(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019 년 10 월 10 일 (10.10.2019)

WIPO | PCT

(10) 국제공개번호
WO 2019/194428 A1

(51) 국제특허분류:
G06F 21/33 (2013.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01)

(21) 국제출원번호: PCT/KR2019/002946

(22) 국제출원일: 2019 년 3 월 14 일 (14.03.2019)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0038366 2018 년 4 월 2 일 (02.04.2018) KR

(71) 출원인: 삼성전자 주식회사 (**SAMSUNG ELECTRONICS CO., LTD.**) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(72) 발명자: 양이 (**YANG, Yi**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 김종환 (**KIM, Jonghwan**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 강문석 (**KANG, Moonseok**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 최보근 (**CHOI, Bokun**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

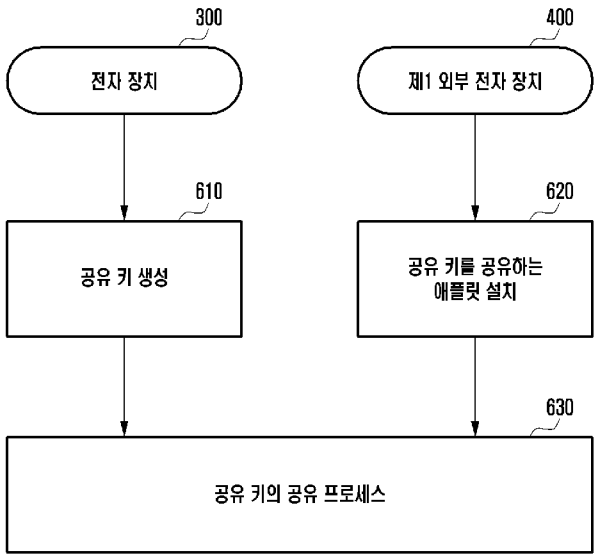
(74) 대리인: 윤앤리특허법인(유한) (**YOON & LEE INTERNATIONAL PATENT & LAW FIRM**); 08502 서울시 금천구 가산디지털1로 226, 에이스 하이엔드타워 5차 3 층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2019/194428 A1

(54) **Title:** ELECTRONIC DEVICE SHARING KEY WITH EXTERNAL ELECTRONIC DEVICE AND OPERATING METHOD FOR ELECTRONIC DEVICE

(54) **발명의 명칭:** 외부 전자 장치의 키를 공유하는 전자 장치 및 전자 장치의 동작 방법



300 ... Electronic device
400 ... First external electronic device
610 ... Generate shared key
620 ... Install applet for sharing shared key
630 ... Sharing process of shared key

(57) **Abstract:** In an electronic device and an operating method for the electronic device according to various embodiments, the electronic device may comprise: a processor; at least one communication module supporting wireless communication; and a security module having an applet installed therein so as to store and manage a shared key to be transmitted to a first external electronic device and an authentication key used to perform authentication with a second external electronic device, wherein the processor is configured to: receive a request for transmission of the authentication key to the first external electronic device; transmit, to the security module, information for generation of the shared key and a command to generate the shared key; perform control such that the security module generates the shared key on the basis of the information for generation of the shared key; and perform control such that the security module transmit, to the first external electronic device, the generated shared key and information associated with the generated shared key. Various other embodiments are possible.

(57) **요약서:** 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 전자 장치는 프로세서, 무선 통신을 지원하는 적어도 하나의 통신 모듈 및 제 1 외부 전자 장치로 전송될 공유 키 및 제 2 외부 전자 장치와의 인증에 이용되는 인증 키의 저장 및 관리를 수행하는 애플릿이 설치된 보안 모듈을 포함하고, 상기 프로세서는 상기 인증 키의 제 1 외부 전자 장치로의 전송의 요청을 수신하고, 상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 상기 보안 모듈에 전송하고, 상기 공유 키 생성을 위한 정보에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈을 제어하고, 상기 생성된 공유 키 및 생성된 공유 키와 관련된 정보를 제 1 외부 전자 장치로 전송하도록 상기 보안 모듈을 제어하도록 설정될 수 있다. 이 밖에 다양한 실시예들이 가능하다.

[다음 쪽 계속]

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 외부 전자 장치의 키를 공유하는 전자 장치 및 전자 장치의 동작 방법

기술분야

[1] 본 발명의 다양한 실시예는, 외부 전자 장치의 키를 공유하는 전자 장치 및 전자 장치의 동작 방법에 관한 것이다.

배경기술

[2] 무선 통신을 통하여 도어락, 운송 수단 등 외부 전자 장치를 제어할 수 있는 스마트 키와 관련된 기술이 개발되고 있다. 예를 들어, 외부 전자 장치가 운송 수단인 경우, 운송 수단의 문의 잠금을 해제하거나, 운송 수단의 엔진의 시동을 켜는 등의 운송 수단이 제공할 수 있는 기능을 수행할 수 있는 스마트 키와 관련된 기술이 개발되고 있다. 스마트 키는 운송 수단과 근거리 통신을 이용해 인증 절차를 수행하고, 인증 완료 후 잠금 해제나 시동 등 운송 수단의 기능을 활성화할 수 있다.

[3] 최근에는 외부 전자 장치의 기능을 활성화하기 위한 별도의 스마트 키를 이용하지 않고, 사용자가 휴대 가능한 스마트폰, 웨어러블 기기 등 휴대 단말을 이용하여 외부 전자 장치가 제공할 수 있는 기능을 수행하는 기술이 등장하고 있다.

발명의 상세한 설명

기술적 과제

[4] 외부 전자 장치의 키의 관리를 위한 어플리케이션은, 보안성을 제공하기 위해서, 휴대 단말에 별도로 구비된 보안 모듈(security module)에 기반한 외부 전자 장치 키 솔루션을 이용할 수 있다.

[5] 외부 전자 장치를 이용하고자 하는 외부 전자 장치의 소유주 이외의 다른 사용자는 자신의 휴대 단말에 외부 전자 장치의 키를 설치함으로써, 외부 전자 장치를 이용할 수 있다. 운송 수단의 키는 외부 전자 장치의 제조사가 제공하는 별도의 키 제공 서버(provisioning server)를 이용하여 공유할 수 있다. 외부 전자 장치의 제조사가 제공하는 키 제공 서버를 이용하는 경우, 별도의 키 제공 비용을 지불해야 한다.

[6] 외부 전자 장치의 제조사가 제공하는 키 제공 서버를 이용하지 않고, 외부 전자 장치의 키를 휴대 단말간 공유하는 경우, 외부 전자 장치의 마스터 키가 여러 휴대 단말간 공유되어 보안에 문제가 발생될 수 있다.

과제 해결 수단

[7] 본 발명의 다양한 실시예에 따른 전자 장치는 프로세서, 무선 통신을 지원하는 적어도 하나의 통신 모듈 및 제 1 외부 전자 장치로 전송될 공유 키 및 제 2 외부 전자 장치와의 인증에 이용되는 인증 키의 저장 및 관리를 수행하는 애플릿이

설치된 보안 모듈을 포함하고, 상기 프로세서는 상기 인증 키의 제 1 외부 전자 장치로의 전송의 요청을 수신하고, 상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 상기 보안 모듈에 전송하고, 상기 공유 키 생성을 위한 정보에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈을 제어하고, 상기 생성된 공유 키 및 생성된 공유 키와 관련된 정보를 제 1 외부 전자 장치로 전송하도록 상기 보안 모듈을 제어하도록 설정될 수 있다.

