가 중단된다. 인가시 사용자 페르소나 인증이 업데이트(536)되어, 미디어 키들이 새로운 신뢰 루트에 의해 접근되고 DM(502)으로 리턴(538)될 수 있게 진행한다.

[0069] [77] DM(502)은 업데이트되고 있는 자산들을 서명하고, 서명된 해시들을 리턴한다. 예를 들어, 업데이트되고 있는 자산들은 다시 서명된 해시들로 업데이트되는 서명들을 가질 수도 있고 그리고/또는 새로운 서명들로 업데이트(542)될 수도 있다. 각각의 업데이트 이후 페르소나 트랜지션 파일이 체크포인트(540)되어 프로세스가 중단된 업데이트에서부터 재시작될 수 있게 한다. 업데이트가 완료된 후, 버퍼 데이터가 플래시(508)로 플러시(544)되고, 페르소나 트랜지션 파일이 삭제(546)되며, 모바일 통신 디바이스(10)가 재부팅(548)된다.

[0070] [78] 페르소나 소유권이 새로운 페르소나 소유자에게 양도된 후, 이전 페르소나 소유자와 신뢰 관계를 갖고 있던 임의의 페르소나들과 트랜지션된 페르소나 사이에 새로운 신뢰 관계가 구축될 필요가 있을 수도 있다. 보다 구체적으로, 모바일 통신 디바이스(10) 상에서 작동하는 다른 페르소나들의 페르소나 구성은 새로운 페르소나 소유자와 신뢰 관계를 구축하여 이전 페르소나 소유자와 동일한 기능을 유지하도록 업데이트되어야 할 수도 있다.

[0071] [79] 도 9는 모바일 통신 디바이스(10)에 사용될 수 있는 새로운 페르소나를 로딩하는 예시적인 방법의 흐름도이다. 예시적인 구현에서, 운영자(600)는 디바이스 매니저(DM) 워크스테이션(602)에서부터 모바일 통신 디바이스(10)까지 USB 케이블을 연결한다. 디바이스 관리 소프트웨어가 실행되고 운영자(600)는 모바일 통신 디바이스(10)에 재부팅을 지시(612)한다. 재부팅(612) 동안, 모바일 통신 디바이스(10)는 USB 접속을 검출하여, 페르소나 운영 시스템들이 로딩하지 않도록 프로그래밍 모드에 진입한다. 운영자(600)는 다음에, 디바이스 소유자가 보유하는 디바이스 패스워드로 USB 접속을 인가하도록 프롬프트(614)되며, 디바이스 패스워드가 입력(616)되고 인증(618)되어 보안 엘리먼트(606)를 언로크한다. 대안적인 구현에서, 모바일 통신 디바이스(10)는 다시 초기화되어 공장 구성으로 리셋될 수도 있다.

[0072] [80] DM 소프트웨어는 다음에, 모바일 통신 디바이스(10)로부터의 페르소나의 디바이스 지오메트리 데이터를 요청(620)하고, 운영자(600)는 페르소나 패키지를 특정 페르소나 슬롯에 로딩(622)하도록 DM 워크스테이션(602)에 지시한다. 디바이스 지오메트리 데이터는 페르소나의 OS 및 TEE 컴포넌트들의 크기를 포함할 수도 있지만, 이에 한정되는 것은 아니다. 페르소나 지오메트리가 디바이스 지오메트리와 매칭한다면 소프트웨어 업데이트가 진행되고, 미스매칭이 있다면 소프트웨어 업데이트가 중단되고 에러가 표시된다. 대안적인 구현에서, 페르소나 소유자가 업데이트의 호환성을 검증할 수 있도록 개정 번호의 페르소나 소유 패키지들이 또한 제공될 수도 있다.

[0073] [81] DM 소프트웨어는 모바일 통신 디바이스(10)에 로딩될 소프트웨어를 송신함으로써 로딩 프로세스를 시작한다. 한 구현에서, 페르소나의 구성 파일을 모바일 통신 디바이스(10)에 송신(624)함으로써 소프트웨어 로딩이 시작된다. 다음에, 보안 수퍼바이저(604)가 구성 파일의 지오메트리, 신뢰 루트 및 서명을 검사하고 평가하여 모바일 통신 디바이스(10) 상에 이미 로딩된 다른 구성 파일들과 충돌이 발생할지 여부를 결정한다. 구성 파일이 승인(626)된다면 소프트웨어 로딩이 진행되고, 구성 파일들 간에 충돌이 있다면 소프트웨어 로딩이 중단된다. 일부 구현들에서, 새로운 페르소나 OS 및 새로운 TEE가 모바일 통신 디바이스(10)에 로딩(628, 630)된다.

