(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년04월09일
(11) 등록번호 10-1252921
(24) 등록일자 2013년04월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/22 (2006.01) *G06F 13/14* (2006.01)
(21) 출원번호 10-2010-7022126
(22) 출원일자(국제) 2009년03월02일
심사청구일자 2010년10월04일
(85) 번역문제출일자 2010년10월04일
(65) 공개번호 10-2010-0126472
(43) 공개일자 2010년12월01일
(86) 국제출원번호 PCT/US2009/035755
(87) 국제공개번호 WO 2009/111411
국제공개일자 2009년09월11일
(30) 우선권주장
61/033,728 2008년03월04일 미국(US)
(56) 선행기술조사문헌
WO2006101549 A2
전체 청구항 수 : 총 13 항

(73) 특허권자
애플 인크.
미합중국 95014 캘리포니아 쿠퍼티노 인피니트 루프 1
(72) 발명자
드 아틀리, 달라스
미국 94114 캘리포니아주 샌 프란시스코 17번 스트리트 넘버2 4508
판더, 헤이코
미국 94114 캘리포니아주 샌 프란시스코 17번 스트리트 4347
(뒷면에 계속)
(74) 대리인
백만기, 양영준

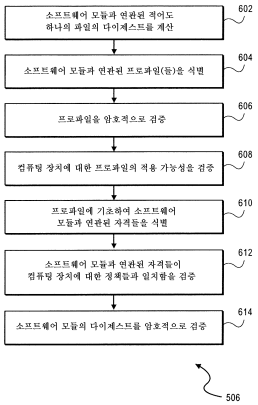
심사관 : 이강하

(54) 발명의 명칭 **사업자에게 부여된 자격들에 기초하여 장치 내의 소프트웨어 코드의 실행을 인가하는 시스템 및 방법**

(57) 요 약

실시예들은 적어도 하나의 사업자 프로파일에 기초하여 보안 동작 환경에서 소프트웨어 코드가 실행되거나 능력들을 액세스하도록 인가하기 위한 시스템들 및 방법들을 포함한다. 다른 주체들에 대해 신뢰를 확장하도록 신뢰 주체들에 의해 사업자 프로파일들이 발행되어 이러한 다른 주체들이 특정한 컴퓨팅 장치들과 같은 보안 동작 환경에서 애플리케이션들을 제공하거나 그 실행을 제어하도록 허용할 수 있다. 사업자 프로파일들은 신뢰 인가 기관에 의한 각각의 배포의 재인가 없이 주체들이 소프트웨어 코드를 장치에 추가하거나, 또는 다른 주체들에 의해 제어 또는 인가되는 한정된 그룹의 장치들에 추가하도록 허용한다.

대 표 도 - 도6



(72) 발명자

아들러, 미첼

미국 95014 캘리포니아주 쿠퍼티노 파사데나 애비뉴 넘버비3 10090

쿠퍼, 사이몬

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1

브로워, 마이클

미국 95136 캘리포니아주 산 호세 레드 리버 웨이 141

레다, 매트

미국 95118 캘리포니아주 산 호세 델란트 테라스 1599

특허청구의 범위

청구항 1

소프트웨어를 인가하는 컴퓨터화된 방법으로서,

전자 장치상에 저장된 소프트웨어 모듈을 시험하기 위해 상기 소프트웨어 모듈을 실행하도록 하는 요청을, 프로세서상에서 실행 중인 운영 체제의 신뢰 공간에서 실행되는 커널에 의해 수신하는 단계 - 상기 신뢰 공간은 상기 프로세서의 시동시 상기 커널의 인증에 의해 수립됨 - ;

상기 커널에 의해, 상기 소프트웨어 모듈을 나타내는 데이터를, 상기 프로세서상에서 실행 중인 상기 운영 체제의 비신뢰 공간에서 실행되는 정책 서비스에 대해 통신(communicating)하는 단계 - 상기 비신뢰 공간은 상기 신뢰 공간이 아닌 나머지 공간의 적어도 일부임 - ;

상기 정책 서비스에 의해, 상기 소프트웨어 모듈에 대한 실행 가능 명령어들의 적어도 일 부분으로부터 생성된 다이제스트(digest)를 획득하는 단계;

상기 정책 서비스에 의해, 이동 네트워크 서비스 공급자(mobile network service provider)에 대한 적어도 하나의 프로파일을 식별하는 단계 - 상기 적어도 하나의 프로파일은, 상기 전자 장치상에서 실행되는 소프트웨어에 대하여 상기 이동 네트워크 서비스 공급자에 의해 허용되는 동작들의 유형을 나타내는 자격 데이터를 포함함 - ;

상기 정책 서비스에 의해, 상기 이동 네트워크 서비스 공급자에 대한 상기 적어도 하나의 프로파일을 인증하는 단계;

상기 정책 서비스에 의해, 상기 이동 네트워크 서비스 공급자의 상기 프로파일과 연관된 상기 자격 데이터와 상기 다이제스트에 적어도 부분적으로 기초하여, 상기 소프트웨어 모듈과 연관된 적어도 하나의 자격을 인증하는 단계;

상기 정책 서비스에 의해, 상기 적어도 하나의 자격을 상기 커널에 대해 통신하는 단계;

상기 커널에 의해, 상기 적어도 하나의 자격에 기초하여, 상기 프로세서상에서 상기 소프트웨어 모듈에 의한 하나 이상의 유형의 동작의 실행을 허용하는 단계; 및

상기 커널에 의해, 상기 적어도 하나의 자격에 기초하여, 상기 프로세서상에서 상기 소프트웨어 모듈에 의한 하나 이상의 유형의 동작의 실행을 허용하지 않는 단계

를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 소프트웨어 모듈은 애플리케이션 프로그램 또는 공유 라이브러리 중 적어도 하나를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 5

제1항에 있어서,

상기 소프트웨어 모듈을 나타내는 데이터는 상기 소프트웨어 모듈과 연관된 실행 가능 명령어들 중 적어도 일부에 대한 참조를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 다이제스트는 상기 소프트웨어 모듈의 각각의 부분들을 나타내는 복수의 다이제스트 값들에 기초하여 생성되는, 컴퓨터화된 소프트웨어 인가 방법.

청구항 8

제1항에 있어서,

상기 다이제스트는 상기 적어도 일 부분을 나타내는 SHA-1 해시(hash)를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 9

제1항에 있어서,

상기 소프트웨어 모듈의 적어도 하나의 자격을 인증하는 단계는 상기 소프트웨어 모듈의 개발자의 암호화 키에 기초하여 상기 다이제스트의 암호화 서명을 인증하는 단계를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 10

제9항에 있어서,

상기 다이제스트의 암호화 서명을 인증하는 단계는,

상기 개발자의 공개 키에 기초하여 상기 다이제스트의 암호화 서명을 계산하는 단계; 및

상기 계산된 서명을 상기 다이제스트와 연관되어 저장되어 있는 서명과 비교하는 단계

를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 11

제9항에 있어서,

상기 이동 네트워크 서비스 공급자에 대한 상기 적어도 하나의 프로파일은 적어도 하나의 장치 식별자를 나타내는 데이터를 더 포함하고,

상기 소프트웨어 모듈의 상기 적어도 하나의 자격을 인증하는 단계는,

상기 적어도 하나의 프로파일의 상기 적어도 하나의 장치 식별자를 상기 전자 장치의 장치 식별자에 대해 비교하는 단계; 및

상기 비교에 기초하여, 상기 적어도 하나의 자격을 인증하는 단계

를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 12

삭제

청구항 13

제1항에 있어서,

상기 이동 네트워크 서비스 공급자의 상기 적어도 하나의 프로파일을 인증하는 단계는, 신뢰 기관의 암호화 키에 기초하여 상기 적어도 하나의 프로파일을 인증하는 단계

를 포함하는 컴퓨터화된 소프트웨어 인가 방법.

청구항 14

삭제

청구항 15

컴퓨팅 장치로서,

상기 컴퓨팅 장치상에서 실행하기 위한 소프트웨어 모듈을 저장하고, 이동 네트워크 서비스 공급자에 대한 적어도 하나의 프로파일 - 상기 적어도 하나의 프로파일은 상기 이동 네트워크 서비스 공급자에 의해 허용되는 동작들을 나타내는 자격 데이터를 포함함 - 을 저장하도록 구성되는 저장소; 및

적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

상기 소프트웨어 모듈을 실행하도록 하는 요청을, 상기 프로세서상에서 실행 중인 운영 체제의 신뢰 공간에서 실행되는 커널에 의해 수신하고 - 상기 신뢰 공간은 상기 프로세서의 시동시 상기 커널의 인증에 의해 수립됨 - ;

상기 커널에 의해, 상기 소프트웨어 모듈을 나타내는 데이터를, 상기 프로세서상에서 실행 중인 운영 체제의 비신뢰 공간에서 실행되는 정책 서비스에 대해 통신하고 - 상기 비신뢰 공간은 상기 신뢰 공간이 아닌 나머지 공간의 적어도 일부임 - ;

상기 정책 서비스에 의해, 상기 소프트웨어 모듈에 대한 실행 가능 명령어들의 적어도 일 부분으로부터 생성된 다이제스트를 획득하고;

상기 정책 서비스에 의해, 상기 이동 네트워크 서비스 공급자의 상기 적어도 하나의 프로파일을 인증하고;

상기 정책 서비스에 의해, 상기 이동 네트워크 서비스 공급자의 상기 적어도 하나의 프로파일과 연관된 상기 자격 데이터와 상기 다이제스트에 적어도 부분적으로 기초하여, 상기 소프트웨어 모듈과 연관된 적어도 하나의 자격을 인증하고;

상기 정책 서비스에 의해, 상기 적어도 하나의 자격을 상기 커널에 대해 통신하고;

상기 커널에 의해, 상기 적어도 하나의 자격에 기초하여, 상기 소프트웨어 모듈에 의한 하나 이상의 유형의 동작의 실행을 허용하고;

상기 커널에 의해, 상기 적어도 하나의 자격에 기초하여, 상기 소프트웨어 모듈에 의한 하나 이상의 유형의 동작의 실행을 허용하지 않도록 구성된,

컴퓨팅 장치.

청구항 16

삭제

청구항 17

제15항에 있어서,

상기 소프트웨어 모듈은 애플리케이션 프로그램 또는 공유 라이브러리 중 적어도 하나를 포함하는 컴퓨팅 장치.

청구항 18

삭제

청구항 19

제15항에 있어서,

상기 소프트웨어 모듈을 나타내는 데이터는 상기 소프트웨어 모듈과 연관된 실행 가능 명령어들 중 적어도 일부에 대한 참조를 포함하는 컴퓨팅 장치.

청구항 20

전자 장치의 적어도 하나의 프로세서에 의해 실행될 수 있는, 프로세스를 수행하기 위한 코드들을 나타내는 데이터를 포함하는 유형의(tangible) 컴퓨터 판독 가능 저장 매체로서, 상기 프로세스는,

전자 장치상에 저장된 소프트웨어 모듈을 시험하기 위해 상기 소프트웨어 모듈을 실행하도록 하는 요청을, 프로세서상에서 실행 중인 운영 체제의 신뢰 공간에서 실행되는 커널에 의해 수신하는 단계 - 상기 신뢰 공간은 상기 프로세서의 시동시 상기 커널의 인증에 의해 수립됨 - ;

상기 커널에 의해, 상기 소프트웨어 모듈을 나타내는 데이터를, 상기 프로세서상에서 실행 중인 상기 운영 체제의 비신뢰 공간에서 실행되는 정책 서비스에 대해 통신하는 단계 - 상기 비신뢰 공간은 상기 신뢰 공간이 아닌 나머지 공간의 적어도 일부임 - ;

상기 정책 서비스에 의해, 상기 소프트웨어 모듈에 대한 실행 가능 명령어들의 적어도 일 부분으로부터 생성된 다이제스트를 획득하는 단계;

상기 정책 서비스에 의해, 이동 네트워크 서비스 공급자에 대한 적어도 하나의 프로파일을 식별하는 단계 - 상기 적어도 하나의 프로파일은, 상기 전자 장치상에서 실행되는 소프트웨어에 대하여 상기 이동 네트워크 서비스 공급자에 의해 허용되는 동작들의 유형을 나타내는 자격 데이터를 포함함 - ;

상기 정책 서비스에 의해, 상기 이동 네트워크 서비스 공급자에 대한 상기 적어도 하나의 프로파일을 인증하는 단계;

상기 정책 서비스에 의해, 상기 이동 네트워크 서비스 공급자의 상기 프로파일과 연관된 상기 자격 데이터와 상기 다이제스트에 적어도 부분적으로 기초하여, 상기 소프트웨어 모듈과 연관된 적어도 하나의 자격을 인증하는 단계;

상기 정책 서비스에 의해, 상기 적어도 하나의 자격을 상기 커널에 대해 통신하는 단계;

상기 커널에 의해, 상기 적어도 하나의 자격에 기초하여, 상기 프로세서상에서 상기 소프트웨어 모듈에 의한 하나 이상의 유형의 동작의 실행을 허용하는 단계; 및

상기 커널에 의해, 상기 적어도 하나의 자격에 기초하여, 상기 프로세서상에서 상기 소프트웨어 모듈에 의한 하나 이상의 유형의 동작의 실행을 허용하지 않는 단계

를 포함하는 유형의 컴퓨터 판독 가능 저장 매체.

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

명 세 서

기 술 분 야

[0001] 본 출원은 소프트웨어 코드의 실행을 제어하는 것과 관련된다.

배 경 기 술

[0002] 상이한 네트워크 사업자(network carrier)들은 이동 컴퓨팅 장치들이 이들의 각각의 네트워크들 또는 이들이 실행할 수 있는 애플리케이션들과 어떻게 상호 작용할 수 있는지에 관해 종종 상이한 요건들을 갖는다. 이동 컴퓨팅 장치가 올바르게 동작하고 네트워크 정책들을 준수하도록 보장하기 위해, 이동 컴퓨팅 장치는 전형적으로 준비 프로세스(provisioning process)를 거치는데, 이는 사업자의 네트워크 상에서 동작하도록 펌웨어 업데이트(firmware update)를 통해 전화를 구성한다.

