(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년12월10일
(11) 등록번호 10-1000630
(24) 등록일자 2010년12월06일

(51) Int. Cl.
H04B 1/40 (2006.01) *H04B 5/02* (2006.01)
H04W 8/24 (2009.01)
(21) 출원번호 10-2009-7007136
(22) 출원일자(국제출원일자) 2006년09월07일
심사청구일자 2009년04월07일
(85) 번역문제출일자 2009년04월07일
(65) 공개번호 10-2009-0068234
(43) 공개일자 2009년06월25일
(86) 국제출원번호 PCT/FI2006/050383
(87) 국제공개번호 WO 2008/028989
국제공개일자 2008년03월13일
(56) 선행기술조사문헌
US20020083228 A1
WO0199925141 A1
WO2006040115 A1
전체 청구항 수 : 총 23 항

(73) 특허권자
노키아 코포레이션
핀란드핀-02150 에스푸 카일알라덴티에 4
(72) 발명자
사리살로 미코
핀란드 에프아이-02460 칸트빅 니이티폴쿠 6 비
(74) 대리인
김창세, 김원준

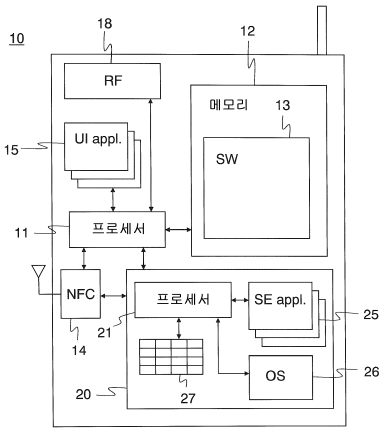
심사관 : 김희주

(54) 보안 모듈 호스팅 장치 및 방법, 보안 모듈 및 프로그램 코드

(57) 요 약

적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈을 호스팅할 수 있는 장치가 개시된다. 이 장치는 보안 모듈로의 연결성을 제공한다. 프로세싱 모듈은 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 보안 모듈로부터 획득한다. 프로세싱 모듈은 획득된 정보에 기초하여 호환가능 대응 애플리케이션이 장치에 존재하는지의 여부를 검사한다. 통신 모듈은 호환가능 대응 애플리케이션이 장치에 존재하지 않는 경우에 외부 소스로부터 호환가능 대응 애플리케이션을 획득한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈을 호스팅할 수 있는 장치로서,

상기 장치는 상기 보안 모듈로의 연결성(connectivity)을 제공하고,

상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하되, 상기 획득된 정보에 기초하여 호환가능 대응 애플리케이션이 상기 장치에 존재하는지의 여부를 검사하는 프로세서와,

상기 프로세서와 연결되며, 호환가능 대응 애플리케이션이 상기 장치에 존재하지 않는 경우, 외부 소스로부터 상기 호환 가능 대응 애플리케이션을 획득하는 통신 모듈을 포함하는

보안 모듈 호스팅 장치.

청구항 2

제 1 항에 있어서,

상기 장치는 상기 보안 모듈로의 연결성을 제공하는 인터페이스를 포함하는

보안 모듈 호스팅 장치.

청구항 3

제 1 항에 있어서,

상기 프로세서는 상기 대응 애플리케이션을 획득하라는 명령을 상기 통신 모듈에 전송하는

보안 모듈 호스팅 장치.

청구항 4

제 1 항에 있어서,

상기 정보는 상기 호환가능 대응 애플리케이션의 명칭 또는 명칭 식별자 및 버전 식별자(version identifier)를 포함하는

보안 모듈 호스팅 장치.

청구항 5

제 1 항에 있어서,

상기 정보는 요구되는 호환가능 대응 애플리케이션을 설치하거나 갱신하는 방법에 대한 인스트럭션을 포함하는

보안 모듈 호스팅 장치.

청구항 6

제 1 항에 있어서,

상기 정보는 상기 호환가능 대응 애플리케이션 또는 갱신이 다운로드될 수 있는 네트워크 리소스를 나타내는

보안 모듈 호스팅 장치.

청구항 7

제 1 항에 있어서,

상기 대응 애플리케이션은 상기 보안 모듈 또는 보안 모듈 애플리케이션용 사용자 인터페이스를 제공하는

보안 모듈 호스팅 장치.

청구항 8

제 1 항에 있어서,

상기 장치는 외부의 비접촉 판독기와 상기 보안 모듈 사이에 정보를 통신하는 근접장 통신 모듈(a near field communication module)을 포함하는

보안 모듈 호스팅 장치.

청구항 9

장치로서,

적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈과,

상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하되, 상기 획득된 정보에 기초하여 상기 장치에 존재하는지를 검사하는 프로세서와,

상기 프로세서와 연결되며, 호환가능 대응 애플리케이션이 상기 장치에 존재하지 않는 경우, 외부 소스로부터 상기 호환 가능 대응 애플리케이션을 획득하는 통신 모듈을 포함하는

장치.

청구항 10

제 9 항에 있어서,

상기 장치는 상기 보안 모듈로의 연결성을 제공하는 인터페이스를 포함하는

장치.

청구항 11

제 9 항에 있어서,

상기 대응 애플리케이션은 상기 보안 모듈 또는 보안 모듈 애플리케이션용 사용자 인터페이스를 제공하는

장치.

청구항 12

제 9 항에 있어서,

상기 장치는 외부의 비접촉 판독기와 상기 보안 모듈 사이에 정보를 통신하는 근접장 통신 모듈을 포함하는

장치.