[8] 본 발명의 다양한 실시예에 따른 전자 장치는 프로세서, 무선 통신을 지원하는 적어도 하나의 통신 모듈 및 제 2 외부 전자 장치의 인증에 이용되는 인증 키를 관리하는 애플릿과 관련된 정보를 관리하고, 애플릿 식별자(applet identification, AID) 리스트 및 상기 애플릿을 저장하는 보안 모듈을 포함하고, 상기 보안 모듈은 상기 애플릿과 관련된 정보를 요청하는 신호를 상기 제 1 외부 전자 장치로부터 수신하고, 상기 애플릿과 관련된 정보를 상기 제 1 외부 전자 장치로 전송하고, 상기 제 1 외부 전자 장치로부터 상기 공유 키 및 상기 공유 키와 관련된 정보를 수신하고, 상기 수신한 공유 키 및 상기 공유 키와 관련된 정보를 상기 보안 모듈 상에 설치하도록 설정될 수 있다.

[9] 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법은 제 2 외부 전자 장치와의 인증에 이용되는 인증 키에 기반하여 생성되는 공유 키의 전송 요청을 상기 제 1 외부 전자 장치로부터 수신하는 동작, 상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 보안 모듈에 전송하는 동작, 상기 정보 및 상기 명령에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈을 제어하는 동작 및 상기 생성된 공유 키 및 상기 생성된 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치로 전송하도록 상기 보안 모듈을 제어하는 동작을 포함할 수 있다.

발명의 효과

[10] 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법은 전자 장치의 보안 모듈에 저장된 마스터 키에 기반하여 생성된 공유 키를 보안을 유지하여 공유할 수 있다.

[11] 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법은 외부 전자 장치의 키를 송/수신하는 전자 장치의 보안 모듈간 통신(secure module to secure module, SE2SE) 규격을 이용하여, 외부 전자 장치의 키를 공유할 수 있어, 별도의 프로비저닝 서버가 요구되지 않아, 프로비저닝 서버로 인한 비용을 줄일 수 있다.

도면의 간단한 설명

[12] 도 1은 본 발명의 다양한 실시예에 따른, 전자 장치의 블록도이다.

[13] 도 2는 본 발명의 다양한 실시예에 따른 전자 장치 상에서 동작하는 프로그램의 블록도이다.

[14] 도 3은 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.

[15] 도 4는 본 발명의 다양한 실시예에 따른 제 1 외부 전자 장치의 블록도이다.

[16] 도 5는 본 발명의 다양한 실시예에 따른 제 1 외부 전자 장치에서, 보안 모듈을 도시한 블록도이다.

[17] 도 6은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법의 동작 흐름도이다.

[18] 도 7은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 제 2 외부 전자 장치의 인증에 이용되는 공유 키를 생성하는 방법을 도시한 동작 흐름도이다.

[19] 도 8은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 생성된 공유 키를 보안 모듈의 키 공유 애플릿에 저장하는 방법을 도시한 동작 흐름도이다.

[20] 도 9는 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 공유 키를 수신하는 제 1 외부 전자 장치 상에 공유 키를 수신하기 위한 애플릿을 설치하는 방법을 도시한 동작 흐름도이다.

[21] 도 10은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 공유 키를 송/수신하는 구체적인 방법을 도시한 동작 흐름도이다.

[22] 도 11은 공유 키를 전송하는 전자 장치가 공유 키를 제 1 외부 전자 장치로 전송하는 전송 모드를 도시한 도면이다.

[23] 도 12는 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 공유 키를 송/수신하는 구체적인 데이터를 도시한 동작 흐름도이다.

[24] 도 13은 공유 키를 전송하는 전자 장치가 공유 키를 전송하는 전송 모드에서 일반 모드로 전환되는 실시예를 도시한 도면이다.

[25] 도 14는 공유 키를 수신한 제 1 외부 전자 장치와 제 2 외부 전자 장치 사이, 제 2 외부 전자 장치가 공유 키의 유효성을 검증하는 실시예를 도시한 도면이다.

발명의 실시를 위한 형태

[26] 도 1은, 다양한 실시예들에 따른, 네트워크 환경(100) 내의 전자 장치(101)의 블럭도이다. 도 1을 참조하면, 네트워크 환경(100)에서 전자 장치(101)는 제 1 네트워크(198)(예: 근거리 무선 통신 네트워크)를 통하여 전자 장치(102)와 통신하거나, 또는 제 2 네트워크(199)(예: 원거리 무선 통신 네트워크)를 통하여 전자 장치(104) 또는 서버(108)와 통신할 수 있다. 일실시예에 따르면, 전자 장치(101)는 서버(108)를 통하여 전자 장치(104)와 통신할 수 있다. 일실시예에 따르면, 전자 장치(101)는 프로세서(120), 메모리(130), 입력 장치(150), 음향 출력 장치(155), 표시 장치(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 포함할 수 있다. 어떤 실시예에서는, 전자 장치(101)에는, 이 구성요소들 중 적어도 하나(예: 표시 장치(160) 또는 카메라 모듈(180))가 생략되거나, 하나 이상의 다른 구성 요소가 추가될 수 있다. 어떤 실시예에서는, 이 구성요소들 중 일부들은 하나의 통합된

회로로 구현될 수 있다. 예를 들면, 센서 모듈(176)(예: 지문 센서, 홍채 센서, 또는 조도 센서)은 표시 장치(160)(예: 디스플레이)에 임베디드된 채 구현될 수 있다

[27] 프로세서(120)는, 예를 들면, 소프트웨어(예: 프로그램(140))를 실행하여 프로세서(120)에 연결된 전자 장치(101)의 적어도 하나의 다른 구성요소(예: 하드웨어 또는 소프트웨어 구성요소)을 제어할 수 있고, 다양한 데이터 처리 또는 연산을 수행할 수 있다. 일실시예에 따르면, 데이터 처리 또는 연산의 적어도 일부로서, 프로세서(120)는 다른 구성요소(예: 센서 모듈(176) 또는 통신 모듈(190))로부터 수신된 명령 또는 데이터를 휘발성 메모리(132)에 로드하고, 휘발성 메모리(132)에 저장된 명령 또는 데이터를 처리하고, 결과 데이터를 비휘발성 메모리(134)에 저장할 수 있다. 일실시예에 따르면, 프로세서(120)는 메인 프로세서(121)(예: 중앙 처리 장치 또는 어플리케이션 프로세서), 및 이와는 독립적으로 또는 함께 운영 가능한 보조 프로세서(123)(예: 그래픽 처리 장치, 이미지 시그널 프로세서, 센서 허브 프로세서, 또는 커뮤니케이션 프로세서)를 포함할 수 있다. 추가적으로 또는 대체적으로, 보조 프로세서(123)은 메인 프로세서(121)보다 저전력을 사용하거나, 또는 지정된 기능에 특화되도록 설정될 수 있다. 보조 프로세서(123)는 메인 프로세서(121)와 별개로, 또는 그 일부로서 구현될 수 있다.