[0003] 또한, 종종 이러한 컴퓨팅 장치들은 컴퓨터 시스템 상에서 실행되는 코드가 신뢰 기관(trusted party)에 의해 인가될 것을 요구하도록 구성될 수 있다. 예컨대, 이러한 인가는 컴퓨팅 장치의 무결성이 악성 또는 비인가 코드에 의해 손상되지 않도록 보장하는 것을 돕는 데 사용될 수 있다. 일부 사례들에 있어서, 컴퓨팅 장치들은 컴퓨팅 장치 상에서 실행되도록 하고/하거나 장치의 특정한 자원 또는 서비스를 액세스하는 소프트웨어의 실행을 제어하기 위해 코드가 신뢰 기관에 의해 디지털적으로 서명되고 검증될 것을 요구하도록 구성될 수 있다. 디지털 서명의 검증은 기초가 되는 애플리케이션 코드가 신뢰 인가 기관(trusted authority)에 의해 디지털적으로 서명된 이래로 수정되지 않았음을 보장하는 것을 돕는다.

[0004] 그러나, 이동 장치들은 종종 사업자들이 자신들의 네트워크들 상에서 활용되기를 원하지 않는 능력들을 갖는다. 예컨대, 이동 장치는 블루투스(Bluetooth) 기능을 갖도록 설계될 수 있지만, 사업자는 자신의 사용자들이 그러한 능력을 활용하는 것을 방지하기를 원할 수 있다. 이러한 장치들 상의 다양한 애플리케이션이 또한 제한될 필요가 있을 수 있다. 불행히도, 앞서 언급한 애플리케이션 서명 보안을 이용하는 이동 장치들에 대해 이러한 제한을 강제하기는 어렵다.

도면의 간단한 설명

[0005] 도 1은 소프트웨어 코드가 하나 이상의 사업자로부터 컴퓨팅 장치들로 배포되는 컴퓨팅 환경의 예를 도시하는 블록도.

도 2는 도 1에 도시된 바와 같은 환경 내의 컴퓨팅 장치의 소프트웨어 컴포넌트(software component)들의 일 실시예를 도시하는 블록도.

도 3은 도 2에 도시된 바와 같은 장치 상에서 소프트웨어의 실행을 제어하기 위한 프로파일(profile)의 일 실시예를 도시하는 블록도.

도 4는 도 2에 도시된 바와 같은 컴퓨팅 장치의 일 실시예의 소프트웨어 컴포넌트들 사이의 데이터 흐름을 도시

하는 블록도.

도 5는 도 2에 도시된 바와 같은 프로파일들에 기초하여 소프트웨어를 실행하는 방법의 일 실시예를 도시하는 흐름도.

도 6은 도 5의 방법의 일부를 보다 상세히 도시하는 흐름도.

도 7은 도 2에 도시된 바와 같은 컴퓨팅 장치의 일례를 도시하는 블록도.

도 8a 및 8b는 도 2에 도시된 바와 같은 컴퓨팅 장치의 일례를 도시하는 블록도들.

도 9는 도 8a 및 8b에 도시된 바와 같은 이동 장치의 일 구현예를 도시하는 블록도.

발명을 실시하기 위한 구체적인 내용

[0006] 본 명세서에 기술된 다양한 실시예는 예컨대 강제 사업자 프로파일(enforced carrier profile)에 기초하여 사업자 네트워크들 상에서 컴퓨팅 장치들을 제어하기 위한 시스템들 및 방법들을 제공한다. 일부 사례들에서, 컴퓨팅 장치는 컴퓨팅 장치 상에서 실행되기 위해 코드의 일부 또는 전부가 신뢰 기관에 의해 디지털적으로 서명되고 검증될 것을 요구하도록 구성될 수 있다. 사업자들이 자신들의 프로파일들을 자신들의 네트워크에 접속된 컴퓨팅 장치 상에 설치하도록 할 수 있는 시스템들 및 방법들이 본 명세서에 개시된다. 따라서, 본 명세서에 개시된 시스템들 및 방법들을 사용하여, 사업자들은 이러한 컴퓨팅 장치들에게 프로파일들을 효과적으로 적용할 수 있어, 신뢰받는 애플리케이션들이 또한 사업자의 원하는 정책들을 준수하는 방식으로 장치들 상의 설비들 및 자원들에 대한 액세스를 제어할 수 있다.

[0007] 일부 실시예들에서, 자신의 프로파일이 컴퓨팅 장치 상에 설치되도록 하기 위해, 사업자(또는 그 대표)는 신뢰 인가 기관에게 요청들을 발송할 수 있다. 이러한 요청은 사업자가 장치들이 자신의 네트워크 상에서 동작하는 동안에 갖기를 원하는 액세스 및 기능의 유형들을 지정할 수 있다. 신뢰 인가 기관은 사업자를 위해 사업자 프로파일을 생성할 수 있는데, 이는 사업자의 네트워크 상의 장치들에 대한 사업자의 원하는 네트워크 정책들을 반영하거나, 사업자로 하여금 장치를 적절히 수정할 수 있도록 한다. 액세스 프로파일 및 정책 프로세스는 또한 이러한 사업자 프로파일을 강제하도록 지정된 장치들 상에 제공되고 설치될 수 있다.

[0008] 코드가 장치 상에서 실행되는 경우, 정책 프로세스는 사업자 프로파일에서 지정된 자격(entitlement)들을 검사하여 코드 실행 요청이 허용될 수 있는지 여부를 결정할 수 있다. 사업자 프로파일이 필요한 자격들을 포함하는 경우, 코드는 요청된 데이터 및/또는 시스템 기능을 액세스하도록 허용될 수 있다. 사업자 프로파일이 필요한 자격들을 포함하지 않는 경우, 코드가 장치 상의 소정의 데이터 및/또는 기능을 액세스하는 능력이 제한될 수 있다.

[0009] 본 발명의 실시예들을 예시하기 위해, 이제 도 1 내지 7이 아래에 제시될 것이다. 도 1은 실시예들이 구현될 수 있는 전체 시스템 도면을 도시한다. 도 2 및 3은 소프트웨어의 실행을 제어하기 위한 소프트웨어 컴포넌트들 및 예시적인 프로파일의 실시예들을 도시한다. 도 4는 소프트웨어 컴포넌트들 사이의 데이터 흐름의 일례를 도시한다. 이후 도 5 및 6은 프로파일들에 기초하여 소프트웨어를 실행하기 위한 프로세스 흐름도들을 도시한다. 도 7은 이동 컴퓨팅 장치의 일례를 도시하도록 제공된다. 이러한 도면들은 이제 도 1을 참조하는 것에서부터 시작하여 아래에 더 기술될 것이다.

[0010] 도 1은 본 명세서에 기술된 다양한 실시예를 실시하는 데 적합한 환경의 예이다. 도시된 시스템에서, 컴퓨팅 장치들(100)은 신뢰 인가 기관(102)으로부터 제공 또는 제어될 수 있고, 사업자(104)에 의해 동작되는 네트워크를 활용할 수 있다. 이제 이러한 주체들 및 컴포넌트들이 더 기술될 것이다.

[0011] 컴퓨팅 장치들(100)은 이동 전화, 이동 스마트폰, 또는 소정의 다른 유형의 이동 장치와 같은 이동 컴퓨팅 장치들일 수 있다. 컴퓨팅 장치들(100)은 실행되는 코드의 일부 또는 전부가 신뢰 인가 기관(102)에 의해 승인될 것을 요구하는 운영 체제를 실행시키도록 구성될 수 있다. 따라서, 소프트웨어가 비인가 상태에서 컴퓨팅 장치들(100)에게 전달되는 경우, 장치들이 인가되지 않았기 때문에 이들이 소프트웨어에 포함된 코드 명령어들을 완전히 실행하는 것이 불가능할 수 있다.

[0012] 본 개시 내용이 이동 장치들과 관련되지만, 컴퓨팅 장치들(100)은 데스크톱 컴퓨터, 랩톱 컴퓨터, 핸드헬드(handheld) 컴퓨터, PDA(Personal Digital Assistant) 장치, 이동 전화 장치 및 미디어 재생 장치 등을 포함하는 임의의 개수의 상이한 유형의 컴퓨팅 장치일 수 있다.

[0013] 사용자가 자신들의 컴퓨팅 장치(100)를 사업자(104)의 네트워크 상에서 동작시키기를 원하는 경우, 그 장치

(100)는 이것이 네트워크 상에서 동작할 수 있도록 준비 또는 활성화될 필요가 있을 수 있다. 하나 이상의 실시예에서, 활성화 서비스(106)가 이러한 준비 프로세스를 수행하는 데 사용된다. 활성화 서비스(106)는 컴퓨팅 장치(100)에 데이터를 송신하는, 인터넷과 같은 네트워크 상의 하나 이상의 서버로서 구현될 수 있는데, 이후 이는 사업자(104)의 네트워크 상에서 동작하도록 장치(100)를 구성하는 데 사용된다.

[0014] 활성화 서비스(106)에 의해 송신되는 데이터는 사업자 준비 프로파일로 일컬어질 수 있는 형태를 취할 수 있다. 사업자 준비 프로파일은 장치(100)가 장치(100) 상의 설비들 및/또는 자원들을 어떻게 사용할 수 있는지, 그리고 장치(100)가 사업자(104)에 의해 운영되는 네트워크 서비스들과 어떻게 상호 작용할 수 있는지에 관한 정책 및 자격들을 지정할 수 있다.

[0015] 신뢰 인가 기관(102)은 코드가 컴퓨팅 장치(100) 상에서 실행될 수 있도록 코드를 인가할 수 있는 임의의 개인 또는 조직일 수 있다. 물론, 특정한 장치(100)는 둘 이상의 신뢰 인가 기관(102)을 가질 수 있다. 일부 실시예들에서, 신뢰 인가 기관(102)은 컴퓨팅 장치(100)의 운영 체제 및 보안 모델에 대한 제어를 행사하는 조직 및/또는 주체일 수 있다.

[0016] 본 명세서에서 사용되는 바처럼, 사업자(104)는 컴퓨팅 장치들(100)에 대한 네트워크 액세스를 제공하는 주체 또는 서비스 공급자일 수 있다. 사업자들(104)의 잘 알려진 예들은 Verizon, AT&T, T-Mobile 및 Sprint 등과 같은 이동 전화 서비스 공급자들이다.

[0017] 주목한 바처럼, 활성화 서비스(106)는 장치들(100)을 준비시키는 데 사용되는 시스템들 및 프로세스들일 수 있다. 활성화 서비스(106)는 네트워크 상에서 준비 데이터를 송신하도록 구성되는 네트워크 접속된 컴퓨팅 장치들 상에서 동작하는 하나 이상의 네트워크 애플리케이션 및 서버를 포함할 수 있다.

[0018] 일부 실시예들에서, 활성화 서비스(106)는 개인용 컴퓨터 상에서 실행되는 로컬 애플리케이션에게 준비 데이터를 송신할 수 있다. 장치들(100) 중 하나 이상이 개인용 컴퓨터에 연결되어 개인용 컴퓨터 상의 준비 애플리케이션을 통해 준비 데이터를 수신할 수 있다. 선택적으로, 컴퓨팅 장치(100)는 장치(100)로 하여금 사업자 네트워크에 접속하여 활성화 서비스(106)로부터 준비 데이터를 수신하도록 하는 기본 기능을 가지고 출하될 수 있다. 활성화 서비스(106)는 예컨대 사업자(104)의 네트워크를 통해 준비 데이터를 장치들(100)에 직접 송신할 수도 있다. 준비 데이터는 또한 컴퓨터 판독 가능 매체로부터, 또는 서버에 연결된 저장 장치 상에서 설치될 수 있다.

[0019] 도 2는 사업자(104) 또는 이들의 지정된 대표와 같은 신뢰 인가 기관(102) 이외의 주체에 의해 서명된 소프트웨어 모듈들(206)을 실행하기 위해 사업자 프로파일들(208)을 활용하도록 컴퓨팅 장치(100)가 어떻게 구성될 수 있는지에 관한 일례를 제공하는 블록도이다.

[0020] 소프트웨어(106)는 장치(100) 상에 저장되거나 그에 의해 액세스될 수 있는 하나 이상의 소프트웨어 모듈(206)을 포함할 수 있다. 일 실시예에서, 컴퓨팅 장치(100)의 저장소(209)는 소프트웨어 모듈들(206) 및 프로파일들(208) 중 하나 또는 둘 다를 저장하도록 구성될 수 있는 컴퓨터 판독 가능 저장 매체(휘발성 및/또는 비휘발성)를 포함할 수 있다. 저장소(209)는 또한 운영 체제(202)의 코드를 저장하도록 구성될 수 있고, 장치(100)를 위한 범용 저장소를 더 포함할 수 있다. 소프트웨어 모듈들(206)은 장치(100)에 일시적으로 또는 장치(100)에 영구적으로 저장될 수 있다.

[0021] 컴퓨팅 장치(100)는 운영 체제를 포함할 수 있다. 운영 체제는 MacOS, Windows, Linux, Unix, 또는 Symbian 등과 같은 잘 알려진 운영 체제일 수 있다. 앞서 간략히 논의된 바처럼, 운영 체제의 일부, 예컨대 운영 체제(202)의 커널은 장치(100) 상에서 실행되는 코드가 장치 상에서 그 실행을 허용하기 전에 인가될 것을 요구하도록 구성될 수 있다. 이러한 인가는 신뢰 인가 기관(102)이 소프트웨어 모듈들(206)의 일부 또는 전부를 디지털적으로 서명하는 형태를 취할 수 있다. 일부 실시예들에서, 신뢰 인가 기관(102)은 코드 서명 인증서를 활용할 수 있는데, 이는 서명된 컴퓨터 코드의 출처 및 무결성을 검증하는 데 사용될 수 있다.