청구항 13

보안 모듈로서,

상기 보안 모듈 내에 적어도 하나의 보안 모듈 애플리케이션을 설치하는 프로세싱 요소와,

상기 프로세싱 요소에 연결되며,

상기 보안 모듈 애플리케이션에 관한 호환가능 대응 애플리케이션 식별 정보를 상기 보안 모듈 내에 저장하는 메모리를 포함하는

보안 모듈.

청구항 14

제 13 항에 있어서,

상기 보안 모듈은 호스팅 장치로부터 상기 보안 모듈을 액세스하는 인터페이스를 포함하는

보안 모듈.

청구항 15

제 13 항에 있어서,

상기 보안 모듈은 요청자가 요청된 정보를 상기 보안 모듈로부터 수신할 적절한 권리를 갖는지의 여부를 검사하는 보안 검사 모듈을 포함하는

보안 모듈.

청구항 16

제 13 항에 있어서,

상기 보안 모듈은 스마트카드인

보안 모듈.

청구항 17

적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈을 호스팅할 수 있는 장치의 방법으로서,

상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하는 단계와,

상기 획득된 정보에 기초하여, 호환가능 대응 애플리케이션이 상기 장치에 존재하는지의 여부를 검사하는 단계와,

호한 가능한 대응 애플리케이션이 상기 장치에 존재하지 않는 경우에 상기 호환가능 대응 애플리케이션을 외부 소스로부터 획득하는 단계를 포함하는

방법.

청구항 18

제 17 항에 있어서,

상기 정보는 상기 호환가능 대응 애플리케이션의 명칭 또는 명칭 식별자 및 버전 식별자를 포함하는

방법.

청구항 19

제 17 항에 있어서,

상기 정보는 요구되는 호환가능 대응 애플리케이션을 설치 또는 갱신하는 방법에 대한 인스트럭션을 포함하는

방법.

청구항 20

제 17 항에 있어서,

상기 정보는 상기 호환가능 대응 애플리케이션 또는 갱신이 다운로드될 수 있는 네트워크 리소스를 나타내는

방법.

청구항 21

보안 모듈을 관리하는 방법으로서,

적어도 하나의 보안 모듈 애플리케이션을 상기 보안 모듈에 설치하는 단계와,

상기 적어도 하나의 보안 모듈 애플리케이션에 관한 호환가능 대응 애플리케이션 식별 정보를 상기 보안 모듈에

저장하는 단계를 포함하는

방법.

청구항 22

컴퓨터 프로그램을 저장하는 컴퓨터 판독가능 매체로서,

상기 컴퓨터 프로그램은,

적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 보안 모듈로부터 획득하는 컴퓨터 실행가능 프로그램 코드와,

상기 획득된 정보에 기초하여, 호환가능 대응 애플리케이션이 장치에 존재하는지의 여부를 검사하는 컴퓨터 실행가능 프로그램 코드와,

호환가능 대응 애플리케이션이 장치에 존재하지 않는 경우에 외부 소스로부터 상기 호환가능 대응 애플리케이션을 획득하는 컴퓨터 실행가능 프로그램 코드를 포함하는

컴퓨터 판독가능 매체.

청구항 23

컴퓨터 프로그램을 저장하는 컴퓨터 판독가능 매체로서,

상기 컴퓨터 프로그램은,

적어도 하나의 보안 모듈 애플리케이션을 보안 모듈에 설치하는 컴퓨터 판독가능 프로그램 코드와,

상기 적어도 하나의 보안 모듈 애플리케이션에 관한 호환가능 대응 애플리케이션 식별 정보를 상기 보안 모듈 내에 저장하는 컴퓨터 판독가능 프로그램 코드를 포함하는

컴퓨터 판독가능 매체.

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 보안 요소 또는 보안 모듈 애플리케이션에 관한 정보의 관리에 관한 것이다.

배 경 기 술

[0002] 전통적으로, 지불 및/또는 티켓발급 애플리케이션은 신용카드 크기의 플라스틱 스마트 카드 상에 내장된 보안 칩에 상주하고 있다.

[0003] 보다 최근에, 비접촉 지불/티켓발급이 더욱 더 보편화되었을 때, 지불 도구 및/또는 공공 운송 수단 티켓을 포함하는 보안 칩을 이동 전화에 설치하기 시작했다. 일 실시예에서, 이동 디바이스는 무선 주파수 식별(RFID) 모듈일 수 있는 근접장 통신 모듈(a near field communication module) 및 스마트카드 모듈을 포함한다. 스마트카드 모듈은 필요한 보안 요소 애플리케이션, 예를 들어 지불/티켓발급 애플리케이션을 포함하는 보안 요소이다. 보안 요소 애플리케이션은 이동 디바이스의 콘텍스트 및/또는 위치에 기초하여 사용자에 의해 또는 자동으로 시작될 수 있다. 예를 들어, 이동 디바이스가 포스 단말기(a point of sales terminal)의 영역에 위치한다면, 보안 요소 애플리케이션은 자동으로 시작할 수 있다. 근접장 통신 모듈이 기동되고, 후속하여 비접촉 지불 트랜잭션이 실행될 수 있다.