[0074] [82] 송신된 소프트웨어는 플래시 메모리(608) 상에 저장되고 신뢰 앵커와 비교하여 승인된다. 다음에, 페르소나 트랜지션 파일이 생성(632)되어 중복 기재를 표시하도록 작성된다. 중복 기재 표시는 업데이트 프로세스가 중단된다면 적절한 복구 조치들이 취해져 실패로부터 복구될 수 있도록 지속적인 방식으로 작성되는 센티널(sentinel) 값이다. 보다 구체적으로, 페르소나에 대한 보안 엘리먼트(606) 내의 저장소 미디어 키들이 삭제(634)되고, 구 페르소나 구성 파일이 소거(636)되고, 페르소나 플래시 파일시스템들이 소거(638)되며, 신뢰할 수 있는 플랫폼 모듈(TPM)(610)이 강제로 클리어(forceclear)(640)된다.

[0075] [83] 다음에, 지속적인 방식으로 모바일 통신 디바이스(10)에 새로운 페르소나가 로딩될 수 있다. 보다 구체적으로, 새로운 구성 파일이 플래시(608)에 작성(642)되고, 보안 수퍼바이저(604)에 의해 사용자 인증 데이터가 판독(644)되며, 사용자가 인증(646)되어 보안 엘리먼트(606)를 언로크한다. 다음에, 개인, 공개 키 쌍의 공개 암호 키(PEK)가 생성(648)되어 보안 엘리먼트(606)로부터 페르소나 소유자에게 내보내(650)질 수 있다. 페르소나 소유자는 자신의 인증서 권한으로 PEK를 서명하고, 구성 파일이 승인(652)된다면 소프트웨어 로딩(654)이 진행된다. 다음에, PEK가 보안 엘리먼트(606)에 리턴되어 저장(656)된다.

[0076] [84] PEK 개인, 공개 키 쌍의 비밀 키가 보안 엘리먼트(606)로부터 내보내지지 않도록 이는 보안 엘리먼트(606) 내에 저장되어 보호된다. 이는 페르소나 소유자가 개인 키에 의해 서명된 응답에 의해, 서비스를 수행하기 위한 요청이 인가된 디바이스로부터 왔음을 검증할 수 있게 한다. PEK는 페르소나 소유권이 정의될 때 생성될 수 있으며 예를 들어, 소프트웨어 업데이트, 요청 및/또는 패키지를 인증하는 데 사용될 수도 있다. 대안적인 구현에서, 페르소나 소유자가 특정 디바이스를 타깃으로 하는 데이터를 암호화할 수 있도록 그리고 다른 디바이스들이 데이터를 복호화하는 것이 불가능하도록 제 2 개인, 공개 키 쌍이 생성되어 암호화에 사용될 수도 있다.

[0077] [85] 다음에, 새로운 페르소나 OS 파일시스템이 플래시(608)에 작성(658)되고, 새로운 페르소나 TEE 파일시스템이 플래시(608)에 작성(660)되고, 새로운 페르소나 데이터 분할이 생성(662)된다. 타깃 플래시 파일시스템

들은 이전에 저장된 메모리 콘텐츠로부터 프로그래밍되고, 구성 파일로부터의 저장소 키들을 사용하여 양도 중에 암호화된다. 업데이트가 완료된 후, 페르소나 트랜지션 파일이 삭제(664)되며, 모바일 통신 디바이스(10)가 재부팅(666)된다.

[0078] [86] 또한, 본 개시는 다음 조항들에 따른 실시예들을 포함한다:

[0079] 조항 1. 비-일시적 컴퓨터 판독 가능 매체가, 복수의 동작 상태들을 가지며 프로세서, 하우징 및 하우징에 연결된 입력 디바이스를 포함하는 모바일 통신 디바이스를 작동시키기 위한 컴퓨터 실행 가능 명령들을 저장하며, 컴퓨터 실행 가능 명령들은 프로세서로 하여금,

[0080] 입력 디바이스가 작동될 때 모바일 통신 디바이스의 동작 상태를 변경하는 것과 검증하는 것 중 적어도 하나를 하게 하고; 그리고

[0081] 모바일 통신 디바이스의 동작 상태를 기초로 사용자에게 피드백을 제공하도록 표시자를 활성화하게 한다.