[0022] 일부 실시예들에서, 컴퓨팅 장치들(100)은 또한 디버깅(debugging), 트레이싱(tracing), 또는 프로파일링 소프트웨어와 같은 개발 및 시험 관련 소프트웨어를 컴퓨팅 장치들(100) 상에 설치되는 표준 배포의 일부로서, 사전 준비 프로세스의 일부로서, 또는 임의의 다른 시기에 포함할 수 있다. 일부 실시예들에서, 컴퓨팅 장치들(100)은 이러한 추가적인 개발 관련 소프트웨어를 미리 공급받는다. 다른 실시예들에서, 개발 관련 소프트웨어는 액세스 프로파일과 함께, 또는 그와 관련하여 장치 상에 설치될 수 있다.

[0023] 운영 체제(202)에 의해 사용되는 메모리의 커널 공간은 개념적으로 신뢰 공간으로 간주될 수 있다. 신뢰는 커널의 부팅시 인증에 의해 수립될 수 있다. 일 실시예에서, 컴퓨팅 장치(100)는 운영 체제(202)에 의해 사용되

는 커널 공간 및 이것의 컨텐츠의 부팅시 인증을 제공하기 위한 하드웨어 지원을 포함할 수 있다. 예컨대, 일 실시예에서, 컴퓨팅 장치(100)의 부트 로더(boot loader)는 커널을 로딩하고 부팅하기 전에 예컨대 적합한 공개 키 서명 검증을 사용하여 커널 소프트웨어의 서명을 인증할 수 있다.

[0024] 디지털 서명은 예컨대 메시지 다이제스트(message digest)를 생성하기 위해 소프트웨어에 대해 해시(hash) 기능을 수행함으로써 생성될 수 있는 다이제스트를 포함할 수 있다. 일부 실시예들에서, 증분적인 코드 서명이 사용될 수 있다. 해시값은 소프트웨어의 전부 또는 특정한 부분에 대해 생성되는 해시값일 수 있다. 예컨대, 일부 실시예들에서, 소프트웨어는 하나 이상의 페이지와 같은 하나 이상의 유닛으로 분할된다. 해시값은 소프트웨어의 각 유닛 또는 페이지에 대해 생성된다. 이러한 실시예들에서 소프트웨어에 대한 다이제스트는 각 코드 또는 페이지의 해시값들의 어레이(array) 또는 테이블(table)에 대해 생성되는 해시값을 포함한다. 이후 메시지 다이제스트는 신뢰 인가 기관(102)과 연관된 개인 암호화 키를 사용하여 암호화될 수 있다. 일 실시예에서, 잘 알려진 SHA-1 함수가 메시지 다이제스트를 생성하는 데 사용될 수 있다. 이후 암호화된 메시지 다이제스트(서명이라고도 일컬어짐)는 소프트웨어 모듈들(206) 중 하나 이상에 추가될 수 있다.

[0025] 일부 실시예들에서, 소프트웨어 코드를 실행하기 위한 요청이 장치 상에서 이루어지는 경우, 운영 체제(202)는 디지털 서명을 승인함으로써 소프트웨어 코드의 출처 및 무결성을 검증하여 상기 요청을 처리할 수 있다. 코드의 출처가 신뢰 인가 기관(102)이고 코드의 무결성이 손상되지 않았으면, 운영 체제(202)는 코드가 컴퓨팅 장치(100) 상에서 수행되도록 허용할 수 있다.

[0026] 컴퓨팅 장치(100)는 또한 장치 식별자(204)를 포함할 수 있다. 장치 식별자(204)는 다양한 형태를 취할 수 있다. 일 실시예에서, 장치 식별자(204)는 컴퓨팅 장치(100)를 고유하게 식별하는 일련 번호일 수 있다. 다른 실시예들에서, 장치 식별자(204)는 운영 체제(202)에 의해 생성되는 고유한 식별자일 수 있다.

[0027] 앞서 주목한 바처럼, 컴퓨팅 장치(100)는 또한 신뢰 인가 기관(102)에 의해 생성된 사업자 프로파일(208)을 가질 수 있다. 개발자 액세스 프로파일(208)은 소정의 장치들이 신뢰 인가 기관(102)에 의해 서명되지 않은 소프트웨어를 실행하도록 허용됨을 나타내는 데이터의 집합을 포함할 수 있다. 일 실시예에서, 사업자 프로파일(208)은 신뢰 인가 기관(102)으로부터 추가적인 코드 서명 서비스를 요청할 필요 없이 사업자들(104)이 이들 자신의 소프트웨어 모듈들(206)을 수정 및/또는 제공할 수 있도록 한다. 선택적으로, 사업자(104)는 이들의 소프트웨어 모듈들(206)을 디지털적으로 서명하고, 사업자(104)에 의해 서명된 코드가 장치(100) 상에서 실행될 수 있음을 지정하는 사업자 프로파일들(208)을 갖는 컴퓨팅 장치들(100) 상에서 소프트웨어를 실행하도록 허용될 수 있다. 일부 실시예들에서, 사업자 프로파일은 또한 사업자(104)가 소프트웨어 모듈들(206)을 실행하면서 수행할 수 있는 소정의 동작들을 지정할 수 있다. 컴퓨팅 장치(100)는 또한 둘 이상의 사업자 프로파일(208)을 가질 수 있다.

[0028] 일부 실시예들에서, 사업자 프로파일(208)은 정책 서비스(210)와 관련하여 동작할 수 있다. 정책 서비스(210)는 운영 체제의 사용자(비신뢰) 메모리 공간에서 실행되는 데몬(daemon) 또는 다른 프로세스의 형태를 취할 수 있다. 정책 서비스(210)는 사업자 프로파일(208)에서 지정되는 정책들을 시행하도록 더 구성될 수 있다.

[0029] 정책 서비스(210)는 처음에 운영 체제(202)에 의해 시작될 수 있는데, 이는 서비스(210)의 암호적으로 보안된 다이제스트를 서비스를 로딩하기 전에 검증할 수 있다. 운영 체제(202)는 인터프로세스(interprocess) 통신 또는 유사한 적합한 포트를 통해 서비스(210)에 대한 참조를 유지할 수 있다. 따라서, 프로파일 서비스(210)는 비신뢰 또는 사용자 모드 공간에서 실행되는 반면, 프로파일 서비스(210)의 코드는 실행시에 신뢰 인가 기관에 의해 서명되도록 검증될 수 있다.

[0030] 도 3은 사업자 프로파일(208)의 보다 상세한 도면이다. 앞서 주목한 바처럼, 사업자 프로파일(208)은 장치가 신뢰 인가 기관(102)에 의해 서명되지 않았더라도 소프트웨어를 실행하도록 허용될 수 있음을 나타내는, 장치(100)의 메모리에 저장된 데이터의 집합일 수 있다. 사업자 프로파일(208)은 장치 식별자 데이터(302), 사업자 식별자 데이터(304) 및 자격 데이터(306)를 포함할 수 있다.

[0031] 장치 식별자 데이터(302)는 사업자 프로파일(208)이 적용되는 하나 이상의 장치 식별자(302)를 지정한다. 장치들(100)이 이동 전화 장치들인 실시예들에서, 장치 식별자 데이터(302)는 이동 전화 장치 일련 번호들의 어레이를 포함할 수 있다.

[0032] 사업자 프로파일(208)에 대한 장치 식별자 데이터(302)는 상이한 장치들에 대한 하나 이상의 장치 식별자(204)를 포함할 수 있다. 일 실시예에서, 장치 식별자들(204)은 특정한 장치들에 대한 숫자 또는 수문자 데이터로서 표현될 수 있는 특정한 식별자들일 수 있다. 다른 실시예들에서, 보다 일반화된 장치 식별 데이터가 활용될 수

있다. 예컨대, 일부 장치 판매자들 및/또는 제조자들은 조직에 특정되는 장치 식별자들을 갖는 장치들을 제공할 수 있다. 예컨대, 장치 판매자 및/또는 제조자는 장치들과 연관된 장치 식별자들(204)의 소정의 국면들을 이들이 전달되는 조직에 기초하여 커스터마이징(customize)할 수 있다.

[0033] 장치 식별자 데이터(302)는 각각의 개별 장치 식별자 값을 열거하는 대신 장치 식별자들의 범위들을 포함할 수 있다. 또 다른 실시예들에서, 지정된 식별자 특성들을 갖는 모든 장치들에 사업자 프로파일이 적용됨을 지정하기 위해 비트 마스크(bit mask) 또는 와일드 카드(wild card) 문자들이 사용될 수 있다. 또 다른 실시예들에서, 장치 식별자 데이터(302)는 사업자 프로파일(208)이 모든 장치들에 적용됨을 지정할 수 있다. 예컨대, 이러한 일 실시예에서, 사업자 식별자 데이터(302)에서 식별된 사업자들 중 하나 이상에 의해 서명된 소프트웨어는 사업자 프로파일(208)이 설치될 수 있는 임의의 장치(100) 상에서 실행되도록 인가될 수 있다.

[0034] 주목한 바처럼, 사업자 프로파일(208)은 사업자 프로파일(208)이 적용되는 사업자들(104)을 지정하는 사업자 식별자 데이터(304)를 더 포함할 수 있다. 사업자 식별자 데이터(304)는 다양한 형태를 취할 수 있다. 일부 실시예들에서, 사업자 식별자 데이터(304)는 사업자 프로파일(208)에 의해 포괄되는 사업자들(104)과 연관된 공개키들일 수 있다. 다른 유형의 식별자들이 또한 사용될 수 있다. 일부 실시예들에서, 사업자 식별자 데이터(304)는 사업자 프로파일 내에 저장된 어레이 데이터 구조에 저장될 수 있다. 물론, 임의의 적합한 데이터 구조들이 사용될 수 있다.

[0035] 또한, 사업자 프로파일(208)은 자격 데이터(306)를 포함할 수 있다. 자격 데이터(306)는 장치 식별자 데이터(302)에서 지정된 장치들(100) 상에서 사업자 식별자 데이터(304)에서 식별된 사업자들에 의해 서명된 소프트웨어 모듈들(206)에 대해 허용되는 동작들의 유형들을 나타내는 데이터를 포함할 수 있다. 특정한 사업자 프로파일(208)은 둘 이상의 사업자(104)가 사업자 프로파일(208)에 의해 인가된 코드를 디지털적으로 서명하도록 인가된 것으로 지정할 수 있다.

[0036] 자격 데이터(306)는 장치 식별자 데이터(302)에서 식별된 장치들(100)에 관하여 사업자 식별자 데이터(304)에서 식별된 사업자들(104)에 의해 서명된 애플리케이션들에 대해 허용되는 액세스의 유형들을 지정할 수 있다. 자격 데이터(306)는 키값 쌍(key-value pair)들의 형태를 취할 수 있다. 상기 값들은 예컨대 숫자, 부울(Boolean), 또는 수문자 데이터를 포함할 수 있다. 일 실시예에서, 자격 데이터(306)는 다양한 지정된 자격을 나타내는 미리 정의된 부울 변수들의 어레이 또는 다른 데이터 구조를 포함할 수 있다.

[0037] 일 실시예에서, 자격 데이터(306)는 실행될 수 있는 능력을 포함할 수 있다. 다른 자격들은 장치(100)의 네트워킹 자원, 주소록 데이터와 같은 보안 또는 프라이버시 관련성을 갖는 데이터, 라이브러리들, 또는 애플리케이션들에 대한 액세스를 제어할 수 있다. 또한, 다른 자격들은 전화, 네트워킹, 주소 또는 전화 저장소, 또는 멀티미디어 API들을 포함하는 특정한 사업자 API들에 대한 액세스를 제어할 수 있다.

[0038] 도 4는 컴퓨팅 장치(100)의 일 실시예의 소프트웨어 컴포넌트들 사이에서 시스템에 의해 요청이 수신 및 처리될 수 있는 경우에 발생하는 이벤트들 사이의 관계들을 도시하는 블록도이다. 도시된 바처럼, 이벤트 1에서, 신뢰 공간을 포함할 수 있는 운영 체제(202)는 {특정한 소프트웨어 모듈(206)을 실행하기 위한 사용자 요청에 응답하여 또는 특정한 소프트웨어 모듈(206)을 실행하기 위한 장치(100) 상의 다른 소프트웨어 컴포넌트의 요청에 응답하여} 식별된 소프트웨어 모듈(206)을 실행하기 위한 요청을 수신할 수 있다. 일 실시예에서, 상기 요청은 소프트웨어 모듈(206)의 실행 가능한 명령어 코드를 저장하는 저장소(209)의 디렉토리 또는 파일에 대한 참조를 포함할 수 있다.

[0039] 이벤트 2에서, 운영 체제(202)는 소프트웨어 모듈(206)을 인증하기 위한 요청을 정책 서비스(210)에 대해 통신할 수 있다. 일 실시예에서, 상기 인증 요청은 소프트웨어 모듈(206)과 연관된 저장소(209) 내의 저장 위치에 대한 참조를 포함할 수 있다. 운영 체제(202)는 또한 소프트웨어 모듈(206)의 적어도 일부의 다이제스트를 정책 서비스(210)에 제공할 수 있다. 선택적으로, 또는 그에 추가하여, 정책 서비스(210)는 소프트웨어 모듈(206)의 전부 또는 일부의 다이제스트를 생성할 수 있다. 일 실시예에서, 상기 다이제스트는 소프트웨어 모듈(206)과 연관된 각각의 코드 페이지 또는 각각의 파일에 대해 결정된 다이제스트 값들에 기초할 수 있다. 일 실시예에서, 정책 서비스(210)에 대한 요청들은 시행될 특정한 자격들과 같은 다른 데이터를 포함할 수 있다

[0040] 예컨대, 운영 체제(202)는 상기 자격이 지정된 시스템 자원을 실행하거나 액세스하기 위한 자격일 수 있음을 지정할 수 있다. 운영 체제(202) 또는 장치(100)의 운영 체제의 다른 부분은 이동 전화 네트워크, 블루투스 스택(Bluetooth stack)과 같은 특정한 네트워크들에 대한 액세스, 또는 장치(100)의 마이크, 스피커, 카메라, 또는 다른 I/O 인터페이스를 액세스하는 것과 같은 장치(100)의 특정한 능력들에 대한 액세스를 위한 자격 인가를 요

청하도록 구성될 수 있다.