[0004] 보안 요소 애플리케이션을 포함하는 보안 요소가 이동 전화에 설치되므로, 이것은 편리한 특징, 즉 보안 요소에 저장된 다양한 애플리케이션을 관측 및 제어하는 수단을 전화의 사용자에게 제공하는 사용자 인터페이스를 인에이블링할 가능성을 인에이블링한다. 이동 디바이스의 사용자 인터페이스는 보안 요소에 대한 사용자 인터페이스로서 사용될 수 있다. 일반적으로, 이것은 2개의 애플리케이션, 즉 보안 요소에 설치되어 보안 중요 기능(the security critical functionality)을 제공하는 제 1 애플리케이션(보안 요소 애플리케이션)과, 이동 전화 내에 설치되어 적절한 보안 레벨이 제공된 경우에 제 1 애플리케이션을 제어하고 사용자 인터페이스를 제공하는 제 2 애플리케이션(사용자 인터페이스 애플리케이션)을 필요로 한다. 2개의 전혀 다른 애플리케이션을 제공하였으므로, 전체 기능은 이들 2개의 애플리케이션이 동조하지 않고 그에 의해 적절한 동작을 붕괴시킬 위험성을 가져온다.

[0005] 다시 말해, 몇몇 이유로 이동 디바이스가 필요한 대응 애플리케이션(사용자 인터페이스 애플리케이션)을 갖지 않을 때에는 사용자 인터페이스 기능이 디스에이블링될 것이다. 이것은, 예를 들어 보안 요소가 이동 디바이스로부터 다른 디바이스(이 디바이스는 필요한 애플리케이션을 포함하지 않음)로 변경될 때 또는 전화의 소프트웨어가 갱신되고 있을 때 발생할 수 있다.

발명의 상세한 설명

[0006] 본 발명의 제 1 양상에 따르면, 적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈을 호스팅할 수 있

는 장치로서, 상기 장치는 상기 보안 모듈로의 연결성(connectivity)을 제공하고, 상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하되, 상기 획득된 정보에 기초하여 호환가능 대응 애플리케이션이 상기 장치에 존재하는지의 여부를 검사하는 프로세싱 모듈과, 상기 프로세싱 모듈과 연결되며, 호환가능 대응 애플리케이션이 상기 장치에 존재하지 않는 경우, 외부 소스로부터 상기 호환 가능 대응 애플리케이션을 획득하는 통신 모듈을 포함하는 보안 모듈 호스팅 장치가 제공된다.

[0007] 일 실시예에서, 대응 애플리케이션은 보안 모듈 외부의 (호스팅) 장치에 존재하는 호환가능 애플리케이션이다. 일 실시예에서, 대응 애플리케이션은 보안 요소 애플리케이션과 함께 동작하도록 설계된 애플리케이션이다. 일 실시예에서, 대응 애플리케이션은 이동국에서 사용자 인터페이스에 보안 모듈을 제공하는 애플리케이션이다. 일 실시예에서, 대응 애플리케이션은 외부로부터의 보안 모듈의 동작을 제어하는 제어 애플리케이션이다. 다른 실시예에서, 대응 애플리케이션은 보안 모듈을 관리하는 다른 애플리케이션이다.

[0008] 본 발명의 제 2 양상에 따르면, 적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈과, 상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하되, 상기 획득된 정보에 기초하여 상기 장치에 존재하는지를 검사하는 프로세싱 모듈과, 상기 프로세싱 모듈과 연결되며, 호환가능 대응 애플리케이션이 상기 장치에 존재하지 않는 경우, 외부 소스로부터 상기 호환 가능 대응 애플리케이션을 획득하는 통신 모듈을 포함하는 장치가 제공된다.

[0009] 일 실시예에서, 이동 단말과 같은 호스팅 장치는 보안 모듈 내에서 인터페이스 정보를 통해 액세스한다. 일 실시예에서, 액세스된 정보는 하나 이상의 원거리 소스로부터 단말로 제어 또는 사용자 인터페이스 소프트웨어를 페치(fetch)하는 방법에 대한 인스트럭션을 포함한다. 이동 단말이 이미 설치된 이러한 소프트웨어를 갖지 않는 경우, 소프트웨어가 페치될 수 있다. 페치된 소프트웨어의 도움으로, 단말의 사용자는 보안 모듈에 저장된 다양한 보안 모듈 애플리케이션을 액세스 및 관리할 수 있다.

[0010] 본 발명의 제 3 양상에 따르면, 상기 보안 모듈 내에 적어도 하나의 보안 모듈 애플리케이션을 설치하는 프로세싱 요소와, 상기 프로세싱 요소에 연결되며, 상기 보안 모듈 애플리케이션에 관한 호환가능 대응 애플리케이션 식별 정보를 상기 보안 모듈 내에 저장하는 메모리를 포함하는 보안 모듈이 제공된다.

[0011] 일 실시예에서, 보안 모듈은, 이동 단말의 사용자 인터페이스의 도움으로 보안 요소 내에 저장된 애플리케이션(들)을 관리하는 적절한 데이터를 포함하는 전용 레지스트리 또는 데이터베이스를 (애플리케이션 특정 보안 이유로) 물리적 집적 회로일 수 있는 보안 모듈 내에 지속시킨다.

[0012] 본 발명의 제 4 양상에 따르면, 적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈을 호스팅할 수 있는 장치의 방법으로서, 상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하는 단계와, 상기 획득된 정보에 기초하여, 호환가능 대응 애플리케이션이 상기 장치에 존재하는지의 여부를 검사하는 단계와, 호한 가능한 대응 애플리케이션이 상기 장치에 존재하지 않는 경우에 상기 호환가능 대응 애플리케이션을 외부 소스로부터 획득하는 단계를 포함하는 방법이 제공된다.