[0082] 조항 2. 조항 1에 따른 비-일시적 컴퓨터 판독 가능 매체는 프로세서로 하여금,

[0083] 모바일 통신 디바이스 상에서 작동하는 페르소나들 사이에서 모바일 통신 디바이스의 포커스를 트랜지션하게 하는 컴퓨터 실행 가능 명령들을 더 포함한다.

[0084] 조항 3. 조항 1에 따른 비-일시적 컴퓨터 판독 가능 매체는 프로세서로 하여금,

[0085] 제 1 페르소나에 포커스가 맞춰지면 제 1 시각적 표시자를 활성화하게 하고; 그리고

[0086] 제 2 페르소나에 포커스가 맞춰지면 제 2 시각적 표시자를 활성화하게 하는 컴퓨터 실행 가능 명령들을 더 포함한다.

[0087] 조항 4. 조항 1에 따른 비-일시적 컴퓨터 판독 가능 매체는 프로세서로 하여금,

[0088] 모바일 통신 디바이스에 사용자 크리덴셜들을 입력하기 위한 응답을 요청하면서 신뢰 루트 정보를 디스플레이하게 하는 컴퓨터 실행 가능 명령들을 더 포함한다.

[0089] 조항 5. 조항 1에 따른 비-일시적 컴퓨터 판독 가능 매체는 프로세서로 하여금,

[0090] 입력 디바이스가 작동될 때 모바일 통신 디바이스에 대해 사용자의 물리적 존재를 증명하게 하는 컴퓨터 실행 가능 명령들을 더 포함한다.

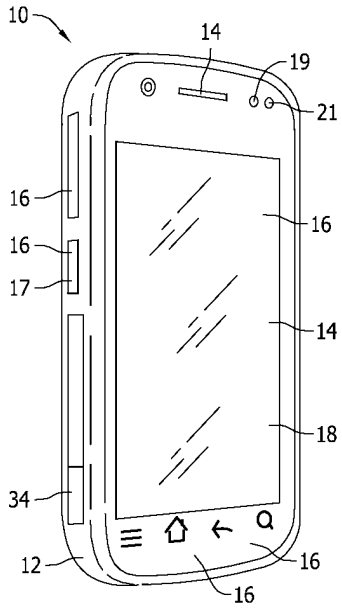
[0091] 조항 6. 조항 1에 따른 비-일시적 컴퓨터 판독 가능 매체는 프로세서로 하여금,

[0092] 모바일 통신 디바이스 상에서 작동하는 신뢰할 수 없는 코드로부터 입력 디바이스 및 표시자가 접근 불가능하도록 입력 디바이스 및 표시자를 격리시키게 하는 컴퓨터 실행 가능 명령들을 더 포함한다.

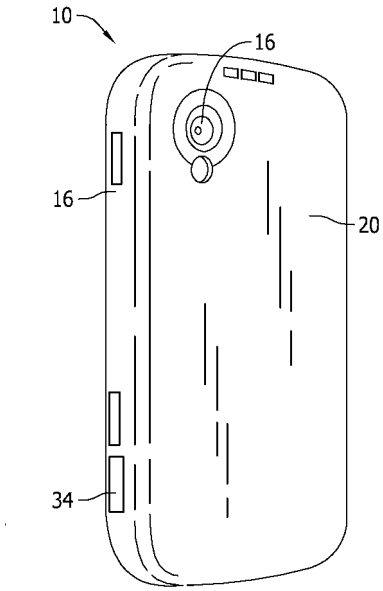
[0093] [87] 이러한 서면 기술은 최선 모드를 포함하는 다양한 구현들을 개시하기 위해 그리고 또한 해당 기술분야에서 통상의 지식을 가진 임의의 자가 임의의 디바이스들 또는 시스템들을 제작하여 사용하고 임의의 통합된 방법들을 수행하는 것을 비롯해 다양한 구현들을 실시할 수 있게 하기 위해 예들을 사용한다. 본 개시의 특허 가능 범위는 청구항들에 의해 정의되고, 해당 기술분야에서 통상의 지식을 가진 자들에게 일어나는 다른 예들을 포함할 수도 있다. 그러한 다른 예들은 그들이 청구항들의 문언과 다르지 않은 구조적 엘리먼트들을 갖는다면, 또는 그들이 청구항들의 문언과 사소한 차이들을 갖는 동등한 구조적 엘리먼트들을 포함한다면, 청구항들의 범위 내에 있는 것으로 의도된다.