[28] 보조 프로세서(123)는, 예를 들면, 메인 프로세서(121)가 인액티브(예: 슬립) 상태에 있는 동안 메인 프로세서(121)를 대신하여, 또는 메인 프로세서(121)가 액티브(예: 어플리케이션 실행) 상태에 있는 동안 메인 프로세서(121)와 함께, 전자 장치(101)의 구성요소들 중 적어도 하나의 구성요소(예: 표시 장치(160), 센서 모듈(176), 또는 통신 모듈(190))와 관련된 기능 또는 상태들의 적어도 일부를 제어할 수 있다. 일실시예에 따르면, 보조 프로세서(123)(예: 이미지 시그널 프로세서 또는 커뮤니케이션 프로세서)는 기능적으로 관련 있는 다른 구성 요소(예: 카메라 모듈(180) 또는 통신 모듈(190))의 일부로서 구현될 수 있다.

[29] 메모리(130)는, 전자 장치(101)의 적어도 하나의 구성요소(예: 프로세서(120) 또는 센서모듈(176))에 의해 사용되는 다양한 데이터를 저장할 수 있다. 데이터는, 예를 들어, 소프트웨어(예: 프로그램(140)) 및, 이와 관련된 명령에 대한 입력 데이터 또는 출력 데이터를 포함할 수 있다. 메모리(130)는, 휘발성 메모리(132) 또는 비휘발성 메모리(134)를 포함할 수 있다.

[30] 프로그램(140)은 메모리(130)에 소프트웨어로서 저장될 수 있으며, 예를 들면, 운영 체제(142), 미들 웨어(144) 또는 어플리케이션(146)을 포함할 수 있다.

[31] 입력 장치(150)는, 전자 장치(101)의 구성요소(예: 프로세서(120))에 사용될 명령 또는 데이터를 전자 장치(101)의 외부(예: 사용자)로부터 수신할 수 있다. 입력 장치(150)은, 예를 들면, 마이크, 마우스, 또는 키보드를 포함할 수 있다.

[32] 음향 출력 장치(155)는 음향 신호를 전자 장치(101)의 외부로 출력할 수 있다. 음향 출력 장치(155)는, 예를 들면, 스피커 또는 리시버를 포함할 수 있다.

스피커는 멀티미디어 재생 또는 녹음 재생과 같이 일반적인 용도로 사용될 수 있고, 리시버는 착신 전화를 수신하기 위해 사용될 수 있다. 일실시예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

[33] 표시 장치(160)는 전자 장치(101)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 표시 장치(160)은, 예를 들면, 디스플레이, 홀로그램 장치, 또는 프로젝터 및 해당 장치를 제어하기 위한 제어 회로를 포함할 수 있다. 일실시예에 따르면, 표시 장치(160)는 터치를 감지하도록 설정된 터치 회로(touch circuitry), 또는 상기 터치에 의해 발생되는 힘의 세기를 측정하도록 설정된 센서 회로(예: 압력 센서)를 포함할 수 있다.

[34] 오디오 모듈(170)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 일실시예에 따르면, 오디오 모듈(170)은, 입력 장치(150)를 통해 소리를 획득하거나, 음향 출력 장치(155), 또는 전자 장치(101)와 직접 또는 무선으로 연결된 외부 전자 장치(예: 전자 장치(102)) (예: 스피커 또는 헤드폰))를 통해 소리를 출력할 수 있다.

[35] 센서 모듈(176)은 전자 장치(101)의 작동 상태(예: 전력 또는 온도), 또는 외부의 환경 상태(예: 사용자 상태)를 감지하고, 감지된 상태에 대응하는 전기 신호 또는 데이터 값을 생성할 수 있다. 일실시예에 따르면, 센서 모듈(176)은, 예를 들면, 제스처 센서, 자이로 센서, 기압 센서, 마그네틱 센서, 가속도 센서, 그립 센서, 근접 센서, 컬러 센서, IR(infrared) 센서, 생체 센서, 온도 센서, 습도 센서, 또는 조도 센서를 포함할 수 있다.

[36] 인터페이스(177)는 전자 장치(101)이 외부 전자 장치(예: 전자 장치(102))와 직접 또는 무선으로 연결되기 위해 사용될 수 있는 하나 이상의 지정된 프로토콜들을 지원할 수 있다. 일실시예에 따르면, 인터페이스(177)는, 예를 들면, HDMI(high definition multimedia interface), USB(universal serial bus) 인터페이스, SD카드 인터페이스, 또는 오디오 인터페이스를 포함할 수 있다.

[37] 연결 단자(178)는, 그를 통해서 전자 장치(101)가 외부 전자 장치(예: 전자 장치(102))와 물리적으로 연결될 수 있는 커넥터를 포함할 수 있다. 일실시예에 따르면, 연결 단자(178)은, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.

[38] 햅틱 모듈(179)은 전기적 신호를 사용자가 촉각 또는 운동 감각을 통해서 인지할 수 있는 기계적인 자극(예: 진동 또는 움직임) 또는 전기적인 자극으로 변환할 수 있다. 일실시예에 따르면, 햅틱 모듈(179)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.

[39] 카메라 모듈(180)은 정지 영상 및 동영상을 촬영할 수 있다. 일실시예에 따르면, 카메라 모듈(180)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.

[40] 전력 관리 모듈(188)은 전자 장치(101)에 공급되는 전력을 관리할 수 있다. 일실시예에 따르면, 전력 관리 모듈(388)은, 예를 들면, PMIC(power management

integrated circuit)의 적어도 일부로서 구현될 수 있다.

[41] 배터리(189)는 전자 장치(101)의 적어도 하나의 구성 요소에 전력을 공급할 수 있다. 일실시예에 따르면, 배터리(189)는, 예를 들면, 재충전 불가능한 1차 전지, 재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.

[42] 통신 모듈(190)은 전자 장치(101)와 외부 전자 장치(예: 전자 장치(102), 전자 장치(104), 또는 서버(108))간의 직접(예: 유선) 통신 채널 또는 무선 통신 채널의 수립, 및 수립된 통신 채널을 통한 통신 수행을 지원할 수 있다. 통신 모듈(190)은 프로세서(120)(예: 어플리케이션 프로세서)와 독립적으로 운영되고, 직접(예: 유선) 통신 또는 무선 통신을 지원하는 하나 이상의 커뮤니케이션 프로세서를 포함할 수 있다. 일실시예에 따르면, 통신 모듈(190)은 무선 통신 모듈(192)(예: 셀룰러 통신 모듈, 근거리 무선 통신 모듈, 또는 GNSS(global navigation satellite system) 통신 모듈) 또는 유선 통신 모듈(194)(예: LAN(local area network) 통신 모듈, 또는 전력선 통신 모듈)을 포함할 수 있다. 이들 통신 모듈 중 해당하는 통신 모듈은 제 1 네트워크(198)(예: 블루투스, WiFi direct 또는 IrDA(infrared data association) 같은 근거리 통신 네트워크) 또는 제 2 네트워크(199)(예: 셀룰러 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부 전자 장치와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성 요소(예: 단일 칩)으로 통합되거나, 또는 서로 별도의 복수의 구성 요소들(예: 복수 칩들)로 구현될 수 있다. 무선 통신 모듈(192)은 가입자 식별 모듈(196)에 저장된 가입자 정보(예: 국제 모바일 가입자 식별자(IMSI))를 이용하여 제 1 네트워크(198) 또는 제 2 네트워크(199)와 같은 통신 네트워크 내에서 전자 장치(101)를 확인 및 인증할 수 있다.