[0041] 이벤트 5에서, 정책 서비스(210)는 소프트웨어 모듈(206)의 실행과 연관된 하나 이상의 프로파일(208)에 액세스할 수 있다. 일 실시예에서, 프로파일들은 저장소(209)로부터 액세스된다. 일 실시예에서, 프로파일들(208)은 사업자(104)와 연관된 특정한 프로파일을 포함한다. 본 명세서에서 프로파일들이 신뢰 인가 기관(102) 이외의 사업자들(104)에 관하여 기술되지만, 신뢰 인가 기관(102), 예컨대 장치 또는 운영 체제 개발자에 의해 제공되는 소프트웨어 모듈들에 대한 액세스가 또한 본 명세서에 기술된 시스템들 및 방법들을 사용하여 제어될 수 있음을 인식할 수 있다.

[0042] 이벤트 5에서, 정책 서비스(210)는 다이제스트 및/또는 프로파일(208)에 기초하여 소프트웨어 모듈(206)의 실행 권한들을 검증할 수 있다. 예컨대, 정책 서비스(210)는 소프트웨어 모듈(206)의 다이제스트와 연관된 서명을 수신하고 상기 다이제스트를 암호적으로 검증하도록 구성될 수 있다. 일 실시예에서, 정책 서비스(210)는 프로파일(208)의 일부로서 포함될 수 있는, 특정한 사업자(104)와 연관된 공개 키를 사용하여 다이제스트의 서명을 검증할 수 있다.

[0043] 일 실시예에서, 프로파일 및 사업자 키가 신뢰될 수 있음을 보장하기 위해, 정책 서비스(210)는 프로파일이 신뢰 인가 기관(102)에 의해 신뢰될 수 있음을 암호적으로 검증한다. 이러한 실시예에서, 정책 서비스(210)는 장치(100) 상에 저장되거나 또는 그렇지 않으면 장치(100)에 의해 예컨대 데이터 네트워크를 통해 액세스될 수 있는 신뢰 인가 기관(102)의 공개 키를 사용하여 프로파일의 다이제스트 또는 다른 서명(및 이것의 컨텐츠)을 검증함으로써 프로파일을 검증할 수 있다.

[0044] 정책 서비스(210)는 소프트웨어 모듈(206)이 특정한 장치(100)에 대해 인가될 수 있음을 검증하도록 더 구성될 수 있다. 예컨대, 일 실시예에서, 프로파일(208)은 부합하는 장치 식별자들{예컨대 장치들(100)의 지정된 그룹에 부합하는 마스크 또는 와일드카드}에 대한 하나 이상의 장치 식별자 또는 데이터를 포함할 수 있다.

[0045] 정책 서비스(210)는 식별자들을 장치(100)에 의해 안전하게 유지되는 식별자와 비교할 수 있고, 정책(208)의 식별자 데이터가 장치(100)의 것에 부합하는 경우 소프트웨어 모듈을 인가한다. 장치 식별자는 제조자 일련번호, 이동 전화 장치의 장치 또는 가입자 식별자들, 예컨대 ICCID(Integrated Circuit Card ID), 장치(100)에 현재 삽입된 SIM 카드의 IMSI(International Mobile Subscriber Identifier), 장치 상에 인코딩된 IMEI(International Mobile Equipment Identifier), ESN(Electronic Serial Number), 또는 특정한 소프트웨어 모듈(206)이 인가될 수 있는 장치들(100)을 식별하는 데 적합한 임의의 다른 데이터를 포함하는, 식별에 사용될 수 있는 장치 상에 저장된 임의의 데이터를 포함할 수 있다.

[0046] 정책 서비스(210)는 프로파일들(208)에 의해 지정되는 바와 같은 추가적인 자격들 또는 다른 능력들에 기초하여 소프트웨어 모듈(206)을 인가하도록 구성될 수 있다. 실행 가능 또는 실행 불가능이 자격의 예로서 간주될 수 있다. 다른 자격들은 프로파일들(208) 중 하나 이상에 기초하고 정책 서비스(210)가 시행하도록 구성될 수 있는 임의의 다른 정책에 기초하여 특정한 소프트웨어 모듈(206)이 서비스를 실행하거나 액세스할 수 있는지 여부를 지정할 수 있다.

[0047] 정책 서비스(210)는 사용자 공간에서 실행되도록 구성되어, 사용자 공간에서 시행되는 정책들 및 프로파일들이 임의적으로 복잡하고, 커널 또는 다른 보호 메모리 공간의 크기를 증가시키지 않고 업데이트되며, 커널 프로그래밍과 일반적으로 연관되는 어려움 없이 보다 쉽게 개발 및 개정될 수 있도록 할 수 있다.

[0048] 도 5는 운영 체제(202)가 특정한 소프트웨어 모듈(206)이 실행될 자격을 갖는지 여부를 결정하는 예를 도시하지만, 본 명세서에 기술된 방법들 및 시스템들은 장치 하드웨어 능력들, 커널의 다른 서비스들, 다른 운영 체제 서비스들, 또는 다른 소프트웨어 모듈(208)의 서비스들에 대한 액세스를 인가하는 데 사용될 수 있음을 인식할 것이다.

[0049] 자격들은 장치와 연관된 하나 이상의 정책을 통해 시행될 수 있다. 예컨대, 자격들을 시행하기 위한 정책은 화이트 리스트(white list)로서 프로파일들 내의 처리 자격 데이터를 포함할 수 있는데, 예컨대 프로파일(208)이 특정한 소프트웨어 모듈(206) 및/또는 특정한 장치(100)에 대한 자격이 존재함을 나타내는 데이터를 포함할 수 있는 경우에 소프트웨어 모듈(206)은 이러한 특정한 자격에 대해 인증될 수 있다. 다른 정책은 블랙리스트(blacklist)에 기초하여 자격들을 시행할 수 있는데, 예컨대 소프트웨어 모듈(206)은 프로파일(208) 또는 적용 가능한 정책이 특정한 소프트웨어 모듈(206) 및/또는 특정한 장치(100)에 대한 자격을 부정하는 데이터를 포함할 수 있는 경우가 아니면 소프트웨어 모듈(206)은 이러한 특정한 자격에 대해 인증될 수 있다. 다른 실시예에서, 일부 자격들이 화이트 리스트를 통해 시행되도록 구성될 수 있는 반면 다른 자격들은 블랙리스트를 통해 시

행되도록 구성될 수 있게끔 하는 정책으로 장치(100)가 구성될 수 있다.

[0050] 특정한 자격들을 보다 정교하게 제어하거나 또는 충돌하는 프로파일 데이터를 해결하기 위해 다른 정책들이 포함될 수 있다. 예컨대, 일 실시예에서, 이동 서비스 공급자는 특정한 장치 능력들, 예컨대 음성 네트워크 또는 다이얼러(dialer) 액세스에 대한 자격들을 더 지정하는 자신의 네트워크 상에서 사용하기 위한 장치들 내에 특정한 사업자 프로파일(208)을 포함시킬 수 있는데, 이는 특정한 소프트웨어 모듈들(206)에 대한 사업자 프로파일(208)과 충돌할 수 있다. 이러한 경우, 장치(100)의 정책은 프로파일들 중 하나의 자격 사양이 제어함을 지정할 수 있다.

[0051] 장치(100)가 사업자(104)에 의해 사업자의 네트워크를 사용하게끔 구성되도록 활성화 또는 준비되는 경우에, 사업자(104)로부터의 프로파일들(208)이 장치(100) 상에서 수신 및 저장될 수 있다. 일 실시예에서, 사업자 프로파일(208)은 사업자의 SIM 카드에 의해 제공되거나 또는 SIM 카드의 삽입에 응답하여 장치(100)에 다운로드될 수 있다. 일 실시예에서, 사업자 프로파일(208)은 소프트웨어 모듈들(206)의 일부 또는 전부에 대해 제공될 수 있었던 자격들을 무효화하거나 제한하는 자격들의 블랙리스트를 포함할 수 있다. 사업자 프로파일(208)은 SIM 카드들을 나타내는 데이터를 포함하여, 장치(100)의 SIM 카드가 상기 데이터에 부합하지 않도록 변경되는 경우에 사업자 프로파일이 인증되지 않도록 할 수 있다. 서비스 공급자 또는 사업자 프로파일(208)은 일 실시예에서 사업자(104)의 디지털 서명으로 서명될 수 있고, 이는 다음으로 신뢰 인가 기관(102)의 디지털 신호에 의해 서명된다.

[0052] 정책 서비스(210)는 서비스 공급자, 제조자 및 소프트웨어 모듈 프로파일들 및 자격들 사이의 충돌을 해결하기 위한 규칙 엔진 또는 다른 로직을 포함할 수 있다. 일 실시예에서, 사업자 프로파일(208)은 소프트웨어 모듈 프로파일들을 무효화할 수 있고, 이는 다음으로 제조자 프로파일을 무효화하거나 확장할 수 있다. 따라서, 예컨대 제조자 프로파일은 소프트웨어 모듈들(206)이 네트워크 스택과 같은 서비스를 액세스하도록 할 수 있다. 특정한 소프트웨어 모듈(206)이 네트워크 스택을 액세스하도록 더 인증될 수 있다. 그러나, 사업자 프로파일(208)은 지정된 사업자 프로파일들에 대해 또는 모든 사업자 프로파일들에 대해 네트워크 스택에 대한 액세스를 블랙리스팅하거나 그렇지 않으면 거부함을 나타내는 데이터를 포함할 수 있다. 정책 서비스(210)는 운영 체제(202)의 커널 내의 이러한 로직을 최소화하기 위해 사용자 공간 프로세스에서의 이러한 복잡함을 해결할 수 있다.

[0053] 이벤트 6에서, 정책 서비스(210)가 소프트웨어 모듈(240)의 자격들 및/또는 다른 실행 권한들을 검증할 수 있는 경우, 정책 서비스(210)는 소프트웨어 모듈(206)의 자격들 및/또는 인증 요청이 이루어진 자격들을 나타내는 데이터를 운영 체제(202) 또는 정책 서비스(210)의 다른 클라이언트에게 제공한다. 이벤트 7에서, 운영 체제(202)는 이후 정책 서비스(210)로부터 수신된 자격 데이터에 따라 소프트웨어 모듈(206)을 실행할 수 있다.

[0054] 도 5는 장치들(100)에서 소프트웨어 모듈들(206)의 자격들을 검증하는 방법(500)의 일 실시예를 도시하는 흐름도이다. 상기 방법은 운영 체제(202)의 신뢰 공간이 특정한 소프트웨어 모듈(206)을 실행하기 위한 요청을 수신하는 블록(502)에서 시작할 수 있다. 일 실시예에서, 상기 신뢰 공간은 로딩 전에 운영 체제(202)를 암호적으로 검증하는 장치(100)의 부트 로더에 의해 장치의 시동시에 수립될 수 있다.

[0055] 블록(504)에서, 신뢰 공간 프로세스는 정책 서비스(210)의 최초 실행시에 신뢰가 부여된 비신뢰 공간에서 실행되는 정책 서비스(210)에 대해 소프트웨어 모듈(206)을 나타내는 데이터를 통신한다. 상기 데이터는 소프트웨어 모듈(206)의 저장 위치에 대한 참조를 포함할 수 있고, 인증되고 있는 특정한 자격을 나타내는 데이터를 선택적으로 포함할 수 있다.

[0056] 다음으로 블록(506)에서, 정책 서비스(210)는 소프트웨어 모듈(206)을 인증한다. 일 실시예에서, 정책 서비스(210)는 암호화 인증에 기초하여 소프트웨어 모듈(206)을 인증한다. 예컨대, 정책 서비스(210)는 비대칭/공개키 암호화와 같은 적합한 암호화 기법들을 사용하여 소프트웨어 모듈(206)의 디지털 서명을 검증함으로써 소프트웨어 모듈(206)을 인증할 수 있다. 또한, 소프트웨어 모듈(206)과 연관된 하나 이상의 자격이 유사한 암호화 기법들을 사용하여 인증될 수 있다. 블록(506)의 추가적인 세부 사항들은 도 6을 참조하여 확인할 수 있다.

[0057] 블록(508)으로 진행하면, 정책 서비스(210)는 소프트웨어 모듈의 실행 권한들을 나타내는 데이터를 운영 체제(202)의 커널에 대해 통신한다. 상기 데이터는 부울 인증 응답, 소프트웨어 모듈(206)의 하나 이상의 자격을 나타내는 데이터, 소프트웨어 모듈(206)의 검증된 다이제스트, 또는 요청과 관련된 임의의 다른 적합한 데이터를 포함할 수 있다.

[0058] 블록(510)에서, 이후 운영 체제(202) 또는 다른 신뢰 프로세스는 소프트웨어 모듈(206)을 실행할 수 있거나 또

는 인증된 자격들에 기초하여 소프트웨어 모듈(206)에 대한 서비스들을 수행할 수 있다.

[0059] 도 6은 도 5의 방법의 블록(506)을 보다 상세하게 도시하는 흐름도이다. 블록(602)에서, 정책 서비스(210)는 소프트웨어 모듈(206)의 실행 가능한 코드와 연관된 적어도 하나의 파일 또는 다른 데이터 구조의 다이제스트를 계산할 수 있다. 다이제스트는 예컨대 SHA-1을 포함하는 임의의 적합한 해시 알고리즘을 사용하여 계산될 수 있다.