[0013] 일 실시예에서, 보안 모듈 애플리케이션 레지스트리는 보안 모듈 내에 구현된다. 일 실시예에서, 레지스트리는 보안 모듈 내에 저장된 각각의 보안 모듈 애플리케이션에 대한 엔트리를 포함한다. 엔트리는 이동 단말의 대응 애플리케이션, 예를 들어 사용자 인터페이스 또는 제어 애플리케이션에 대한 명칭, 벤더(vendor) 및 재설치/갱신 인스트럭션과 같은 다양한 정보를 포함할 수 있다. 일 실시예에서, 레지스트리는 사용자 인터페이스/제어 애플리케이션의 설치 또는 맞물림(engagement)에 관한 그 밖의 정보도 포함할 수 있다. 보안 모듈 애플리케이션에 대응하는 소프트웨어가 이동 단말 내에서 분실되거나 또는 사용자 인터페이스/제어 애플리케이션의 필요성이 몇 가지 이유 또는 그 밖의 이유로 발생한 경우, 이동 단말 소프트웨어는 이 레지스트리를 참고하여 단말 사용자 인터페이스 애플리케이션이 보안 모듈 내에서 저장된 애플리케이션(들)과 동조한 상태를 지속하고 계속 보존하는 데 도움이 되게 할 수 있다.

[0014] 본 발명의 제 5 양상에 따르면, 보안 모듈을 관리하는 방법으로서, 적어도 하나의 보안 모듈 애플리케이션을 상기 보안 모듈에 설치하는 단계와, 상기 적어도 하나의 보안 모듈 애플리케이션에 관한 호환가능 대응 애플리케이션 식별 정보를 상기 보안 모듈에 저장하는 단계를 포함하는 방법이 제공된다.

[0015] 일 실시예에서, 보안 모듈은 비접촉 지불/티켓발급 애플리케이션과 같은 보안 모듈 애플리케이션의 사용을 인에이블링하는 호스팅 장치의 근접장 통신 모듈 또는 RFID 통신 모듈과 직접 통신하는 보안 스마트카드 칩이다.

[0016] 본 발명의 제 6 양상에 따르면, 컴퓨터 판독가능 매체에 저장되어, 장치가 제 4 양상에 따른 방법을 수행하게

하는 컴퓨터 실행가능 프로그램 코드를 포함하는 컴퓨터 프로그램이 제공된다.

[0017] 본 발명의 제 7 양상에 따르면, 컴퓨터 판독가능 매체에 저장되어, 보안 모듈이 제 5 양상에 따른 방법을 수행하게 하는 컴퓨터 실행가능 프로그램 코드를 포함하는 컴퓨터 프로그램이 제공된다.

[0018] 본 발명의 제 8 양상에 따르면, 적어도 하나의 보안 모듈 애플리케이션을 포함하는 보안 모듈을 호스팅할 수 있는 장치로서, 상기 보안 모듈로의 연결성을 제공하는 수단과, 상기 적어도 하나의 보안 모듈 애플리케이션에 관한 정보를 상기 보안 모듈로부터 획득하는 수단과, 상기 획득된 정보에 기초하여 호환가능 대응 애플리케이션이 상기 장치에 존재하는지의 여부를 검사하는 수단과, 호환가능 대응 애플리케이션이 상기 장치에 존재하지 않는 경우에 외부로부터 상기 호환가능 대응 애플리케이션을 획득하는 수단을 포함하는 장치가 제공된다.

[0019] 본 발명의 다양한 실시예는 단지 본 발명의 소정 양상을 참조하여 예시되었다. 대응하는 애플리케이션이 다른 양상에도 역시 적용될 수 있음이 이해될 것이다.

실 시 예

[0026] 도 1은 본 발명의 실시예에 따른 장치를 도시한다. 장치(10)는 프로세서(11), 메모리(12) 및 메모리(12) 내에 저장되는 소프트웨어(13)를 포함한다. 소프트웨어(13)는 프로세서(11)가 장치(11)의 동작을 제어하기 위해서 실행하는 인스트럭션을 포함하는 프로그램 코드를 포함한다. 실시예에서, 장치(10)는 이동 단말 또는 이동 전화이다.

[0027] 장치(10)는 프로세서(21), 운영 체제(26) 및 하나 이상의 보안 요소 애플리케이션(25)을 포함하는 보안 모듈 또는 요소(20)를 더 포함한다. 실시예에서, 보안 요소(20)는 장치(10) 내에 영구적으로 집적되거나 탈착 가능하게 부착되거나 제거 가능하게 탑재된 스마트카드 또는 칩이다. 실시예에서, 장치는 보안 요소(20)가 제공될 수 있는 스마트 카드 슬롯을 포함한다. 실시예에서, 보안 요소(20)는 가입자 식별 모듈(SIM)이다. 일반적으로, 보안 요소(20)는 변형 억제성(tamper-resistant)이어야 한다.

[0028] 장치(10)에는 보안 요소(20)에 대한 연결성(connectivity)이 제공된다. 실제로, 장치(10)는 보안 요소의 물리적 핀 커넥터와 접촉하는 스마트카드 인터페이스 또는 인터페이스 모듈(도시하지 않음)을 포함할 수 있다. 인터페이스는 데이터버스(도시하지 않음)를 통해 프로세서(11)에 연결될 수 있다. 보안 요소(20)는 보안 요소(20)에 포함된 상이한 정보에 대해 상이한 보안 레벨을 정의할 수 있다. 장치(10)는 보안 요소(20)로부터의 인터페이스를 통해 정보를 요청할 수 있다. 요청된 정보의 보안 레벨에 따라, 보안 요소(20)는 요청된 정보를 장치(10)에 전달한다. 이를 위해, 보안 요소(20)는, 예를 들어 보안 검사 모듈 또는 유사품(도시하지 않음)을 포함할 수 있다. 이 모듈은 소프트웨어에 의해 또는 소프트웨어와 하드웨어의 적절한 조합에 의해 구현될 수 있다. 그것은 상이한 보안 레벨에서 상이한 정보를 분류하고, 요청자(예를 들어, 장치(10) 또는 장치의 소프트웨어(13))가 요청된 정보를 보안 모듈(20)로부터 수신할 적절한 권리를 갖는지의 여부를 검사한다.