[43] 안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 일실시예에 따르면, 안테나 모듈(197)은 하나 이상의 안테나들을 포함할 수 있고, 이로부터, 제 1 네트워크 198 또는 제 2 네트워크 199와 같은 통신 네트워크에서 사용되는 통신 방식에 적합한 적어도 하나의 안테나가, 예를 들면, 통신 모듈(190)에 의하여 선택될 수 있다. 신호 또는 전력은 상기 선택된 적어도 하나의 안테나를 통하여 통신 모듈(190)과 외부 전자 장치 간에 송신되거나 수신될 수 있다.

[44] 상기 구성요소들 중 적어도 일부는 주변 기기들간 통신 방식(예: 버스, GPIO(general purpose input and output), SPI(serial peripheral interface), 또는 MIPI(mobile industry processor interface))를 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.

[45] 일실시예에 따르면, 명령 또는 데이터는 제 2 네트워크(199)에 연결된 서버(108)를 통해서 전자 장치(101)와 외부의 전자 장치(104)간에 송신 또는 수신될 수 있다. 전자 장치(102, 104) 각각은 전자 장치(101)와 동일한 또는 다른 종류의 장치일 수 있다. 일실시예에 따르면, 전자 장치(101)에서 실행되는 동작들의 전부 또는 일부는 외부 전자 장치들(102, 104, or 108) 중 하나 이상의

외부 장치들에서 실행될 수 있다. 예를 들면, 전자 장치(101)가 어떤 기능이나 서비스를 자동으로, 또는 사용자 또는 다른 장치로부터의 요청에 반응하여 수행해야 할 경우에, 전자 장치(101)는 기능 또는 서비스를 자체적으로 실행시키는 대신에 또는 추가적으로, 하나 이상의 외부 전자 장치들에게 그 기능 또는 그 서비스의 적어도 일부를 수행하라고 요청할 수 있다. 상기 요청을 수신한 하나 이상의 외부 전자 장치들은 요청된 기능 또는 서비스의 적어도 일부, 또는 상기 요청과 관련된 추가 기능 또는 서비스를 실행하고, 그 실행의 결과를 전자 장치(101)로 전달할 수 있다. 전자 장치(101)는 상기 결과를, 그대로 또는 추가적으로 처리하여, 상기 요청에 대한 응답의 적어도 일부로서 제공할 수 있다.. 이를 위하여, 예를 들면, 클라우드 컴퓨팅, 분산 컴퓨팅, 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다.

[46]

[47] 도 2은 다양한 실시예에 따른 프로그램(140)을 예시하는 블록도(200)이다. 일실시예에 따르면, 프로그램(140)은 전자 장치(101)의 하나 이상의 리소스들을 제어하기 위한 운영 체제(142), 미들웨어(144), 또는 상기 운영 체제(142)에서 실행 가능한 어플리케이션(146)을 포함할 수 있다. 운영 체제(142)는, 예를 들면, Android™, iOS™, Windows™, Symbian™, Tizen™, 또는 Bada™를 포함할 수 있다. 프로그램(140) 중 적어도 일부 프로그램은, 예를 들면, 제조 시에 전자 장치(101)에 프리로드되거나, 또는 사용자에 의해 사용 시 외부 전자 장치(예: 전자 장치(102 또는 104), 또는 서버(108))로부터 다운로드되거나 갱신 될 수 있다.

[48] 운영 체제(142)는 전자 장치(101)의 하나 이상의 시스템 리소스들(예: 프로세스, 메모리, 또는 전원)의 관리(예: 할당 또는 회수)를 제어할 수 있다. 운영 체제(142)는, 추가적으로 또는 대체적으로, 전자 장치(101)의 다른 하드웨어 디바이스, 예를 들면, 입력 장치(150), 음향 출력 장치(155), 표시 장치(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 구동하기 위한 하나 이상의 드라이버 프로그램들을 포함할 수 있다.

[49] 미들웨어(144)는 전자 장치(101)의 하나 이상의 리소스들로부터 제공되는 기능 또는 정보가 어플리케이션(146)에 의해 사용될 수 있도록 다양한 기능들을 어플리케이션(146)으로 제공할 수 있다. 미들웨어(144)는, 예를 들면, 어플리케이션 매니저(201), 윈도우 매니저(203), 멀티미디어 매니저(205), 리소스 매니저(207), 파워 매니저(209), 데이터베이스 매니저(211), 패키지 매니저(213), 커넥티비티 매니저(215), 노티피케이션 매니저(217), 로케이션 매니저(219), 그래픽 매니저(221), 시큐리티 매니저(223), 통화 매니저(225), 또는 음성 인식 매니저(227)를 포함할 수 있다.

[50] 어플리케이션 매니저(201)는, 예를 들면, 어플리케이션(146)의 생명 주기를

관리할 수 있다. 윈도우 매니저(203)는, 예를 들면, 화면에서 사용되는 하나 이상의 GUI 자원들을 관리할 수 있다. 멀티미디어 매니저(205)는, 예를 들면, 미디어 파일들의 재생에 필요한 하나 이상의 포맷들을 파악하고, 그 중 선택된 해당하는 포맷에 맞는 코덱을 이용하여 상기 미디어 파일들 중 해당하는 미디어 파일의 인코딩 또는 디코딩을 수행할 수 있다. 리소스 매니저(207)는, 예를 들면, 어플리케이션(146)의 소스 코드 또는 메모리(130)의 메모리의 공간을 관리할 수 있다. 파워 매니저(209)는, 예를 들면, 배터리(189)의 용량, 온도 또는 전원을 관리하고, 이 중 해당 정보를 이용하여 전자 장치(101)의 동작에 필요한 관련 정보를 결정 또는 제공할 수 있다. 일실시예에 따르면, 파워 매니저(209)는 전자 장치(101)의 바이오스(BIOS: basic input/output system)(미도시)와 연동할 수 있다.

[51] 데이터베이스 매니저(211)는, 예를 들면, 어플리케이션(146)에 의해 사용될 데이터베이스를 생성, 검색, 또는 변경할 수 있다. 패키지 매니저(213)는, 예를 들면, 패키지 파일의 형태로 배포되는 어플리케이션의 설치 또는 갱신을 관리할 수 있다. 커넥티비티 매니저(215)는, 예를 들면, 전자 장치(101)와 외부 전자 장치 간의 무선 연결 또는 직접 연결을 관리할 수 있다. 노티피케이션 매니저(217)는, 예를 들면, 지정된 이벤트(예: 착신 통화, 메시지, 또는 알람)의 발생을 사용자에게 알리기 위한 기능을 제공할 수 있다. 로케이션 매니저(219)는, 예를 들면, 전자 장치(101)의 위치 정보를 관리할 수 있다. 그래픽 매니저(221)는, 예를 들면, 사용자에게 제공될 하나 이상의 그래픽 효과들 또는 이와 관련된 사용자 인터페이스를 관리할 수 있다.