도면

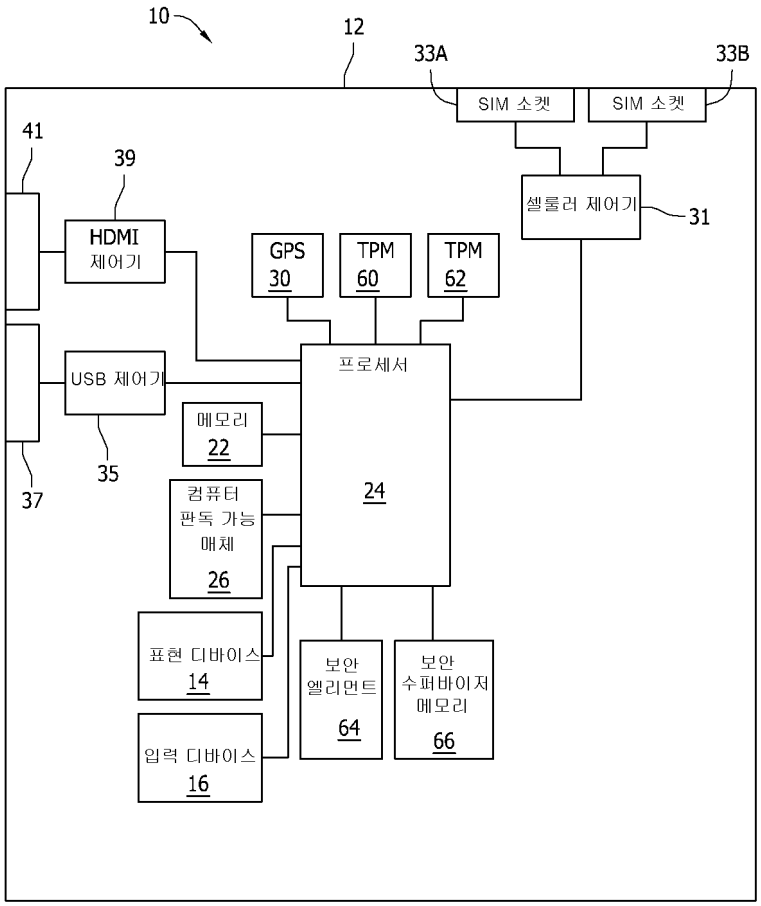
도면1



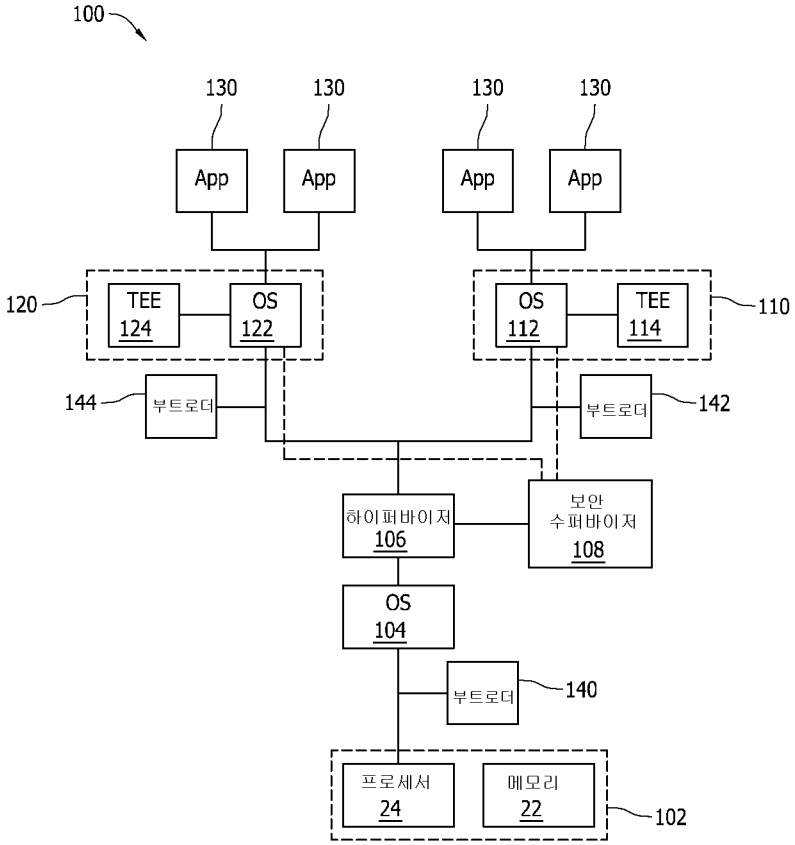
도면2



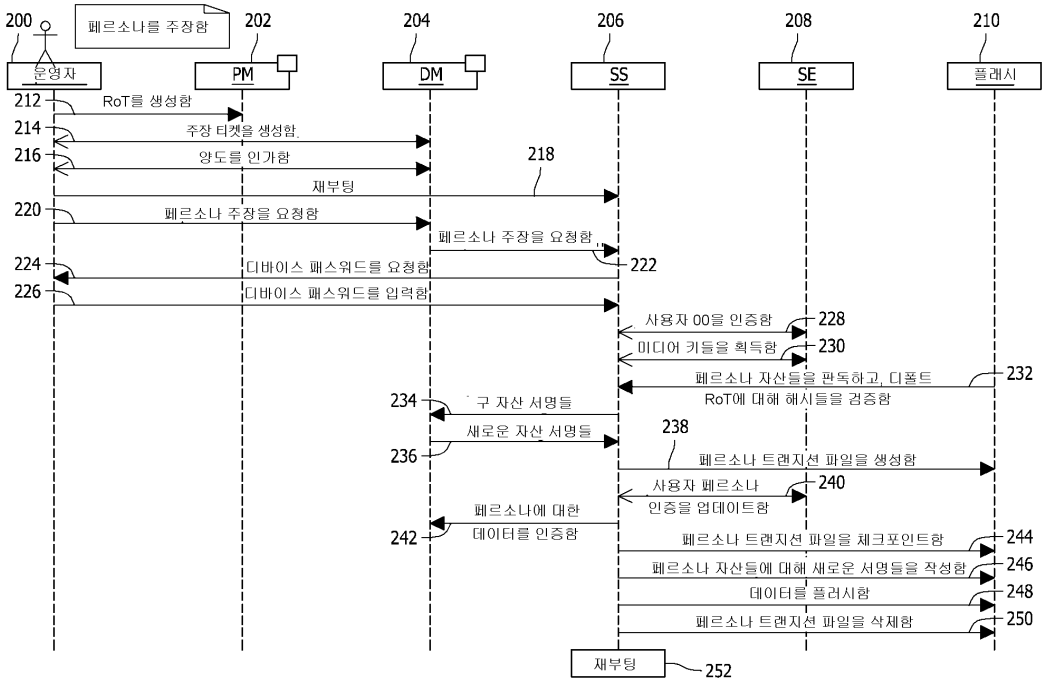
도면3


10
12
33A
33B
SIM 소켓
SIM 소켓
41
39
셀룰러 제어기
31
HDMI
제어기
GPS
30
TPM
60
TPM
62
프로세서
24
USB 제어기
메모리
22
35
37
컴퓨터