[0029] 보안 요소 애플리케이션(25)은, 예를 들어 지불 애플리케이션 또는 티켓발급 애플리케이션일 수 있다. 애플리케이션(25)은 보안 요소 프로세서(21)에 의해 구동된다. 보안 요소(20)의 운영 체제(26)가 자바인 경우, 보안 요소 애플리케이션(25)은 애플릿이라 호칭될 수 있다. 보안 모듈(20)은 외부로부터 (일반적으로는 패시브) 보안 요소를 액세스하기 위한 인터페이스를 제공한다. 이 인터페이스는 소프트웨어에 의해 또는 소프트웨어 및/또는 하드웨어를 이용한 적절한 구성물 및/또는 물리적 구성물, 예를 들어 핀 커넥터에 의해 제공될 수 있다.

[0030] 장치(10)는 안테나를 갖는 근접장 통신 모듈(14)을 더 포함한다. 근접장 통신 모듈(14)은 프로세서(11) 및 보안 요소(20)에 접속된다. 실시예에서, 근접장 통신 모듈(14)은, 예를 들어 태그 모드에서도 작동하기 위한 수단을 구비한 RFID 판독기와 같은 RFID 통신 모듈이다. POS 단말 또는 비접촉 판독기(도 1에는 도시하지 않음)와 같은 외부 디바이스는 근접장 통신 모듈(14)을 통해 보안 요소(20)와 통신할 수 있다.

[0031] 장치(10)는 프로세서(11)에 의해 구동되는 사용자 인터페이스 애플리케이션(15)을 더 포함한다. 이들은 미들릿(midlets)이라 호칭될 수 있다. 각각의 보안 요소 애플리케이션(25)마다 사용자 인터페이스 애플리케이션(15)이 존재해야 한다. 사용자 인터페이스 애플리케이션(15)은 해당하는 보안 요소 애플리케이션(25)에 대한 사용자 인터페이스를 구현한다. 그러한 방법에서는, 장치(10)의 키보드 및 디스플레이가 보안 요소 애플리케이션(25)에 대한 사용자 인터페이스로서 사용될 수 있다.

[0032] 보안 요소(20)는 레지스트리 테이블 또는 데이터베이스(27)를 갖는다. 테이블(27)은 보안 요소 칩 내부의 별도

의 애플리케이션으로서 구현될 수 있다. 대안으로, 기능은 보안 요소 운영 체제(26) 내에 구현될 수 있다. 이 테이블에는 설치된 보안 요소 애플리케이션(25) 및 대응 사용자 인터페이스 애플리케이션(15)에 대한 정보가 보존된다. 각각의 보안 요소 애플리케이션(25)의 경우, 이 테이블은 장치(10)에 존재해야 하는 대응 애플리케이션(15)을 식별하는 정보를 포함한다. 이 정보는 다양한 방법으로 제시될 수 있다. 예를 들어, 이 정보는 필요한 대응 애플리케이션(15)의 명칭(또는 몇몇 다른 식별자) 및 버전 번호를 포함할 수 있다. 대안의 실시예에서, 테이블(27)은 명칭 및 벤더에 대한 정보를 포함한다. 대안의 실시예에서, 테이블(27)은 필요한 대응 애플리케이션(15)을 설치/갱신하는 방법에 대한 인스트럭션을 포함한다. 장치가 필요한 대응 애플리케이션(15) 또는 필요한 버전의 애플리케이션을 갖지 않는다면, 설치 또는 갱신은 인스트럭션에 따라 수행될 수 있다. 상기 인스트럭션은, 예를 들어 애플리케이션 또는 갱신이 다운로드될 수 있는 네트워크 리소스의 어드레스를 포함할 수 있다. 이 어드레스는 URL(Uniform Resource locator)의 형태일 수 있다.

[0033] 도 2는 테이블(27)의 실시예를 예시한다. 이 실시예에서, 테이블은 (예를 들어, 애플리케이션 및 버전 식별자(version identifier)에 의해 식별되는) 각각의 보안 요소 애플리케이션(25)마다 정확한 대응 애플리케이션(15)을 식별하는 정보 및 이 애플리케이션 또는 갱신이 다운로드될 수 있는 네트워크 사이트를 포함한다.

[0034] 도 3은 본 발명의 실시예에 따른 장치에서 애플리케이션을 설치 및/또는 갱신하는 상이한 루트를 도시한다. 한 가지 대안에 따르면, 보안 요소 애플리케이션 또는 애플리케이션 갱신은 근접장 통신 링크를 이용하여 비접촉 방법을 통해 설치된다. 애플리케이션 및/또는 설치 파일은 근접장 통신 링크를 통한 비접촉 판독기(50)로부터 근접장 통신 모듈(14) 및 설치가 실행되는 보안 요소(20)로 전송된다. 다른 대안에 따르면, 보안 요소 애플리케이션 또는 애플리케이션 갱신은 OTA(on-the-air) 설치 방법을 통해 설치된다. 이 대안에서, 애플리케이션 및/또는 설치 파일은 셀룰러 네트워크 접속 지향 또는 접속 분리 통신 서비스를 이용하여 통신 네트워크(40)를 통해 OTA 서버(30)로부터 장치(10)로 전송된다. 이를 위해, 장치는 프로세서(11)에 연결된 셀룰러 무선 송수신기(18)를 포함한다.