[52] 시큐리티 매니저(223)는, 예를 들면, 시스템 보안 또는 사용자 인증을 제공할 수 있다. 통화(telephony) 매니저(225)는, 예를 들면, 전자 장치(101)에 의해 제공되는 음성 통화 기능 또는 영상 통화 기능을 관리할 수 있다. 음성 인식 매니저(227)는, 예를 들면, 사용자의 음성 데이터를 서버(108)로 전송하고, 그 음성 데이터에 적어도 일부 기반하여 전자 장치(101)에서 수행될 기능에 대응하는 명령어(command), 또는 그 음성 데이터에 적어도 일부 기반하여 변환된 문자 데이터를 서버(108)로부터 수신할 수 있다. 일 실시예에 따르면, 미들웨어(244)는 동적으로 기존의 구성요소를 일부 삭제하거나 새로운 구성요소들을 추가할 수 있다. 일 실시예에 따르면, 미들웨어(144)의 적어도 일부는 운영 체제(142)의 일부로 포함되거나, 또는 운영 체제(142)와는 다른 별도의 소프트웨어로 구현될 수 있다.

[53] 어플리케이션(146)은, 예를 들면, 홈(251), 다이얼러(253), SMS/MMS(255), IM(instant message)(257), 브라우저(259), 카메라(261), 알람(263), 컨택트(265), 음성 인식(267), 이메일(269), 달력(271), 미디어 플레이어(273), 앨범(275), 와치(277), 헬스(279)(예: 운동량 또는 혈당과 같은 생체 정보를 측정), 또는 환경 정보(281)(예: 기압, 습도, 또는 온도 정보 측정) 어플리케이션을 포함할 수 있다. 일실시예에 따르면, 어플리케이션(146)은 전자 장치(101)와 외부 전자 장치 사이의 정보 교환을 지원할 수 있는 정보 교환 어플리케이션(미도시)을 더

포함할 수 있다. 정보 교환 어플리케이션은, 예를 들면, 외부 전자 장치로 지정된 정보 (예: 통화, 메시지, 또는 알람)를 전달하도록 설정된 노티피케이션 릴레이 어플리케이션, 또는 외부 전자 장치를 관리하도록 설정된 장치 관리 어플리케이션을 포함할 수 있다. 노티피케이션 릴레이 어플리케이션은, 예를 들면, 전자 장치(101)의 다른 어플리케이션(예: 이메일 어플리케이션(269))에서 발생된 지정된 이벤트(예: 메일 수신)에 대응하는 알림 정보를 외부 전자 장치로 전달할 수 있다. 추가적으로 또는 대체적으로, 노티피케이션 릴레이 어플리케이션은 외부 전자 장치로부터 알림 정보를 수신하여 전자 장치(101)의 사용자에게 제공할 수 있다.

[54] 장치 관리 어플리케이션은, 예를 들면, 전자 장치(101)와 통신하는 외부 전자 장치 또는 그 일부 구성 요소(예: 표시 장치(160) 또는 카메라 모듈(180))의 전원(예: 턴-온 또는 턴-오프) 또는 기능(예: 표시 장치(160) 또는 카메라 모듈(180)의 밝기, 해상도, 또는 포커스)을 제어할 수 있다. 장치 관리 어플리케이션은, 추가적으로 또는 대체적으로, 외부 전자 장치에서 동작하는 어플리케이션의 설치, 삭제, 또는 갱신을 지원할 수 있다.

[55]

[56] 본 발명의 다양한 실시예에 따르면, 전자 장치(예: 도 3의 전자 장치(300))는 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))와 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400)) 사이의 인증을 위한 공유 키를 제 1 외부 전자 장치(400)에 전송하는 전자 장치를 의미할 수 있다.

[57] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)는 전자 장치(300)로부터 공유 키를 수신하는 전자 장치를 의미할 수 있다.

[58] 본 발명의 다양한 실시예에 따르면, 제 2 외부 전자 장치(1401)는 제 1 외부 전자 장치(400) 또는 전자 장치(300) 사이의 인증에 기반하여 다양한 기능을 제공할 수 있는 전자 장치를 의미할 수 있다. 예를 들면, 제 2 외부 전자 장치(1401)는 운송 수단, 또는 도어 락과 같이 인증을 수행한 후 다양한 기능을 제공할 수 있는 전자 장치를 의미할 수 있다.

[59]

[60] 도 3은 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.

[61] 도 3을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(300)(예: 도 1의 전자 장치(101))는 프로세서(310)(예: 도 1의 프로세서(120)), 통신 모듈(320)(예: 도 1의 통신 모듈(190)), 보안 모듈(330), 메모리(340)(예: 도 1의 메모리(130)), 및 디스플레이(350)(예: 도 1의 표시 장치(160))을 포함할 수 있다.

[62] 본 발명의 다양한 실시예에 따르면, 통신 모듈(320)은 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400))와 통신 채널을 설립하고, 제 1 외부 전자 장치(400)와 다양한 데이터를 송수신할 수 있다. 통신 모듈(320)은 근거리 통신(예를 들면, Bluetooth, NFC, 또는 UWB)을 이용하여 제 1 외부 전자 장치(400)와 다양한 데이터를 송수신할 수 있으나, 이에 제한되지 않고, 셀룰러

네트워크(예를 들면, LTE, 또는 5G 네트워크)를 이용하여 제 1 외부 전자 장치(400)와 다양한 데이터를 송수신할 수 있다.

[63] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 프로세서(310) 또는 메모리(340)와 물리적으로 분리된 모듈로써, 보안 모듈(330) 상에 저장된 데이터를 암호화하여 저장할 수 있다. 본 발명의 다른 실시예에 따르면, 보안 모듈(330)은 메모리(340)의 일 영역에 포함될 수 있으며, 보안 모듈(330)은 메모리(340) 상에 저장된 데이터를 암호화하여 저장된 부분을 의미할 수 있다.

[64] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 보안 모듈(330) 상의 데이터의 접근 요청을 수신함에 대응하여, 데이터의 접근 요청의 주체(예를 들면, 메모리(340) 상에 설치된 다양한 어플리케이션 등)의 접근 권한, 무결성 검증을 수행하고, 수행한 결과에 따라 보안 모듈(330) 상에 저장된 데이터의 접근/편집을 허가 또는 저장된 데이터를 전송할 수 있다.

[65] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))의 인증에 이용되는 인증 키를 저장하고, 저장된 인증 키를 관리할 수 있다. 제 2 외부 전자 장치(1401)의 인증은 제 2 외부 전자 장치((1401)가 제공 가능한 다양한 기능을 수행하기 위해서, 인증 키를 저장하고 있는 전자 장치(300)가 유효한 권한을 가지고 있는지 확인하는 동작을 의미할 수 있다.

[66] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)은 프로세서(310)의 제어에 기반하여, 제 1 외부 전자 장치(400)로 전송할 공유 키를 생성하고, 생성된 공유 키를 관리할 수 있다. 제 1 외부 전자 장치(400)로 전송되는 공유 키는 제 2 외부 장치(예: 도 14의 제 2 외부 장치(1401))의 인증에 이용될 수 있으며, 공유 키를 저장하고 있는 제 1 외부 전자 장치(400)는 제 2 외부 장치(1401)과 공유 키를 이용해서 유효한 인증을 수행할 수 있다.