판독 가능
매체
26
표현 디바이스
14
보안
엘리먼트
64
보안
수퍼바이저
메모리
66
입력 디바이스
16

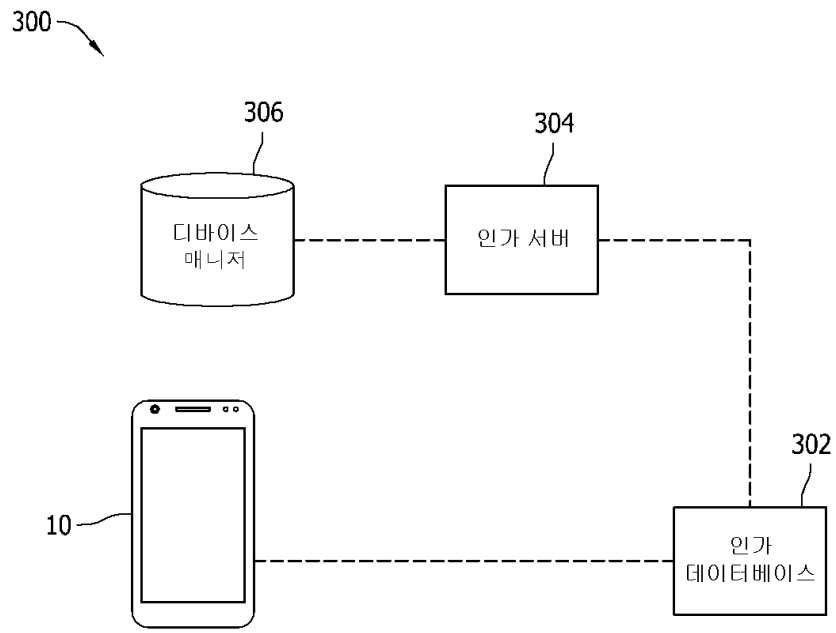
도면4


100
130
130
130
130
App
App
App
App
120
TEE
124
OS
122
OS
112
TEE
114
110
144
부트로더
부트로더
142
하이퍼바이저
106
보안
수퍼바이저
108
OS
104
부트로더
140
프로세서
24
메모리
22
102