[0060] 블록(604)에서, 정책 서비스(210)는 소프트웨어 모듈(206) 및/또는 장치(100)와 연관된 하나 이상의 프로파일(208)을 식별할 수 있다. 일 실시예에서, 프로파일들(208)은 각각 소프트웨어 모듈(206)의 자격들을 나타내는 데이터 및 서명 키를 포함할 수 있다. 예컨대, 자격은 표 1에 도시된 바와 같은 표 형태의 데이터 구조를 포함할 수 있다.

표 1

[0061]

개발자 서명 키	123555
장치 ID1	123FFF
장치 ID2	123FFF
실행 가능	TRUE
디버깅 가능	FALSE
네트워크_액세스_가능	TRUE
코드 다이제스트	AAFF1144BB

[0062] < 예시 프로파일 데이터 >

[0063] 소프트웨어 모듈들(206)은 소프트웨어 모듈(206)의 다이제스트(예컨대 표 1에 도시된 "코드 다이제스트")를 식별하는 프로파일의 키값 쌍들을 통해 프로파일들(208)과 연관될 수 있다. 프로파일(208)은 디지털 서명, 예컨대 신뢰 인가 기관(102)에 의해 암호적으로 서명된 프로파일의 다이제스트를 더 포함할 수 있다. 다음으로 블록(606)에서, 정책 서비스(210)는 예컨대 프로파일(208)의 다이제스트의 암호화 서명이 올바름을 검증함으로써 프로파일(208)을 암호적으로 검증한다.

[0064] 블록(608)으로 이동하면, 정책 서비스(210)는 프로파일(208)이 특정한 장치(100)에 적용 가능할 수 있음을 검증한다. 일 실시예에서, 상기 검증 단계는 특정한 장치(100)의 장치 식별자(204)를 서명된 프로파일(208)에서 열거된 장치 식별자들과 비교하는 단계를 포함할 수 있다. 블록(606)에서의 이전의 서명 검증은 프로파일(208)에서 식별된 장치가 인가 없이 변경 또는 수정되지 않았다는 보증을 제공할 수 있다.

[0065] 다음으로 블록(610)에서, 정책 서비스(210)는 프로파일(들)(208)에 기초하여 소프트웨어 모듈(206)과 연관된 실행 권한들을 식별할 수 있다. 일 실시예에서, 상기 식별 단계는 각 프로파일의 자격들을 액세스하는 단계를 포함할 수 있다.

[0066] 블록(612)에서, 정책 서비스(210)는 소프트웨어 모듈(206)에 대해 검증될 자격들이 컴퓨팅 장치(100)에 대한 정책들과 일치함을 검증할 수 있다. 일 실시예에서, 상기 검증 단계는 요청된 자격이 소프트웨어 모듈(206)과 연관된 프로파일들(208) 및 장치(100)의 정책들 내에 포함될 수 있는지 여부를 결정하는 단계를 포함할 수 있다.

[0067] 블록(614)으로 진행하면, 이후 정책 서비스(210)는 블록(602)에서 계산된 다이제스트 값을 소프트웨어 모듈(206)의 서명된 다이제스트와 비교하고 상기 다이제스트의 암호화 서명을 검증할 수 있다. 실시예에 따라 본 명세서에 기술된 방법들 중 임의의 것의 소정의 동작들 또는 이벤트들이 상이한 순서로 수행되거나, 추가되거나, 병합되거나, 또는 모두 함께 배제될 수 있음을 인식할 것이다(예컨대 상기 방법을 실시하기 위해 모든 기술된 동작들 또는 이벤트들이 필요하지는 않음). 더욱이, 소정의 실시예들에서, 동작들 또는 이벤트들은 순차적으로 수행되는 대신에 예컨대 멀티스레딩(multi-thread)된 처리, 인터럽트(interrupt) 처리, 또는 복수의 프로세서를 통해 동시에 수행될 수 있다.

[0068] 도 7은 이동 장치로서 구현된 장치들(100) 중 하나의 예를 도시하는 블록도이다. 장치(100)는 메모리(704)와 통신할 수 있는 프로세서(702)를 포함할 수 있다. 네트워크 인터페이스(706)는 하나 이상의 적합한 데이터 및/또는 음성 통신 시스템들에 따라 신호들을 통해 통신하도록 구성되는 수신기(724) 및 송신기(726)를 포함할 수 있다. 예컨대, 네트워크 인터페이스(708)는 GSM, CDMA, CDMA2000, EDGE 또는 UMTS와 같은 이동 전화 네트워크들 상에서 음성 및/또는 데이터를 통신할 수 있다. 네트워크 인터페이스(706)는 예컨대 와이파이(WiFi)와 같은 임의의 IEEE 802.x 네트워크 또는 블루투스를 포함하는 다른 데이터 네트워크들에 대한 수신기/송신기들을 더

포함할 수 있다.

[0069] 장치(100)는 또한 디스플레이(710), 키, 터치 스크린, 또는 다른 적합한 촉각 입력 장치와 같은 사용자 입력 장치(712), 통신 링크(106)를 통해 수신된 신호에 기초하여 가청 출력을 제공하도록 적응된 트랜스듀서(transducer)를 포함하는 스피커(714) 및/또는 통신 링크들(106 및 108) 중 하나 또는 둘 다를 통해 송신될 수 있는 신호의 가청 입력을 제공하도록 적응된 트랜스듀서를 포함하는 마이크(716) 중 하나 이상을 포함할 수 있다.

[0070] 일 실시예에서, 입력 장치(712)는 장치의 이동을 탐지하도록 구성되는 가속도계 또는 다른 장치를 포함할 수 있다. 장치(100)는 장치(100)의 하나 이상의 컴포넌트에 전력을 공급하기 위한 배터리(731)를 선택적으로 포함할 수 있다. 장치(100)는 이동 송수화기, PDA, 랩톱 컴퓨터, 헤드셋(headset), 차량 핸즈프리(hands free) 장치, 또는 임의의 다른 전자 장치 중 적어도 하나를 포함할 수 있다. 예컨대, 본 명세서에 설명된 하나 이상의 태양은 전화(예컨대 이동 전화), PDA, 엔터테인먼트 장치(예컨대 음악 또는 비디오 장치), 헤드셋(예컨대 헤드폰, 수화기 등), 마이크, 또는 임의의 다른 전자 장치 내에 포함될 수 있다. 아래에서 도 기술되는 바처럼, 일부 실시예들에서 장치(100)는 이동 장치로서 구현된다.

[0071] 도 8a는 예시 이동 장치(2500)를 도시한다. 이동 장치(2500)는 예컨대 핸드헬드 컴퓨터, PDA, 셀룰러(cellular) 전화, 네트워크 기기, 카메라, 스마트폰, EGPRS(Enhanced General Packet Radio Service) 이동 전화, 네트워크 기지국, 미디어 재생기, 내비게이션 장치, 이메일 장치, 게임 콘솔(game console), 또는 이러한 데이터 처리 장치들 또는 다른 데이터 처리 장치들 중 임의의 둘 이상의 조합일 수 있다.

[0072] 이동 장치 개관

[0073] 일부 구현예들에서, 이동 장치(2500)는 터치 감지 디스플레이(2502)를 포함한다. 터치 감지 디스플레이(2502)는 LCD(Liquid Crystal Display) 기술, LPD(Light Emitting Polymer Display) 기술, 또는 소정의 다른 디스플레이 기술로 구현될 수 있다. 터치 감지 디스플레이(2502)는 사용자와의 햅틱(haptic) 및/또는 촉각적 접촉을 감지할 수 있다.

[0074] 일부 구현예들에서, 터치 감지 디스플레이(2502)는 다중 터치 감지 디스플레이(2502)를 포함할 수 있다. 다중 터치 감지 디스플레이(2502)는 예컨대 복수의 동시에 존재하는 터치 포인트를 처리할 수 있는데, 여기에는 각 터치 포인트의 압력, 각도 및/또는 위치와 관련된 데이터를 처리하는 것이 포함된다. 이러한 처리는 복수의 손가락을 사용한 제스처 및 상호 작용, 코딩(chording) 및 다른 상호 작용을 촉진시킨다. 다른 터치 감지 디스플레이 기술들, 예컨대 스타일러스(stylus) 또는 다른 포인팅 장치를 사용하여 접촉이 이루어지는 디스플레이가 또한 사용될 수 있다. 다중 터치 감지 디스플레이 기술의 일부 예들은 본 명세서에 그 전체가 참고 문헌으로서 포함되는 미국 특허 제6,323,846, 6,570,557, 6,677,932 및 6,888,536호에 기술되어 있다.

[0075] 일부 구현예들에서, 이동 장치(2500)는 다양한 시스템 객체에 대한 사용자 액세스를 제공하고 사용자에게 정보를 전달하기 위한 하나 이상의 그래픽 사용자 인터페이스를 터치 감지 디스플레이(2502) 상에 디스플레이할 수 있다. 일부 구현예들에서, 그래픽 사용자 인터페이스는 하나 이상의 디스플레이 객체(2504, 2506)를 포함할 수 있다. 도시된 예에서, 디스플레이 객체들(2504, 2506)은 시스템 객체들의 그래픽 표현들이다. 시스템 객체들의 일부 예들은 장치 기능, 애플리케이션, 윈도우(window), 파일, 경고, 이벤트, 또는 다른 식별 가능한 시스템 객체들을 포함한다.

[0076] 예시 이동 장치 기능

[0077] 일부 구현예들에서, 이동 장치(2500)는 전화 객체(2510)에 의해 나타낸 바와 같은 전화 장치, 메일 객체(2512)에 의해 나타낸 바와 같은 이메일 장치, 지도 객체(2514)에 의해 나타낸 바와 같은 지도 장치들, 와이파이 기지국 장치(도시되지 않음) 및 웹 비디오 객체(2516)에 의해 나타낸 바와 같은 네트워크 비디오 송신 및 디스플레이 장치와 같은 복수의 장치 기능을 구현할 수 있다. 일부 구현예들에서, 특정한 디스플레이 객체들(2504), 예컨대 전화 객체(2510), 메일 객체(2512), 지도 객체(2514) 및 웹 비디오 객체(2516)는 메뉴 바(menu bar)(2518)에 디스플레이될 수 있다. 일부 구현예들에서, 장치 기능들은 도 8a에 도시된 그래픽 사용자 인터페이스와 같은 최상위 그래픽 사용자 인터페이스로부터 액세스될 수 있다. 객체들(2510, 2512, 2514, 또는 2516) 중 하나를 터치하는 것은 예컨대 대응하는 기능을 호출할 수 있다.

[0078] 일부 구현예들에서, 이동 장치(2500)는 네트워크 배포 기능을 구현할 수 있다. 예컨대, 상기 기능은 사용자로 하여금 이동 장치(2500)를 휴대하고 여행 중에 이것의 연관된 네트워크에 대한 액세스를 제공하도록 할 수 있다. 특히, 이동 장치(2500)는 근처의 다른 무선 장치들에 대해 인터넷 액세스(예컨대 와이파이)를 확장할 수

있다. 예컨대, 이동 장치(2500)는 하나 이상의 장치에 대한 이동국으로서 구성될 수 있다. 그러므로, 이동 장치(2500)는 다른 무선 장치들에 대한 네트워크 액세스를 허가하거나 거부할 수 있다.

[0079] 일부 구현예들에서, 장치 기능의 호출시에, 이동 장치(2500)의 그래픽 사용자 인터페이스가 변화하거나, 또는 다른 사용자 인터페이스 또는 사용자 인터페이스 요소들로 증대되거나 대체되어 대응하는 장치 기능과 연관된 특정한 기능들에 대한 사용자 액세스를 촉진시킨다. 예컨대, 사용자가 전화 객체(2510)를 터치하는 것에 응답하여, 터치 감지 디스플레이(2502)의 그래픽 사용자 인터페이스는 다양한 전화 기능과 관련된 디스플레이 객체들을 제시할 수 있다. 마찬가지로, 메일 객체(2512)를 터치하는 것은 그래픽 사용자 인터페이스로 하여금 다양한 이메일 기능들과 관련된 디스플레이 객체들을 제시하도록 할 수 있다. 지도 객체(2514)를 터치하는 것은 그래픽 사용자 인터페이스로 하여금 다양한 지도 기능들과 관련된 디스플레이 객체들을 제시하도록 할 수 있다. 그리고 웹 비디오 객체(2516)를 터치하는 것은 그래픽 사용자 인터페이스로 하여금 다양한 웹 비디오 기능들과 관련된 디스플레이 객체들을 제시하도록 할 수 있다.

[0080] 일부 구현예들에서, 도 8a의 최상위 그래픽 사용자 인터페이스 환경 또는 상태는 이동 장치(2500)의 하단 근처에 위치한 버튼(2520)을 누름으로써 회복될 수 있다. 일부 구현예들에서, 각각의 대응하는 장치 기능은 터치 감지 디스플레이(2502) 상에 디스플레이되는 대응하는 "홈" 디스플레이 객체들을 가질 수 있고, 도 8a의 그래픽 사용자 인터페이스 환경은 "홈" 디스플레이 객체를 누름으로써 회복될 수 있다.

[0081] 일부 구현예들에서, 최상위 그래픽 사용자 인터페이스는 SMS(Short Messaging Service) 객체(2530), 캘린더(Calendar) 객체(2532), 사진 객체(2534), 카메라 객체(2536), 계산기 객체(2538), 주식 객체(2540), 주소록 객체(2542), 미디어 객체(2544), 웹 객체(2546), 비디오 객체(2548), 설정 객체(2550) 및 노트 객체(도시되지 않음)와 같은 추가적인 디스플레이 객체들(2506)을 포함할 수 있다. SMS 디스플레이 객체(2530)를 터치하는 것은 예컨대 SMS 메시징 환경 및 지원 기능을 호출할 수 있다. 마찬가지로, 디스플레이 객체(2532, 2534, 2536, 2538, 2540, 2542, 2544, 2546, 2548 및 2550)를 각각 선택하는 것은 대응하는 객체 환경 및 기능을 호출할 수 있다.