[67] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)는 보안 모듈(330)에 저장된 인증 키를 공유 또는 인증 키를 제 1 외부 전자 장치(400)로 전송할 수 있다. 예를 들어, 전자 장치(300)는 보안 모듈(330)에 저장된 인증 키를 이용하여 공유 키를 생성하고, 생성된 공유 키를 제 1 외부 전자 장치(400)에 전송할 수 있다. 제 1 외부 전자 장치(400)는 수신한 공유 키를 제 1 외부 전자 장치(400)의 보안 모듈(430)에 저장할 수 있다. 제 1 외부 전자 장치(400)는 수신한 공유 키를 이용하여 제 2 외부 전자 장치(1401)와 인증을 수행할 수 있다. 이하, 공유 키를 생성 및 전송하는 프로세서(310)의 구체적인 동작에 대해서 서술한다.

[68] 본 발명의 다양한 실시예에 따르면, 프로세서(310)는 보안 모듈(330)에 저장되어 있으며, 제 2 외부 전자 장치(1401)와 전자 장치(300)의 인증에 이용되는 인증 키를 제 1 외부 전자 장치(400)로 전송할 것을 요청하는 신호를 수신할 수 있다. 예를 들면, 전자 장치(300)의 사용자가 제 2 외부 전자 장치(1401)의 키 관리 어플리케이션의 사용자 인터페이스를 이용하여 제 1 외부 전자 장치(400)로 인증 키를 전송할 것을 요청할 수 있다. 프로세서(310)는 인증

키의 제 1 외부 전자 장치(400)로의 전송 요청을 수신함에 대응하여, 공유 키의 생성을 위한 정보 및 공유 키 생성 명령을 보안 모듈(330)에 전송할 수 있다.

[69] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성을 위한 정보는 제 1 외부 전자 장치(400)의 사용자의 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화할 기능에 대한 정보를 포함할 수 있다. 제 2 외부 전자 장치(1401)가 제공 가능한 기능들은 제 2 외부 전자 장치(1401)의 이용 허용 시간(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 운행이 가능한 시간), 제 2 외부 전자 장치(1401)의 이용 가능한 지역 범위 정보(geofencing limitation data, 예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 운행이 허용되는 지역적인 범위), 제 2 외부 전자 장치(1401)의 성능 제약(예를 들면, 2 외부 전자 장치(1401)가 운송 수단인 경우, 최대 허용 속도), 제 2 외부 전자 장치(1401)에 포함된 다양한 장치(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 다양한 장치는 트렁크, 콘솔 박스 등이 될 수 있다) 또는 제 2 외부 전자 장치(1401)가 수행 가능한 다양한 기능(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 차선 유지 보조, 차선 이탈 알림, 크루즈 컨트롤, 어댑티브 크루즈 컨트롤, 또는 엔진 사용 가능 여부)의 허용 여부를 지시하는 정보를 포함할 수 있다. 공유 키의 생성을 위한 정보는 전자 장치(300)의 사용자가 제 2 외부 전자 장치(1401)의 키 관리 어플리케이션의 사용자 인터페이스를 이용한 사용자 입력(제 1 외부 전자 장치(400)의 사용자 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화된 기능을 선택하는 사용자 입력)에 의해 생성될 수 있다.

[70] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성을 위한 정보는 생성된 공유키를 암호화하여 제 1 외부 전자 장치(400)로 전송하기 위해 요구되는 데이터를 포함할 수 있다. 예를 들면, 공유 키의 생성을 위한 정보는 생성된 공유키를 대칭 암호화 방식 또는 비대칭 암호화 방식을 이용하여 암호화를 수행하는데 필요한 암호 키를 포함할 수 있다.

[71] 본 발명의 다양한 실시예에 따르면, 프로세서(310)는 공유 키 생성 명령과 공유 키의 생성을 위한 정보를 보안 모듈(330)로 전송할 수 있다. 보안 모듈(330)은, 공유 키 생성 명령을 수신함에 대응하여, 수신한 공유 키의 생성을 위한 정보에 기반하여 공유 키를 생성할 수 있다. 공유 키의 생성은 보안 모듈(330)에 설치된 키 매니징 애플릿(key managing applet, 331)에 의해 구현될 수 있다. 키 매니징 애플릿(331)은 공유 키의 생성을 위한 정보를 이용하여 공유 키를 생성할 수 있다.

[72] 본 발명의 다양한 실시예에 따르면, 키 매니징 애플릿(331)은 보안 모듈(330) 상에 저장되어 있는 인증 키의 종류를 확인할 수 있다. 인증 키의 종류는 마스터 키 또는 마스터 키에 기반하여 생성된 1차 공유 키를 포함할 수 있다. 예를 들어, 마스터 키는 제 2 외부 전자 장치(1401)의 제조사에서, 제 2 외부 전자 장치(1401)의 출고시 제공되는 키를 의미할 수 있다. 예를 들어, 1차 공유 키는

마스터 키에 기반하여 생성된 공유 키를 의미할 수 있다.

[73] 본 발명의 다양한 실시예에 따르면, 키 매니징 애플릿(331)(331)은, 보안 모듈(330) 상에 저장된 인증 키가 마스터 키를 확인함에 대응하여, 1차 공유 키를 생성할 수 있다.

[74] 본 발명의 다양한 실시예에 따르면, 키 매니징 애플릿(331)은, 보안 모듈(330) 상에 저장된 인증 키가 마스터 키에 기반하여 생성된 1차 공유 키를 확인함에 대응하여, 2차 공유 키의 생성을 위한 토큰을 생성할 수 있다. 2차 공유 키의 생성을 위한 토큰은 제 2 외부 전자 장치(1401)에서 공유 키를 생성을 요청하는 데이터를 의미할 수 있다. 예를 들어, 2차 공유 키의 생성을 위한 토큰을 수신한 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)와 통신 연결이 수립되고, 제 2 외부 전자 장치(1401)는 2차 공유 키의 생성을 위한 토큰을 수신할 수 있다. 제 2 외부 전자 장치(1401)는 토큰을 수신함에 대응하여 제 2 외부 전자 장치(1401)에 저장되어 있는 마스터 키 또는 1차 공유 키에 기반하여 2차 공유 키를 생성할 수 있다. 제 2 외부 전자 장치(1401)가 생성한 2차 공유 키는 제 1 외부 전자 장치(400)로 전송될 수 있다.

[75] 본 발명의 다양한 실시예에 따르면, 키 매니징 애플릿(331)은 공유 키(보안 모듈(330)에 저장된 인증 키가 마스터 키인 경우) 또는 공유 키를 생성하기 위한 토큰(보안 모듈(330)에 저장된 인증 키가 공유 키인 경우)을 생성하고, 생성된 공유 키 또는 토큰을 공유 키와 관련된 정보와 함께 키 쉐어링 애플릿(333)에 전송할 수 있다. 공유 키와 관련된 정보는 키 쉐어링 애플릿(333)이 생성된 공유 키 또는 토큰을 암호화하여 전송하는데 이용되는 암호 키, 제 1 외부 전자 장치(400)의 사용자의 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화할 기능에 대한 정보를 포함할 수 있다.