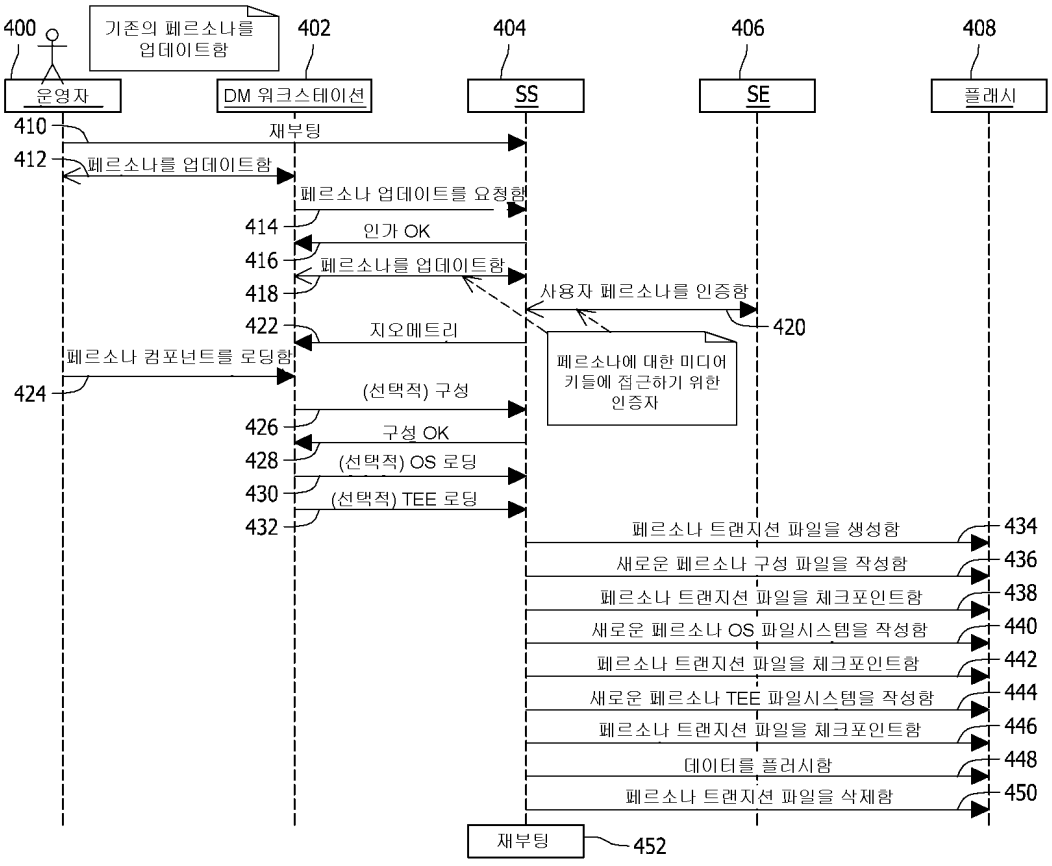
도면5


200
운영자
페르소나를 주장함
202
PM
204
DM
206
SS
208
SE
210
플래시
212
RoT를 생성함
214
주장 티켓을 생성함
216
양도를 인가함
218
재부팅
220
페르소나 주장을 요청함
222
페르소나 주장을 요청함
224
디바이스 패스워드를 요청함
226
디바이스 패스워드를 입력함
228
사용자 00을 인증함
230
미디어 키들을 획득함
232
페르소나 자산들을 판독하고, 디폴트
RoT에 대해 해시들을 검증함
234
구 자산 서명들
236
새로운 자산 서명들
238
페르소나 트랜지션 파일을 생성함
240
사용자 페르소나
인증을 업데이트함
242
페르소나에 대한
데이터를 인증함
244
페르소나 트랜지션 파일을 체크포인트함
246
페르소나 자산들에 대해 새로운 서명들을 작성함
248
데이터를 플러시함
250
페르소나 트랜지션 파일을 삭제함
재부팅
252