[0082] 추가적이고/이거나 상이한 디스플레이 객체들이 또한 도 8a의 그래픽 사용자 인터페이스에 디스플레이될 수 있다. 예컨대, 장치(2500)가 다른 장치들에 대한 기지국으로서 기능하고 있는 경우, 하나 이상의 "접속" 객체가 접속을 나타내도록 그래픽 사용자 인터페이스에 나타날 수 있다. 일부 구현예들에서, 디스플레이 객체들(2506)은 사용자에 의해 구성될 수 있는데, 예컨대 사용자는 어느 디스플레이 객체들(2506)이 디스플레이되는지를 지정할 수 있고/있거나 추가적인 애플리케이션들 또는 다른 기능들 및 대응하는 디스플레이 객체들을 제공하는 다른 소프트웨어를 다운로드할 수 있다.

[0083] 일부 구현예들에서, 이동 장치(2500)는 하나 이상의 입력/출력(I/O) 장치들 및/또는 센서 장치들을 포함할 수 있다. 예컨대, 스피커(2560) 및 마이크(2562)가 전화 및 음성 메일 기능들과 같은 음성 가능 기능들을 촉진하도록 포함될 수 있다. 일부 구현예들에서, 스피커(2560) 및 마이크(2562)의 음량 제어를 위한 업/다운 버튼(2584)이 포함될 수 있다. 이동 장치(2500)는 또한 걸려오는 전화 통화들의 링 표시기를 위한 온/오프 버튼(2582)을 포함할 수 있다. 일부 구현예들에서, 스피커(2564)가 스피커 폰 기능들과 같은 핸즈프리 음성 기능들을 촉진하도록 포함될 수 있다. 오디오 잭(2566)이 또한 헤드폰 및/또는 마이크의 사용을 위해 포함될 수 있다.

[0084] 일부 구현예들에서, 사용자가 사용자의 귀에 근접하여 이동 장치(2500)를 위치시키는 것의 탐지를 촉진하고 그에 응답하여 우발적인 기능 호출을 방지하기 위해 터치 감지 디스플레이(2502)를 해제하도록 근접 센서(2568)가 포함될 수 있다. 일부 구현예들에서, 터치 감지 디스플레이(2502)는 이동 장치(2500)가 사용자의 귀에 근접한 경우에 추가적인 전력을 보존하도록 꺼질 수 있다.

[0085] 다른 센서들이 또한 사용될 수 있다. 예컨대, 일부 구현예들에서, 주변광 센서(2570)가 터치 감지 디스플레이(2502)의 밝기의 조절을 촉진하도록 활용될 수 있다. 일부 구현예들에서, 가속도계(2572)가 방향 화살표(2574)에 의해 표시된 바와 같이 이동 장치(2500)의 이동을 탐지하는 데 활용될 수 있다. 따라서, 디스플레이 객체들 및/또는 미디어는 탐지된 방향에 따라, 예컨대 세로 또는 가로로 제시될 수 있다. 일부 구현예들에서, 이동 장치(2500)는 GPS(Global Positioning System) 또는 다른 위치 파악 시스템들{예컨대 와이파이 액세스 포인트, 텔레비전 신호, 셀룰러 그리드(cellular grid), URL(Uniform Resource Locator)을 사용하는 시스템들}에 의해 제공되는 것과 같은 위치 결정 능력을 지원하기 위한 회로 및 센서들을 포함할 수 있다. 일부 구현예들에서, 위치 파악 시스템(예컨대 GPS 수신기)은 이동 장치(2500) 내에 통합되거나, 또는 위치 기반 서비스에 대한 액세스를 제공하도록 인터페이스{예컨대 포트 장치(2590)}를 통해 이동 장치(2500)에 연결될 수 있는 별개의 장치로

서 제공될 수 있다.

[0086] 일부 구현예들에서, 포트 장치(2590), 예컨대 USB(Universal Serial Bus) 포트, 또는 도킹(docking) 포트, 또는 소정의 다른 유선 포트 접속이 포함될 수 있다. 포트 장치(2590)는 예컨대 다른 통신 장치들(2500), 네트워크 액세스 장치들, 개인용 컴퓨터, 프린터, 디스플레이 스크린, 또는 데이터를 수신 및/또는 송신할 수 있는 다른 처리 장치들과 같은 다른 컴퓨팅 장치들에 대한 유선 접속을 수립하는 데 활용될 수 있다. 일부 구현예들에서, 포트 장치(2590)는 이동 장치(2500)가 예컨대 TCP/IP, HTTP, UDP 및 임의의 다른 알려진 프로토콜과 같은 하나 이상의 프로토콜을 사용하여 호스트 장치와 동기화되도록 한다.

[0087] 이동 장치(2500)는 또한 카메라 렌즈 및 센서(2580)를 포함할 수 있다. 일부 구현예들에서, 카메라 렌즈 및 센서(2580)는 이동 장치(2500)의 배면 상에 위치할 수 있다. 카메라는 정지 이미지들 및/또는 비디오를 포착할 수 있다.

[0088] 이동 장치(2500)는 또한 802.11b/g 통신 장치(2586) 및/또는 블루투스™ 통신 장치(2588)와 같은 하나 이상의 무선 통신 서브시스템을 포함할 수 있다. 다른 802.x 통신 프로토콜들{예컨대 와이맥스(WiMAX), 와이파이, 3G}, CDMA(Code Division Multiple Access), GSM(Global System for Mobile communications), EDGE(Enhanced Data GSM Environment) 등을 포함하는 다른 통신 프로토콜들이 또한 지원될 수 있다.

[0089] 예시적인 구성 가능한 최상위 그래픽 사용자 인터페이스

[0090] 도 8b는 장치(2500)의 구성 가능한 최상위 그래픽 사용자 인터페이스의 다른 일례를 도시한다. 장치(2500)는 디스플레이 객체들의 상이한 집합을 디스플레이하도록 구성될 수 있다.

[0091] 일부 구현예들에서, 장치(2500)의 하나 이상의 시스템 객체 각각은 자신과 연관된 시스템 객체 속성들의 집합을 갖고, 상기 속성들 중 하나는 시스템 객체에 대한 디스플레이 객체가 최상위 그래픽 사용자 인터페이스에 표현될 것인지 여부를 결정한다. 이러한 속성은 시스템에 의해 자동으로 설정될 수 있거나, 또는 아래에 기술되는 바처럼 소정의 프로그램들 또는 시스템 기능들을 통해 사용자에 의해 설정될 수 있다. 도 8b는 노트 객체(2552)(도 8a에 도시되지 않음)가 장치(2500)의 최상위 그래픽 사용자 인터페이스에 어떻게 추가되고 웹 비디오 객체(2516)가 장치(2500)의 최상위 그래픽 사용자 인터페이스로부터 어떻게 제거되는지(예컨대 노트 시스템 객체와 웹 비디오 시스템 객체의 속성들이 수정되는 경우와 같음)에 관한 예를 도시한다.

[0092] 예시 이동 장치 아키텍처

[0093] 도 9는 이동 장치{예컨대 이동 장치(2500)}의 구현예의 블록도(3000)이다. 이동 장치는 메모리 인터페이스(3002), 하나 이상의 데이터 프로세서, 이미지 프로세서 및/또는 중앙 처리 유닛(3004) 및 주변 인터페이스(3006)를 포함할 수 있다. 메모리 인터페이스(3002), 하나 이상의 프로세서(3004) 및/또는 주변 인터페이스(3006)는 별개의 컴포넌트들일 수 있거나 또는 하나 이상의 집적 회로에 통합될 수 있다. 이동 장치 내의 다양한 컴포넌트는 하나 이상의 통신 버스 또는 신호 라인에 의해 연결될 수 있다.

[0094] 센서들, 장치들 및 서브시스템들은 복수의 기능을 촉진하도록 주변 인터페이스(3006)에 연결될 수 있다. 예컨대, 움직임 센서(3010), 광 센서(3012) 및 근접 센서(3014)는 도 8a에 관하여 기술된 방향, 조명 및 근접 기능들을 촉진하도록 주변 인터페이스(3006)에 연결될 수 있다. 위치 파악 시스템(예컨대 GPS 수신기), 온도 센서, 생체 인식 센서, 또는 다른 감지 장치와 같은 다른 센서들(3016)이 또한 관련된 기능들을 촉진하도록 주변 인터페이스(3006)에 접속될 수 있다.

[0095] 카메라 서브시스템(3020) 및 광학 센서(3022), 예컨대 CCD(Charged Coupled Device) 또는 CMOS(Complementary Metal-Oxide Semiconductor) 광학 센서가 사진들 및 비디오 클립들을 기록하는 것과 같은 카메라 기능들을 촉진하도록 활용될 수 있다.

[0096] 통신 기능들은 무선 주파수 수신기들 및 송신기들 및/또는 광학(예컨대 적외선) 수신기들 및 송신기들을 포함할 수 있는 하나 이상의 무선 통신 서브시스템(3024)을 통해 촉진될 수 있다. 통신 서브시스템(3024)의 특정한 설계 및 구현은 이동 장치가 동작하도록 예정되는 통신 네트워크(들)에 의존할 수 있다. 예컨대, 이동 장치는 GSM 네트워크, GPRS 네트워크, EDGE 네트워크, 와이파이 또는 와이맥스 네트워크 및 블루투스™ 네트워크 상에서 동작하도록 설계된 통신 서브시스템들(3024)을 포함할 수 있다. 특히, 무선 통신 서브시스템들(3024)은 이동 장치가 다른 무선 장치들에 대한 기지국으로서 구성될 수 있도록 호스팅 프로토콜들을 포함할 수 있다.

[0097] 오디오 서브시스템(3026)은 음성 인식, 음성 복제, 디지털 기록 및 전화 기능들과 같은 음성 가능 기능들을 촉

진하도록 스피커(3028) 및 마이크(3030)에 연결될 수 있다.

[0098] I/O 서브시스템(3040)은 터치 스크린 제어기(3042) 및/또는 다른 입력 제어기(들)(3044)를 포함할 수 있다. 터치 스크린 제어기(3042)는 터치 스크린(3046)에 연결될 수 있다. 예컨대, 터치 스크린(3046) 및 터치 스크린 제어기(3042)는 정전식, 저항식, 적외선 및 표면 음파 기술들을 포함하지만 이에 한정되지 않는 복수의 터치 감지 기술 중 임의의 것뿐만 아니라 다른 근접 센서 어레이들 또는 터치 스크린(3046)과의 하나 이상의 접촉 지점을 결정하기 위한 다른 요소들을 사용하여 접촉 및 이동 또는 그 중단을 탐지할 수 있다.

[0099] 다른 입력 제어기(들)(3044)은 하나 이상의 버튼, 로커(rocker) 스위치, 썸휠(thumbwheel), 적외선 포트, USB 포트 및/또는 스타일러스와 같은 포인터 장치와 같은 다른 입력/제어 장치들(3048)에 연결될 수 있다. 하나 이상의 버튼(도시되지 않음)은 스피커(3028) 및/또는 마이크(3030)의 음량 제어를 위한 업/다운 버튼을 포함할 수 있다.

[0100] 일 구현예에서, 제1 지속 시간 동안 버튼을 누르는 것은 터치 스크린(3046)의 잠금을 해제할 수 있고, 제1 지속 시간보다 긴 제2 지속 시간 동안 버튼을 누르는 것은 이동 장치에 대한 전원을 켜거나 끌 수 있다. 사용자가 하나 이상의 버튼들의 기능을 커스터마이징하는 것이 가능할 수 있다. 터치 스크린(3046)은 또한 예컨대 가상 또는 소프트 버튼들 및/또는 키보드를 구현하는 데 사용될 수 있다.

[0101] 일부 구현예들에서, 이동 장치는 MP3, AAC 및 MPEG 파일들과 같은 기록된 오디오 및/또는 비디오 파일들을 제시할 수 있다. 일부 구현예들에서, 이동 장치는 iPod™과 같은 MP3 재생기의 기능을 포함할 수 있다. 이동 장치는 따라서 iPod™과 호환 가능한 32핀 접속기를 포함할 수 있다. 다른 입력/출력 및 제어 장치들이 또한 사용될 수 있다.

[0102] 메모리 인터페이스(3002)가 메모리(3050)에 연결될 수 있다. 메모리(3050)는 고속 RAM(Random Access Memory) 및/또는 하나 이상의 자기 디스크 저장 장치, 하나 이상의 광학 저장 장치 및/또는 플래시 메모리(예컨대 NAND, NOR)와 같은 비휘발성 메모리를 포함할 수 있다. 메모리(3050)는 Darwin, RTXC, LINUX, UNIX, OS X, WINDOWS, 또는 VxWorks와 같은 내장형 운영 체제와 같은 운영 체제(3052)를 저장할 수 있다. 운영 체제(3052)는 기본 시스템 서비스들을 취급하고 하드웨어 의존적인 작업들을 수행하기 위한 명령어들을 포함할 수 있다. 일부 구현예들에서, 운영 체제(3052)는 커널(예컨대 UNIX 커널)일 수 있다.