[76] 본 발명의 다양한 실시예에 따르면, 공유 키와 관련된 정보는 공유 키가 전자 장치(300)에 저장된 인증 키에 기반하여 생성되었음을 지시하는 정보를 포함할 수 있다. 제 2 외부 전자 장치(1401)는 공유 키와 관련된 정보를 제 1 외부 전자 장치(400)로부터 수신하고, 전자 장치(300)에 저장된 인증 키에 기반하여 생성되었음을 지시하는 정보에 기반하여 유효한 공유 키인지 검증할 수 있다.

[77] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(333)은 키 매니징 애플릿(331)으로부터 생성된 공유 키 또는 공유 키 생성을 위한 토큰 및 공유 키와 관련된 정보를 수신하고, 제 1 외부 전자 장치(400)와 전자 장치(300)와 설립된 통신 채널을 이용하여 생성된 공유 키 또는 공유 키 생성을 위한 토큰 및 공유 키와 관련된 정보를 제 1 외부 전자 장치(400)로 전송할 수 있다.

[78] 본 발명의 다양한 실시예에 따르면, 키 매니징 애플릿(331)과 키 쉐어링 애플릿(333)은 하나의 애플릿으로 통합될 수 있다. 통합된 애플릿은 키 매니징 애플릿(331)이 수행할 수 있는 공유 키 및 공유 키와 관련된 정보를 생성하는 동작과 키 쉐어링 애플릿(333)이 수행할 수 있는 공유 키 및 공유 키와 관련된 정보를 제 1 외부 전자 장치(400)에 전송할 수 있는 동작을 모두 수행할 수도

있다.

[79] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)와 전자 장치(300) 사이에는 근거리 통신 수단(예를 들면, NFC(near field communication), 블루투스, 또는 UWB와 같은 다양한 통신 수단) 또는 셀룰러 네트워크를 이용한 통신 채널이 생성될 수 있다.

[80]

[81] 도 4는 본 발명의 다양한 실시예에 따른 제 1 외부 전자 장치의 블록도이다.

[82] 도 4를 참조하면, 본 발명의 다양한 실시예에 따른 제 1 외부 전자 장치(400)는 프로세서(410), 통신 모듈(420), 보안 모듈(430) 및 메모리(440)을 포함할 수 있다.

[83] 본 발명의 다양한 실시예에 따르면, 통신 모듈(420)은 전자 장치(예: 도 3의 전자 장치(300))와 통신 채널을 설립하고, 전자 장치(300)와 다양한 데이터를 송수신할 수 있다. 통신 모듈(420)은 근거리 통신(예를 들면, blue-tooth, NFC, 또는 UWB)을 이용하여 전자 장치(300)와 다양한 데이터를 송수신할 수 있으나, 이에 제한되지 않고, 셀룰러 네트워크(예를 들면, LTE, 5G 네트워크 등)를 이용하여 전자 장치(300)와 다양한 데이터를 송수신할 수 있다.

[84] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)와 전자 장치(300) 간 공유 키를 송/수신하기 위해서는, 제 1 외부 전자 장치(400)의 보안 모듈(430) 상에 키 쉐어링 애플릿(431)이 설치되어 있어야 한다. 후술하는 내용은 키 쉐어링 애플릿(431)을 설치하는 구체적인 내용에 대한 것이다.

[85] 본 발명의 다양한 실시예에 따르면, 프로세서(410)는 메모리(440)에 설치된 키 쉐어링 어플리케이션을 실행하고, 전자 장치(300)로부터 수신할 공유 키와 인증을 수행할 제 2 외부 전자 장치(1401) 과 관련된 정보를 입력하는 사용자 입력을 수신할 수 있다. 키 쉐어링 어플리케이션은 메모리(440) 상에 설치되어, 전자 장치(300)로부터 수신한 공유 키 및 공유 키와 관련된 정보를 이용하여 보안 모듈(430)의 키 쉐어링 애플릿(431)에 공유 키를 설치하는 어플리케이션을 의미할 수 있다.

[86] 본 발명의 다양한 실시예에 따르면, 제 2 외부 전자 장치(1401)와 관련된 정보는 제 1 외부 전자 장치(400)의 사용자가 키 쉐어링 어플리케이션의 인터페이스를 이용하여 입력한 정보를 의미할 수 있다. 제 2 외부 전자 장치(1401)와 관련된 정보는 제 2 외부 전자 장치(1401)의 제조사 이름(예를 들면, BMX), 제 2 외부 전자 장치(1401)의 모델 이름(예를 들면, X5)을 포함할 수 있다.

[87] 본 발명의 다양한 실시예에 따르면, 프로세서(410)는 제 1 외부 전자 장치(400)의 사용자가 키 쉐어링 어플리케이션의 인터페이스를 이용하여 입력하는 공유 키의 종류와 관련된 정보를 수신할 수 있다. 공유 키의 종류와 관련된 정보는 전자 장치(300)에 저장된 제 2 외부 전자 장치(1401)의 키와 동일한 공유 키 또는 복수의 이용자가 이용하는 쉐어링 카를 위한 일반적인 공유 키 중 어느 하나를 지정하는 정보를 의미할 수 있다. 상기 내용에 대해서는 도 5에서 후술한다.

[88] 본 발명의 다양한 실시예에 따르면, 프로세서(410)는 수신한 제 2 외부 전자 장치(1401)와 관련된 정보 또는 공유 키의 종류와 관련된 정보 및 키 쉐어링 애플릿(431)을 설치하는 명령을 보안 모듈(430)에 전송할 수 있다. 보안 모듈(430)은 제 2 외부 전자 장치(1401)와 관련된 정보에 포함된 제 2 외부 전자 장치(1401)의 제조사의 식별자(AID)에 대응하는 키 쉐어링 애플릿(431)을 설치할 수 있다. 키 쉐어링 애플릿(431)은 제 2 외부 전자 장치(1401)의 제조사의 식별자에 대응하는 공유 키를 전자 장치(300)로부터 수신할 수 있으며, 이를 위해 제조사의 식별자를 전자 장치(300)의 키 쉐어링 애플릿(333)에 전송할 수 있다. 전자 장치(300) 상에 저장된 공유 키가 제조사의 식별자와 대응하지 않는 경우, 공유 키의 송/수신 동작이 종료될 수 있다.

[89] 본 발명의 다양한 실시예에 다르면, 생성된 키 쉐어링 애플릿(431)은 사용자 정보, 제 2 외부 전자 장치(1401) 정보, 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)간 송수신되는 암호화에 이용되는 복수의 암호 키에 대한 정보를 포함할 수 있다. 키 쉐어링 애플릿(431)은 수신한 공유 키의 상태를 지시하는 정보를 포함할 수 있으며, 수신한 공유 키의 상태는 아래의 표 1에 정의되어 있다.