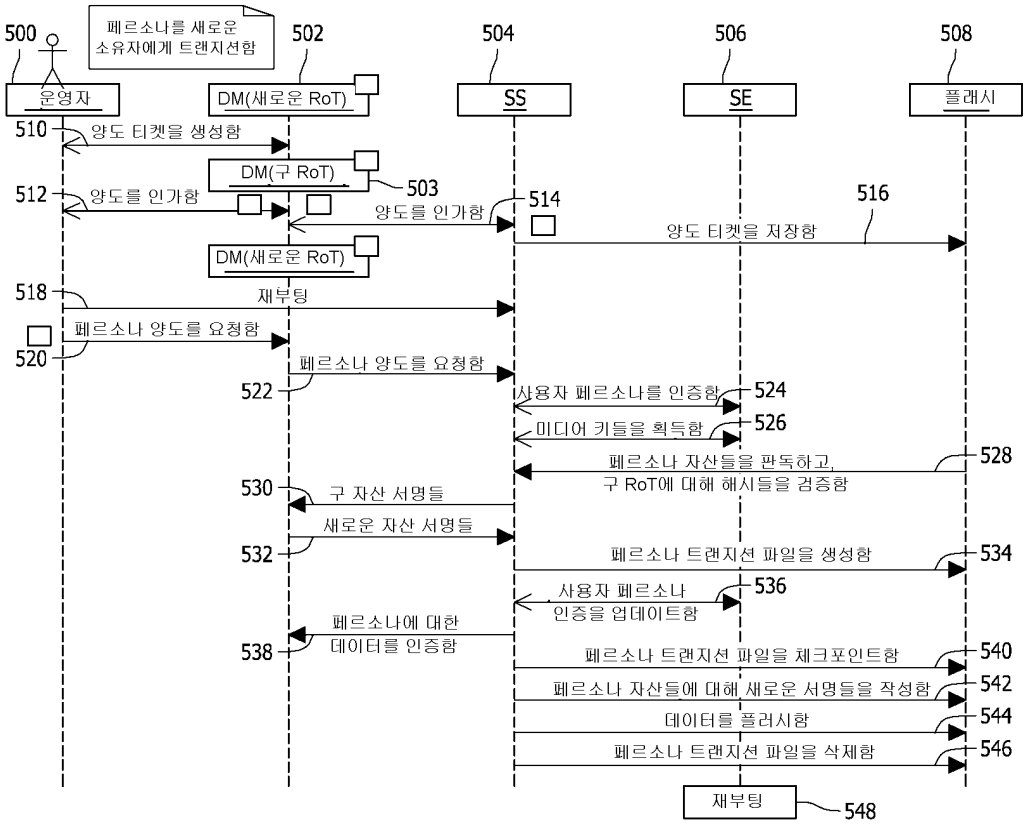
도면6


300
306
디바이스
매니저
304
인가 서버
10
302
인가
데이터베이스

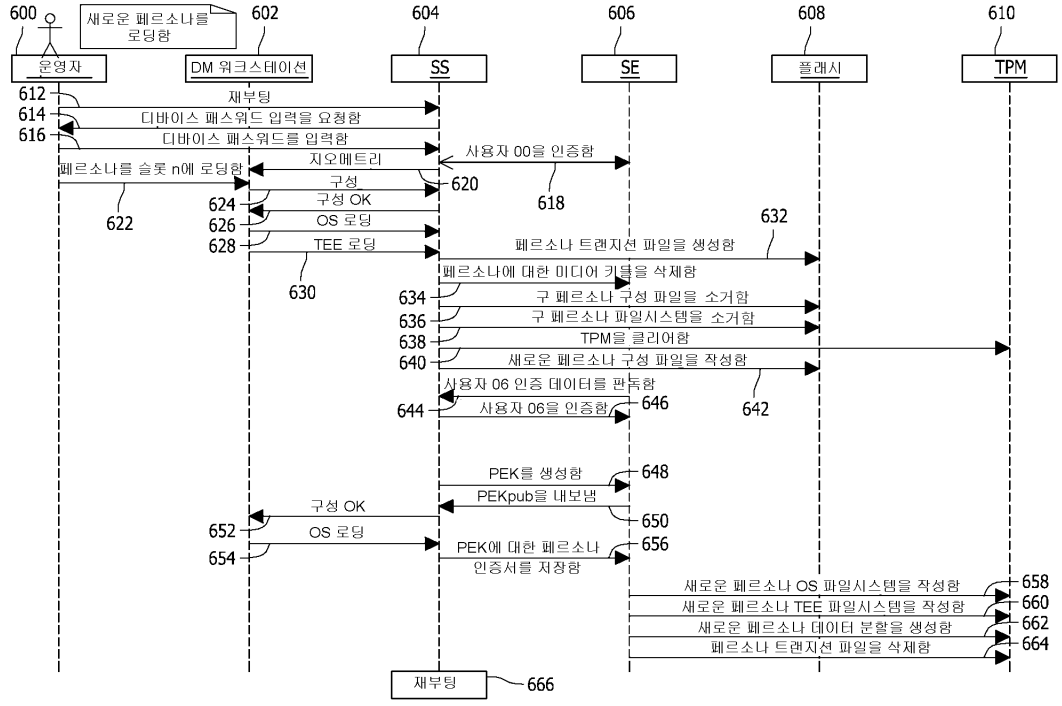
도면7


400
운영자
기존의 페르소나를
업데이트함
402
DM 워크스테이션
404
SS
406
SE
408
플래시
410
재부팅
412
페르소나를 업데이트함
페르소나 업데이트를 요청함
414
인가 OK
416
페르소나를 업데이트함
418
사용자 페르소나를 인증함
420
422
지오메트리
페르소나에 대한 미디어
키들에 접근하기 위한
인증자
페르소나 컴포넌트를 로딩함
424
(선택적) 구성
426
구성 OK
428
(선택적) OS 로딩
430
(선택적) TEE 로딩
432
페르소나 트랜지션 파일을 생성함
434
새로운 페르소나 구성 파일을 작성함
436
페르소나 트랜지션 파일을 체크포인트함
438
새로운 페르소나 OS 파일시스템을 작성함
440
페르소나 트랜지션 파일을 체크포인트함
442
새로운 페르소나 TEE 파일시스템을 작성함
444
페르소나 트랜지션 파일을 체크포인트함
446
데이터를 플러시함
448
페르소나 트랜지션 파일을 삭제함
450
재부팅
452

도면8


500
운영자
페르소나를 새로운 소유자에게 트랜지션함
502
DM(새로운 RoT)
504
SS
506
SE
508
플래시
510
양도 티켓을 생성함
DM(구 RoT)
503
512
양도를 인가함
양도를 인가함
514
516
양도 티켓을 저장함
DM(새로운 RoT)
518
재부팅
페르소나 양도를 요청함
520
페르소나 양도를 요청함
522