[0103] 메모리(3050)는 또한 하나 이상의 추가적인 장치, 하나 이상의 컴퓨터 및/또는 하나 이상의 서버와의 통신을 촉진하기 위한 통신 명령어들(3054)을 저장할 수 있다. 메모리(3050)는 그래픽 사용자 인터페이스 처리를 촉진하기 위한 그래픽 사용자 인터페이스 명령어들(3056), 센서 관련 처리 및 기능들을 촉진하기 위한 센서 처리 명령어들(3058), 전화 관련 프로세스들 및 기능들을 촉진하기 위한 전화 명령어들(3060), 전자 메시징 관련 프로세스들 및 기능들을 촉진하기 위한 전자 메시징 명령어들(3062), 웹 브라우징 관련 프로세스들 및 기능들을 촉진하기 위한 웹 브라우징 명령어들(3064), 미디어 처리 관련 프로세스들 및 기능들을 촉진하기 위한 미디어 처리 명령어들(3066), GPS 및 내비게이션 관련 프로세스들 및 기능들을 촉진하기 위한 GPS/내비게이션 명령어들(3068), 카메라 관련 프로세스들 및 기능들을 촉진하기 위한 카메라 명령어들(3070) 및/또는 다른 프로세스들 및 기능들을 촉진하기 위한 다른 소프트웨어 명령어들(3072)을 포함할 수 있다. 메모리(3050)는 또한 웹 비디오 관련 프로세스들 및 기능들을 촉진하기 위한 웹 비디오 명령어들 및/또는 웹 쇼핑 관련 프로세스들 및 기능들을 촉진하기 위한 웹 쇼핑 명령어들과 같은 다른 소프트웨어 명령들(도시되지 않음)을 저장할 수 있다. 일부 구현예들에서, 미디어 처리 명령어들(3066)은 오디오 처리 관련 프로세스들 및 기능들과 비디오 처리 관련 프로세스들 및 기능들을 각각 촉진하기 위한 오디오 처리 명령어들 및 비디오 처리 명령어들로 분할될 수 있다. 활성화 기록 및 IMEI(International Mobile Equipment Identity)(3074) 또는 유사한 하드웨어 식별자가 또한 메모리(3050)에 저장될 수 있다.

[0104] 이상에 비추어 보면, 애플리케이션들이 일반적으로 하나 이상의 다른 신뢰 주체에 의해 제공되는 실행 환경에서 사업자들이 애플리케이션들을 개발 및 시험하도록 하기 위해 실행 프로파일들을 시행하는 것을 포함할 수 있는 문제들을 실시예들이 극복함을 인식할 것이다. 또한, 기업들과 같은 장치 공급자들은 맞춤 개발된 애플리케이션들을 신뢰 주체들을 통해 배포하지 않고 이러한 애플리케이션들을 배포할 수 있는 유연성을 제공받을 수 있다.

[0105] 당업자들은 본 명세서에 개시된 실시예들과 관련하여 기술된 다양한 예시적인 논리 블록, 모듈, 회로 및 알고리즘 단계가 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 조합들로서 구현될 수 있음을 인식할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 교환 가능성을 명확히 예시하기 위해, 다양한 예시적인 컴포넌트, 블록, 모

듈, 회로 및 단계가 일반적으로 이들의 기능 면에서 앞서 기술되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지의 여부는 특정한 응용예 및 전체 시스템에 부과되는 설계 제약들에 의존한다. 당업자들은 기술된 기능을 각각의 특정한 응용예를 위한 다양한 방식으로 구현할 수 있지만, 이러한 구현 결정들은 본 발명의 범위로부터의 일탈을 야기하는 것으로 해석되지 않아야 한다.

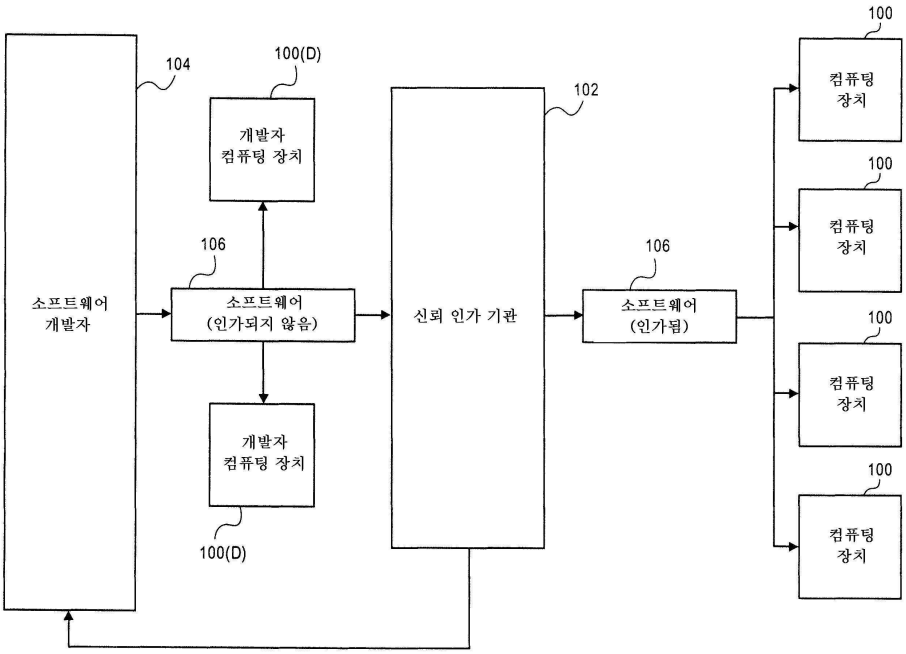
[0106] 본 명세서에 개시된 실시예들과 관련하여 기술된 다양한 예시적인 논리 블록, 모듈 및 회로는 범용 프로세서, DSP(Digital Signal Processor), ASIC(Application Specific Integrated Circuit), FPGA(Field Programmable Gate Array) 또는 다른 프로그램 가능한 로직 장치, 개별 게이트 또는 트랜지스터 로직, 개별 하드웨어 컴포넌트들, 또는 본 명세서에 기술된 기능들을 수행하도록 설계된 이들의 임의의 조합으로 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 선택적으로 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로 제어기(microcontroller), 또는 상태 머신(state machine)일 수 있다. 프로세서는 또한 컴퓨팅 장치들의 조합, 예컨대 DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서, DSP 코어와 관련된 하나 이상의 마이크로프로세서, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0107] 본 명세서에 개시된 실시예들과 관련하여 기술된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 프로세서에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 그 둘의 조합으로 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 본 기술 분야에 알려진 임의의 다른 형태의 저장 매체 내에 상주할 수 있다. 예시적인 저장 매체는 프로세서에 연결되어 프로세서가 저장 매체로부터 정보를 읽고 저장 매체에 정보를 기록할 수 있도록 한다. 선택적으로, 저장 매체는 프로세서에 통합될 수 있다. 프로세서 및 저장 매체는 ASIC 내에 상주할 수 있다. ASIC은 사용자 터미널 내에 상주할 수 있다. 선택적으로, 프로세서 및 저장 매체는 사용자 터미널 내의 개별 컴포넌트들로서 상주할 수 있다.

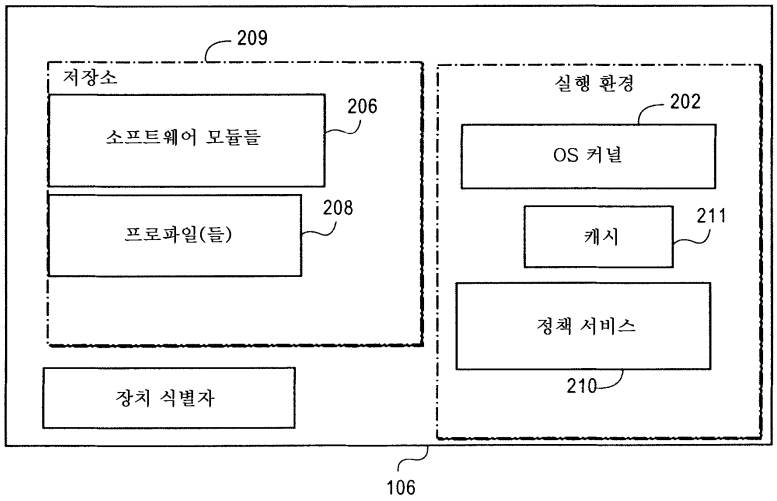
[0108] 이상의 상세한 설명은 다양한 실시예에 적용되는 바와 같은 본 발명의 신규한 특징들을 도시, 기술 및 지적하였지만, 예시된 장치 또는 프로세스의 형태 및 세부 사항들에 있어서 다양한 생략, 치환 및 변경이 본 기술 분야의 당업자에 의해 본 발명의 취지로부터 벗어나지 않고 이루어질 수 있다. 인식되는 바처럼, 본 발명은 본 명세서에 제시된 특징들 및 이점들 모두를 제공하는 것은 아닌 형태 내에서 구현될 수 있는데, 일부 특징들은 다른 특징들과 별개로 사용 또는 실시될 수 있기 때문이다. 본 발명의 범위는 이상의 설명에 의해서가 아닌 첨부된 청구항들에 의해 나타내어진다. 청구항들의 등가물의 의미 및 범위 내에 있게 되는 모든 변화는 이들의 범위 내에서 포괄될 것이다.

도면

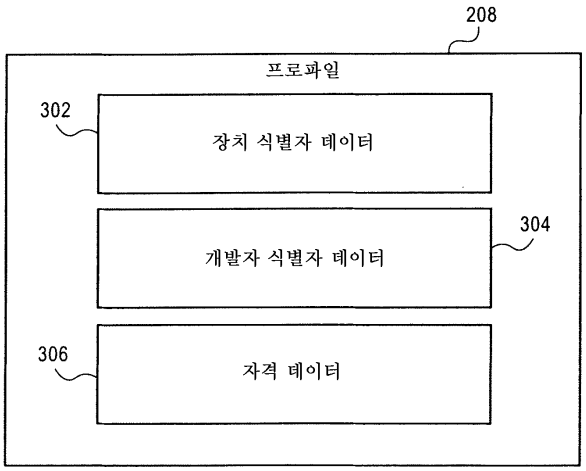
도면1



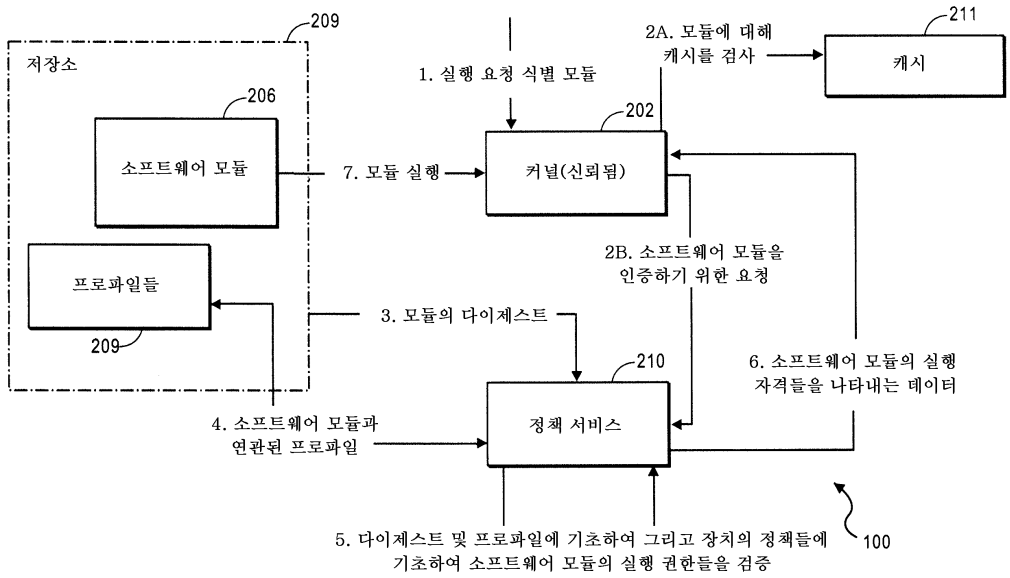
도면2


209
저장소
206
소프트웨어 모듈들
208
프로파일(들)
장치 식별자
실행 환경
202
OS 커널
211
캐시
정책 서비스
210
106

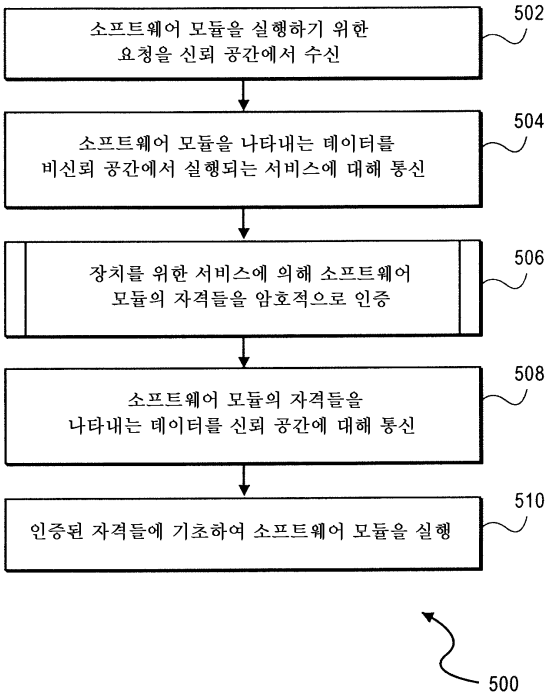
도면3


208
프로파일
302
장치 식별자 데이터
304
개발자 식별자 데이터
306
자격 데이터

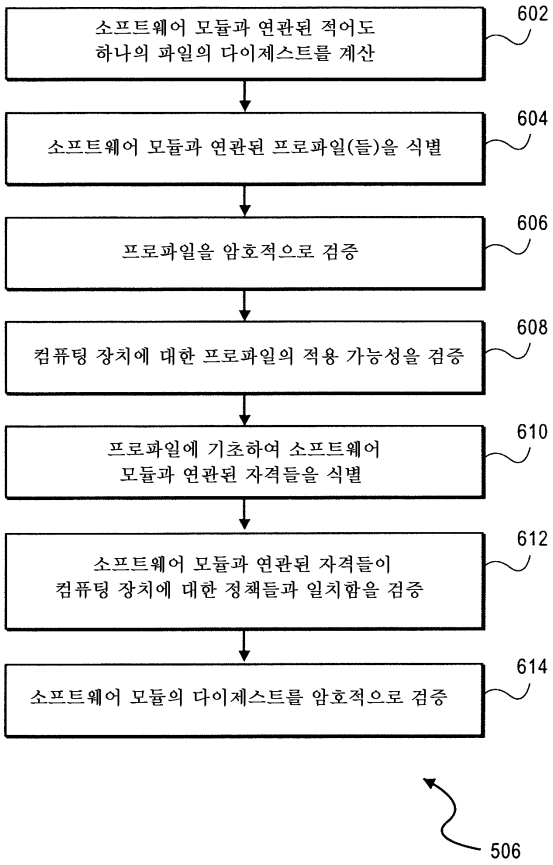
도면4


209
저장소
206
소프트웨어 모듈
프로파일들
209
1. 실행 요청 식별 모듈
2A. 모듈에 대해
캐시를 검사
211
캐시
202
7. 모듈 실행
커널(신뢰됨)
2B. 소프트웨어 모듈을
인증하기 위한 요청
3. 모듈의 다이제스트
210
6. 소프트웨어 모듈의 실행
자격들을 나타내는 데이터
4. 소프트웨어 모듈과
연관된 프로파일
정책 서비스
5. 다이제스트 및 프로파일에 기초하여 그리고 장치의 정책들에
기초하여 소프트웨어 모듈의 실행 권한들을 검증
100