[0035] 도 4는 보안 요소 애플리케이션 또는 애플리케이션 갱신의 설치 프로세스를 예시한 흐름도를 도시한다. 애플리케이션 또는 설치 파일의 수신 시, 보안 요소 프로세서(21)는 보안 요소(20)의 메모리(명료성을 위해 도시하지 않음)에 보안 요소 애플리케이션 또는 애플리케이션 갱신을 설치한다(단계(41)). 새로운 애플리케이션이 설치되면, 엔트리가 테이블(27) 내에 작성된다(단계(42)). 일찍이 제시된 바와 같이, 엔트리는, 예를 들어 정확한 대응 애플리케이션(15)을 식별하는 정보 및 그것을 획득할 장소에 관한 인스트럭션을 포함한다(단계(43)). 설치가 기존 보안 요소 애플리케이션(25)의 갱신이라면, 그에 따라 필요한 경우에 테이블 내의 대응 섹션이 갱신된다(단계(44)). 예를 들어, 갱신된 보안 요소 애플리케이션(25)이 대응 애플리케이션(15)에서의 갱신을 필요로 한다면, 테이블 갱신이 필요할 수 있다.

[0036] 도 5는 실시예에 따라 보안 요소 애플리케이션(25) 및 대응 애플리케이션(15)을 동조 상태로 유지시키는 데 도움이 되는 프로세스를 예시한 흐름도이다. 이 프로세스는 특정 상황, 예를 들어 장치를 작동시킬 때 또는 장치 소프트웨어(실제 장치 소프트웨어 또는 보안 요소 소프트웨어)를 갱신한 직후에 실행될 수 있다. 장치 소프트웨어(13)의 제어 하의 프로세서(11)는, 단계(51)에서 보안 요소 테이블(27)을 판독하고, 단계(52)에서 장치(1)에 설치된 대응 애플리케이션(15)을 검사한다. 장치는 장치에 존재하는 애플리케이션을 알고 있다. 이 정보는 장치 메모리(12), 예를 들어 레지스터 또는 데이터베이스 또는 유사품(도시하지 않음) 내에 보존될 수 있다. 프로세서(11)는 단계(52)에서 이 정보 소스를 참고한다. 단계(53)에서 수행된 비교에 기초하여, 하나 이상의 대응 애플리케이션이 누락되거나, 예를 들어 잘못된 버전을 갖고 있는 것으로 검사되면, 갱신 또는 설치가 트리거되거나 제안된다(단계(54)). 장치 소프트웨어(13)는 갱신 또는 설치를 트리거하여, 사용자 인터페이스 없이, 예를 들어 셀룰러 무선 송수신기(18)를 통한 OTA 설치에 의해 자동으로 수행될 수 있다. 대안으로, 장치 소프트웨어(13)는 사용자로부터 사용자가 갱신 또는 설치의 다운로드를 바라는지를 질문할 수 있다. 장치 소프트웨어는 팝업 윈도우 또는 유사물에 의해 사용자에게 갱신 또는 설치를 제안하고 사용자 응답에 따라 진행할 수 있다.

[0037] 본 발명의 다양한 실시예가 제시되었다. 사용자 인터페이스 애플리케이션이라는 용어가 폭넓게 사용되고 있지만, 대응 애플리케이션은 사용자 인터페이스 애플리케이션으로 제한되는 것이 아니라, 제어 또는 관리 애플리케이션과 같은 다른 대응 애플리케이션 역시 적용될 수 있음은 명백하다.

[0038] 이 문헌에서, 포함하다라는 용어는 배제시키고자하는 의미가 없는 개방적인 표현으로서 사용된다.

[0039] 전술한 설명은 본 발명의 특정 구현예 및 실시예의 비제한적 실례로서 본 발명을 실행하기 위해 발명자에 의해 현재 계획된 가장 양호한 방법 및 장치의 충분하고 유익한 설명을 제공하였다. 그러나, 당업자에게는, 본 발명

이 위에서 제시된 실시예의 세부 사항으로 제한되는 것이 아니라, 본 발명의 특성으로부터 벗어나지 않는 등가의 수단을 이용하는 다른 실시예에서 구현될 수 있음이 명백하다.

[0040] 또한, 본 발명의 전술한 실시예의 특징 중 몇몇은 다른 특징의 해당 사용 없이 유리하게 사용될 수 있다. 이와 같이, 전술한 설명은 단지 본 발명의 원리를 예시하는 것으로 고려되어야 하며, 제한점으로 예시된 것이 아니다. 따라서, 본 발명의 범주는 첨부한 특허청구범위에 의해서만 제한된다.

도면의 간단한 설명

[0020] 본 발명의 첨부한 도면을 참조하여 오로지 실례로서 설명될 것이다.