사용자 페르소나를 인증함
524
미디어 키들을 획득함
526
페르소나 자산들을 판독하고,
구 RoT에 대해 해시들을 검증함
528
530
구 자산 서명들
새로운 자산 서명들
532
페르소나 트랜지션 파일을 생성함
534
사용자 페르소나
인증을 업데이트함
536
페르소나에 대한
데이터를 인증함
538
페르소나 트랜지션 파일을 체크포인트함
540
페르소나 자산들에 대해 새로운 서명들을 작성함
542
데이터를 플러시함
544
페르소나 트랜지션 파일을 삭제함
546
재부팅
548

도면9


600
운영자
새로운 페르소나를 로딩함
602
DM 워크스테이션
604
SS
606
SE
608
플래시
610
TPM
612
재부팅
614
디바이스 패스워드 입력을 요청함
616
디바이스 패스워드를 입력함
지오메트리
사용자 00을 인증함
618
페르소나를 슬롯 n에 로딩함
구성
620
622
624
구성 OK
626
OS 로딩
628
TEE 로딩
630
632
페르소나 트랜지션 파일을 생성함
페르소나에 대한 미디어 키들을 삭제함
634
구 페르소나 구성 파일을 소거함
636
구 페르소나 파일시스템을 소거함
638
TPM을 클리어함
640
새로운 페르소나 구성 파일을 작성함
642
사용자 06 인증 데이터를 판독함
644
사용자 06을 인증함
646
PEK를 생성함
648
PEKpub을 내보냄
650
구성 OK
652
OS 로딩
654
PEK에 대한 페르소나
인증서를 저장함
656
새로운 페르소나 OS 파일시스템을 작성함
658
새로운 페르소나 TEE 파일시스템을 작성함
660
새로운 페르소나 데이터 분할을 생성함
662
페르소나 트랜지션 파일을 삭제함
664
재부팅
666