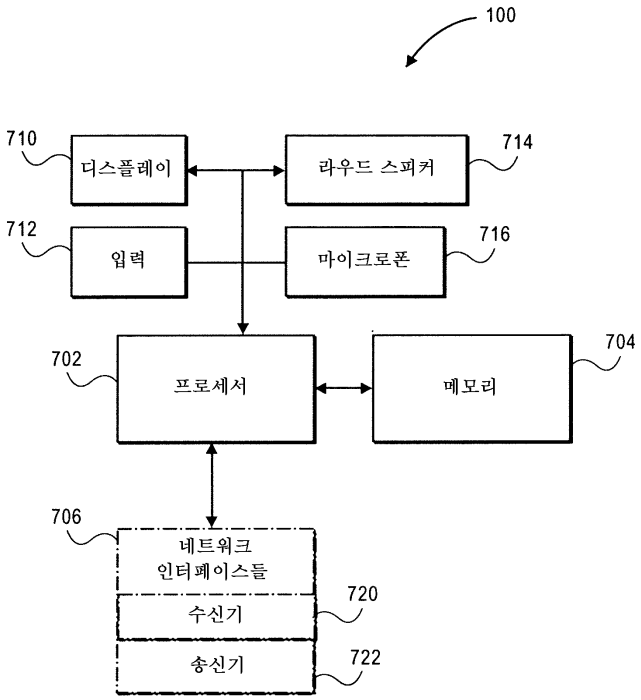
도면5


소프트웨어 모듈을 실행하기 위한
요청을 신뢰 공간에서 수신
502
소프트웨어 모듈을 나타내는 데이터를
비신뢰 공간에서 실행되는 서비스에 대해 통신
504
장치를 위한 서비스에 의해 소프트웨어
모듈의 자격들을 암호적으로 인증
506
소프트웨어 모듈의 자격들을
나타내는 데이터를 신뢰 공간에 대해 통신
508
인증된 자격들에 기초하여 소프트웨어 모듈을 실행
510
500

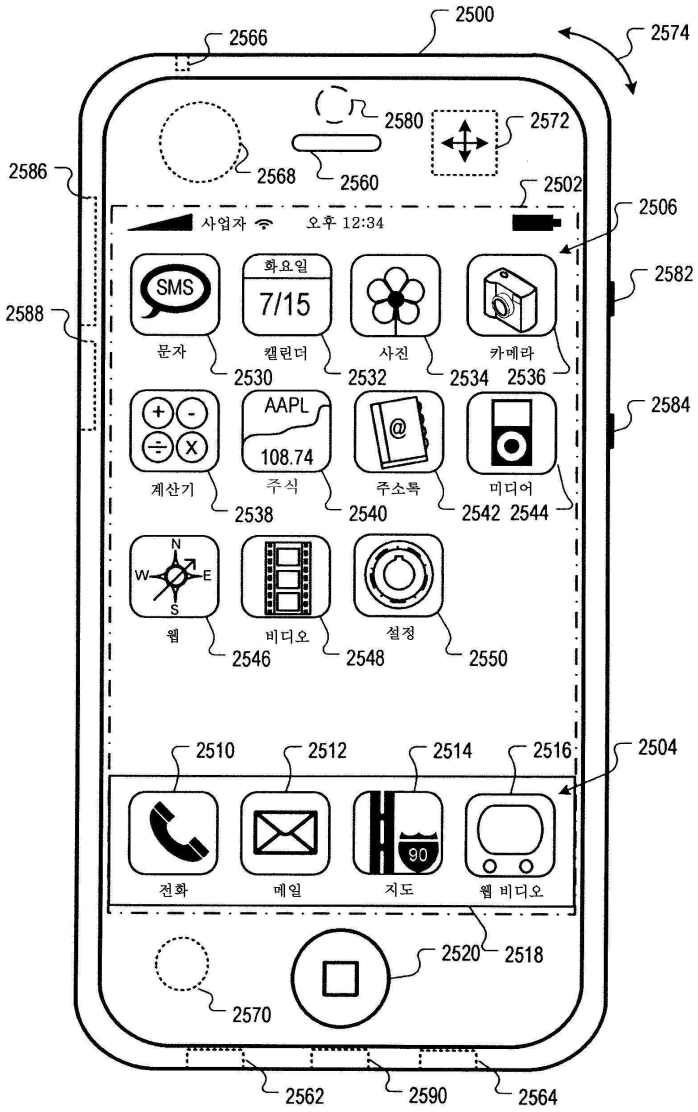
도면6


소프트웨어 모듈과 연관된 적어도 하나의 파일의 다이제스트를 계산
602
소프트웨어 모듈과 연관된 프로파일(들)을 식별
604
프로파일을 암호적으로 검증
606
컴퓨팅 장치에 대한 프로파일의 적용 가능성을 검증
608
프로파일에 기초하여 소프트웨어 모듈과 연관된 자격들을 식별
610
소프트웨어 모듈과 연관된 자격들이 컴퓨팅 장치에 대한 정책들과 일치함을 검증
612
소프트웨어 모듈의 다이제스트를 암호적으로 검증
614
506

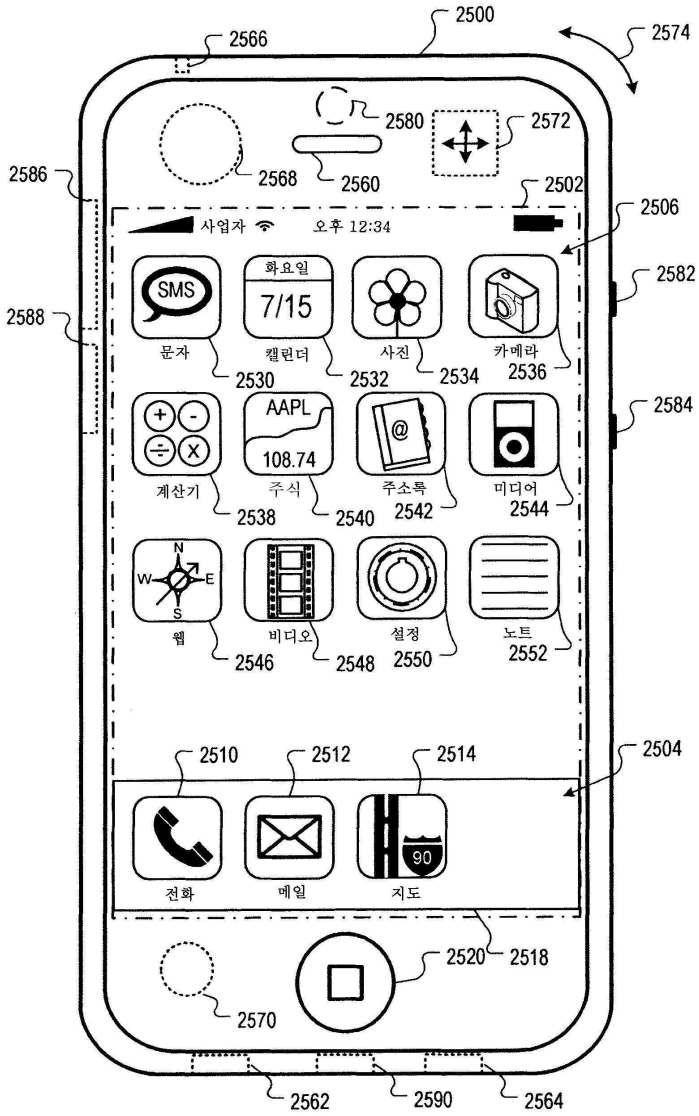
도면7


100
710
디스플레이
714
라우드 스피커
712
입력
716
마이크로폰
702
프로세서
704
메모리
706
네트워크
인터페이스들
720
수신기
722
송신기

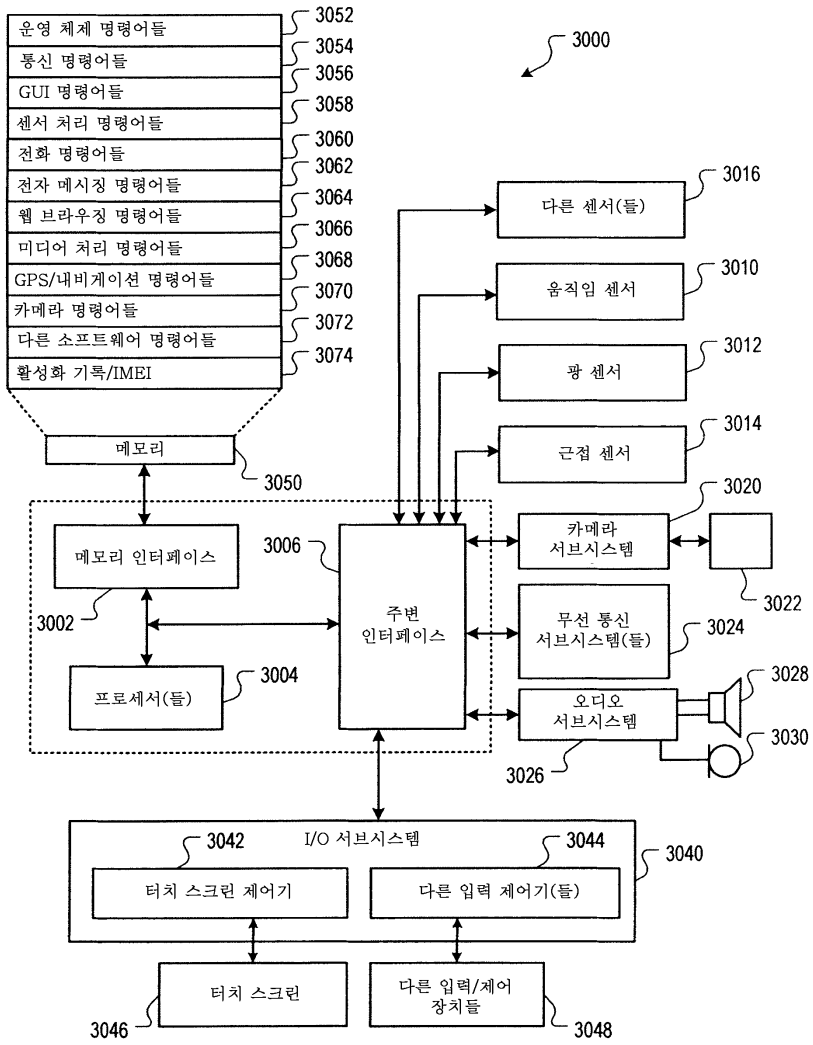
도면8a


2500
2566
2574
2580
2572
2568
2560
2586
2502
2506
사업자
오후 12:34
2582
2588
SMS
화요일
7/15
문자
캘린더
사진
카메라
2530
2532
2534
2536
2584
AAPL
108.74
계산기
주식
주소록
미디어
2538
2540
2542
2544
N
W
E
S
웹
비디오
설정
2546
2548
2550
2510
2512
2514
2516
2504
90
전화
메일
지도
웹 비디오
2520
2518
2570
2562
2590
2564

도면8b


2500
2566
2574
2580
2572
2568
2560
2586
2502
2506
사업자
오후 12:34
2582
SMS
화요일
7/15
2588
문자
캘린더
사진
카메라
2530
2532
2534
2536
2584
AAPL
108.74
계산기
주식
주소록
미디어
2538
2540
2542
2544
N
W
E
S
웹
비디오
설정
노트
2546
2548
2550
2552
2510
2512
2514
2504
90
전화
메일
지도
2520
2518
2570
2562
2590
2564

도면9


운영 체제 명령어들
통신 명령어들
GUI 명령어들
센서 처리 명령어들
전화 명령어들
전자 메시징 명령어들
웹 브라우징 명령어들
미디어 처리 명령어들
GPS/내비게이션 명령어들
카메라 명령어들
다른 소프트웨어 명령어들
활성화 기록/IMEI
3052
3054
3056
3058
3060
3062
3064
3066
3068
3070
3072
3074
3000
메모리
3050
다른 센서(들)
3016
움직임 센서
3010
광 센서
3012
근접 센서
3014
카메라 서브시스템
3020
3022
메모리 인터페이스
3006
3002
주변 인터페이스
무선 통신 서브시스템(들)
3024
프로세서(들)
3004
오디오 서브시스템
3028
3030
3026
I/O 서브시스템
3042
3044
3040
터치 스크린 제어기
다른 입력 제어기(들)
터치 스크린
다른 입력/제어 장치들
3046
3048