[0021] 도 1은 본 발명의 실시예에 따른 장치를 도시한 도면,

[0022] 도 2는 본 발명의 실시예에 따른 레지스트리 테이블을 예시한 도면,

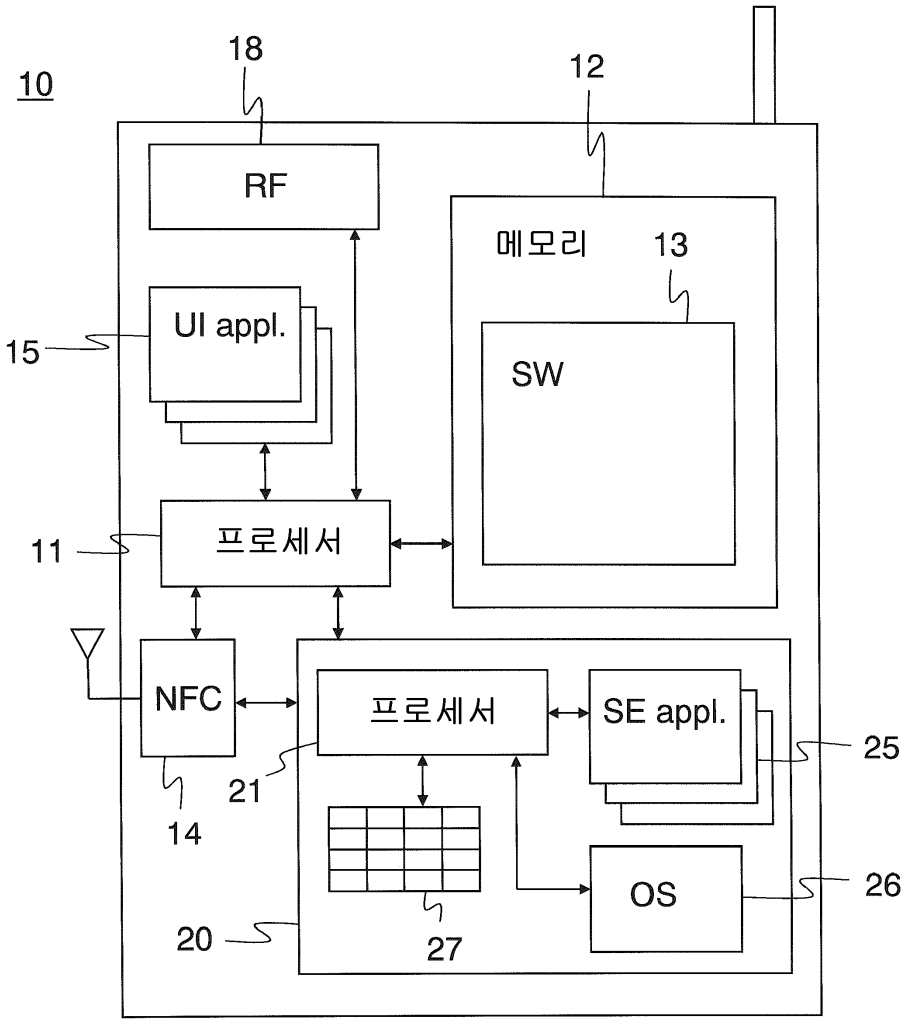
[0023] 도 3은 본 발명의 실시예에 따른 장치에서 애플리케이션을 설치 및/또는 갱신하는 상이한 루트를 도시한 도면,

[0024] 도 4는 본 발명의 실시예에 따른 흐름도,

[0025] 도 5는 본 발명의 다른 실시예에 따른 흐름도이다.

도면

도면1

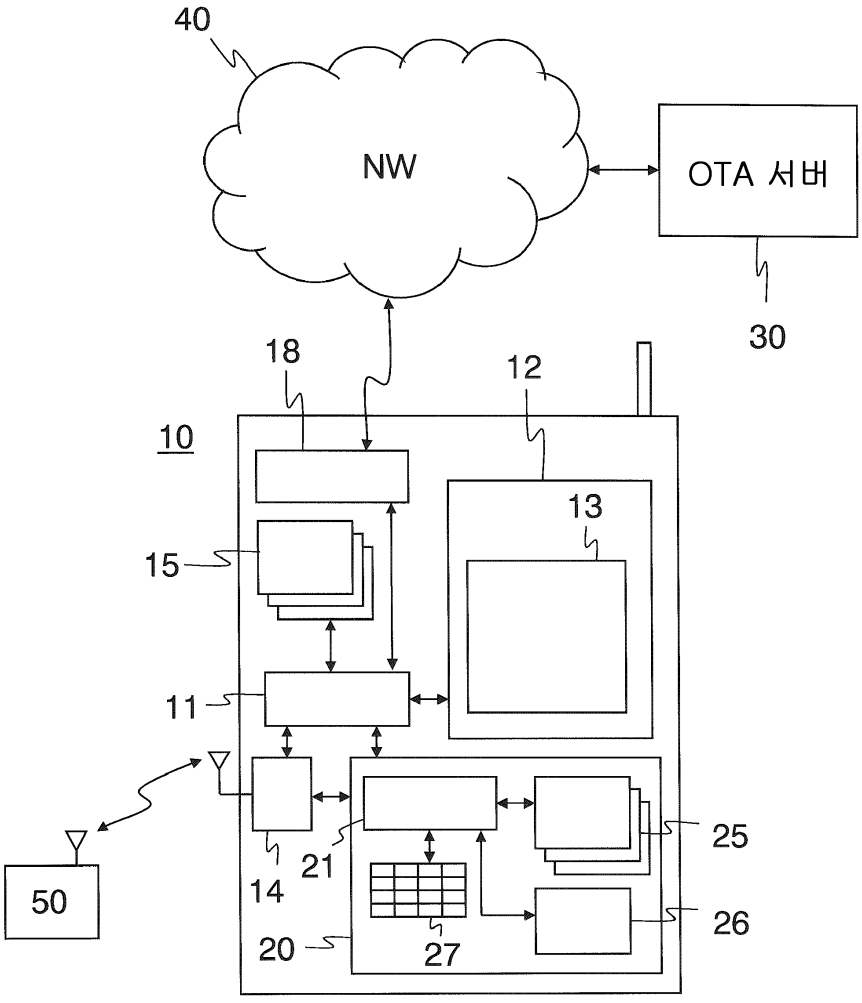


도면2

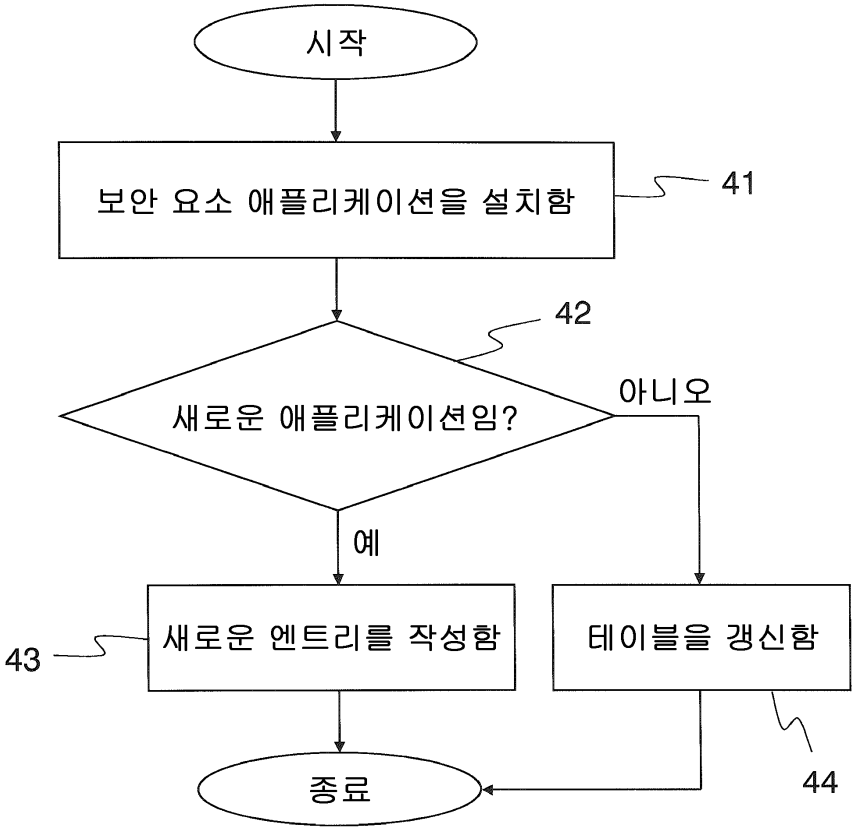
27

SE appln. ID	UI appln. 명칭/ID	UI appln. 버전	UI appln. 사이트/URL
#### ## #	#### ## #	#### ## #	#### ## #
#### ## #	#### ## #	#### ## #	#### ## #
#### ## #	#### ## #	#### ## #	#### ## #

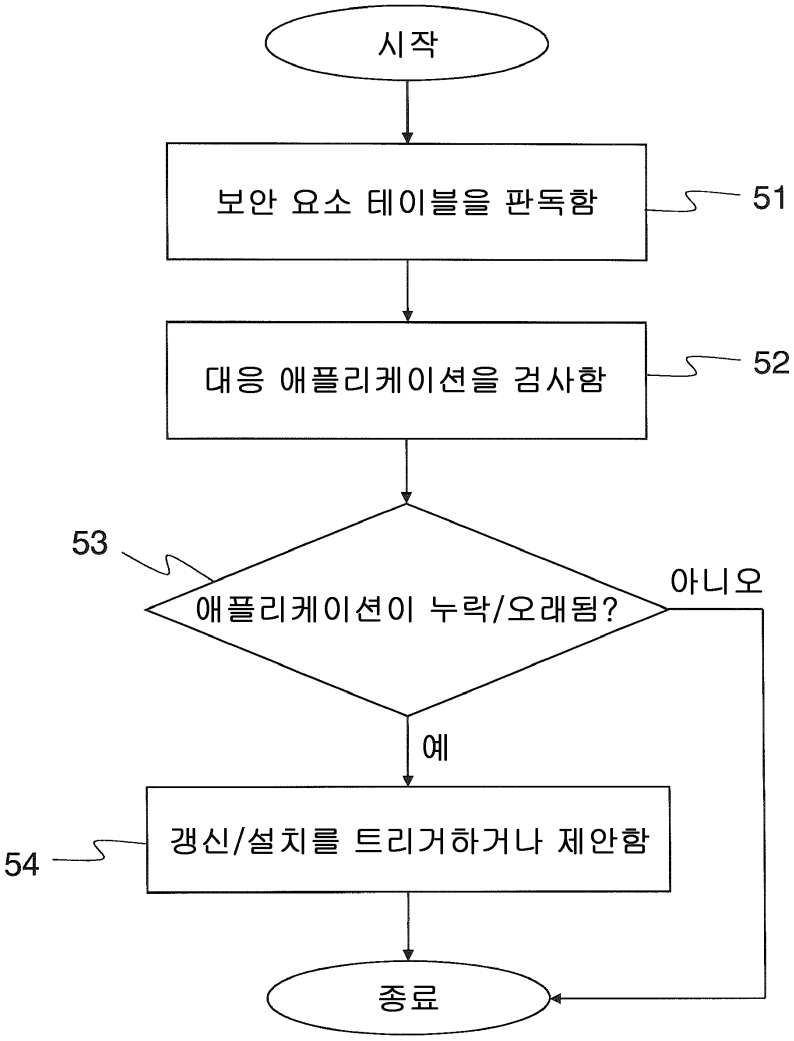
도면3



도면4


시작
보안 요소 애플리케이션을 설치함
41
42
새로운 애플리케이션임?
아니오
예
새로운 엔트리를 작성함
43
테이블을 갱신함
44
종료

도면5


시작
보안 요소 테이블을 판독함
51
대응 애플리케이션을 검사함
52
53
애플리케이션이 누락/오래됨?
아니오
예
54
갱신/설치를 트리거하거나 제안함
종료