[90] [표1]

Index	Status	Description
1	INIT	Initial Status
2	KEY+ PRIVILEGE DEACTIVE	Received the Key + Privilege but vehicle have not accepted yet
3	KEY+ PRIVILEGE ACTIVITE	Received the Key + Privilege and vehicle have accepted
4	Expired	Out of validly

[91] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)은 프로세서(410) 또는 메모리(440)(예: 도 1의 메모리(130))와 물리적으로 분리된 모듈로써, 보안 모듈(430) 상에 저장된 데이터를 암호화하여 저장할 수 있다. 본 발명의 다른 실시예에 따르면, 보안 모듈(430)은 메모리(440)의 일 영역에 포함될 수 있으며, 보안 모듈(430)은 메모리(440) 상에 저장된 데이터를 암호화하여 저장된 부분을 의미할 수 있다. 보안 모듈(430)은 보안 모듈(430) 상의 데이터의 접근 요청을 수신함에 대응하여, 데이터의 접근 요청의 주체(예를 들면, 메모리(440) 상에 설치된 다양한 어플리케이션 등)의 접근 권한, 무결성 검증을 수행하고, 수행한 결과에 따라 보안 모듈(430) 상에 저장된 데이터의 접근/편집을 허가 또는 저장된 데이터를 전송할 수 있다.

[92] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)은 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)와 인증을 수행하는데 이용되는 제 2 외부

전자 장치(1401)의 키 애플릿을 관리하는 CRS(Contactless register service)를 포함할 수 있다. CRS(미도시)는 사용자의 요청에 기반하여 애플릿에 할당된 데이터의 수정, 추가, 또는 삭제를 수행할 수 있다.

[93] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)은 PVKSE(proximity vehicle key system environment)를 포함할 수 있다. PVKSE(예: 도 5의 PVKSE(510))는 보안 모듈(430)에 설치된 키 매니징 애플릿에 할당된 데이터의 수정, 추가, 또는 삭제에 대한 모니터링을 수행하고, 운송 수단 키 애플릿과 관련된 데이터의 변경을 감지하면, 운송 수단 키 애플릿과 관련된 정보를 생성 또는 생성된 애플릿과 관련된 정보를 변경할 수 있다. PVKSE(510)는 보안 모듈(430)에 저장된 데이터를 관리하는 CRS(contactless registry service)와는 소프트웨어적으로 별도로 구현된 구성 요소를 의미할 수 있다. PVKSE(510) 및 CRS(520)를 이용하여 공유 키를 수신하는 구체적인 동작에 대해서는 도 5에서 서술한다.

[94] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)에 설치된 키 쉐어링 애플릿(431)은 전자 장치(300)의 보안 모듈(330)에 설치된 키 쉐어링 애플릿(333)과의 상호 동작을 통하여 전자 장치(300)의 보안 모듈(330)에 설치된 공유 키 및 공유 키와 관련된 정보를 수신할 수 있다.

[95] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(431)를 이용하여 수신한 공유 키는 공유 키를 수신한 후 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)가 서로 처음으로 연결되는 경우 활성화될 수 있다. 제 2 외부 전자 장치(1401)는 제 1 외부 전자 장치(400)가 연결되면서 전송하는 공유 키를 검증하고, 검증 결과에 기반하여 공유 키의 활성화 여부를 결정할 수 있다. 활성화 이전의 공유 키는 표 1의 2 상태(PRIVILEGE DEACTIVE)와 같이 유지되며, 활성화 후의 공유 키는 표 1의 3 상태(PRIVILEGE ACTIVE)로 변화될 수 있다.

[96] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(431)은 2차 공유 키의 생성을 위한 토큰을 수신한 경우, 2차 공유 키의 생성을 위한 토큰을 제 2 외부 전자 장치(1401)에 전송할 수 있다. 제 2 외부 전자 장치(1401)는 2차 공유 키의 생성을 위한 토큰이 전자 장치(300)에 저장된 1차 공유 키에 기반하여 생성되었는지 확인하면서, 2차 공유 키의 생성을 위한 토큰의 유효성을 검증하고, 2차 공유 키를 생성할 수 있다. 생성된 공유 키는 키 쉐어링 애플릿(431)으로 전송될 수 있다. 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)간의 상호 동작에 대해서는 도 14에서 후술한다.

[97]

[98] 도 5는 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))에서, 보안 모듈(330)을 도시한 블록도이다.

[99] 도 5를 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(300)의 보안 모듈(330)은 발급된 보안 도메인(issued security domain, ISD, 581)과 추가 보안

도메인(supplementary security domain, SSD, 582)로 구분될 수 있다.

[100] 본 발명의 다양한 실시예에 따르면, ISD(581)에는 PVKSE(510) 및 CRS(520)가 설치될 수 있다. PVKSE(510)는 SSD(582)에 설치된 적어도 하나 이상의 제 2 외부 전자 장치(1401)의 키 관리 애플릿(530, 540, 550, 560, 또는 570)과 관련된 데이터를 관리할 수 있는 소프트웨어적 요소를 의미할 수 있다. PVKSE(510)는 적어도 하나 이상의 제 2 외부 전자 장치(1401)의 키 관리 애플릿(530, 540, 550, 560, 또는 570)과 관련된 데이터의 변경을 모니터링하고, 변경을 감지한 경우, 데이터 변경을 반영한 애플릿과 관련된 정보를 생성 또는 변경할 수 있다.

[101] 본 발명의 다양한 실시예에 따르면, PVKSE(510)는 적어도 하나 이상의 제 2 외부 전자 장치(1401)의 키 관리 애플릿(530, 540, 550, 560, 또는 570)과 관련된 정보를 관리할 수 있다. 애플릿과 관련된 정보는 제 2 외부 전자 장치(1401)의 제조사의 식별자를 의미하는 애플릿 식별자, 제 2 외부 전자 장치(1401)의 모델을 지시하는 애플릿 라벨, 애플릿의 우선 순위를 지시하는 우선 순위 정보, 또는 애플릿의 구체적인 데이터를 포함할 수 있다.

[102] 본 발명의 다양한 실시예에 따른 보안 모듈(330)은 적어도 하나 이상의 운송 수단 키 관리 애플릿(530, 540, 550, 560, 또는 570)을 관리하는 CRS(520)를 포함하고, CRS(520)의 제어에 기반하여 적어도 하나 이상의 애플릿(530, 540, 550, 560, 또는 570)의 관리를 수행할 수 있다.

[103] 본 발명의 다양한 실시예에 따르면, CRS(520)는 보안 모듈(330) 상에 설치되는 파일을 관리하는 소프트웨어적인 요소를 의미할 수 있다. CRS(520)는 프로세서(예: 도 3의 프로세서(310))의 요청에 기반하여 보안 모듈(330)에 저장된 다양한 데이터의 관리(예를 들면, 데이터의 암호화, 암호화된 데이터의 복호화 등)를 수행할 수 있으며, 보안 모듈(330)에 저장된 데이터를 메모리(예: 도 3의 메모리(350))에 이동시킬 수 있다.

[104] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)의 PVKSE(510)는 보안 모듈(330)상에 저장된 운송 수단 키 애플릿들 각각의 애플릿 식별자(applet identification, AID)를 포함하는 AID 리스트를 생성할 수 있다. AID 리스트는 PVKSE(510)에서 생성 및 관리할 수 있다.

[105] 전자 장치(예: 도 3의 전자 장치(300))는 제 1 외부 전자 장치(400)로 공유 키의 전송을 수행하기 위해서, 제 1 외부 전자 장치(400)의 보안 모듈(430)에 저장된 AID 리스트의 전송을 제 1 외부 전자 장치(400)에 요청할 수 있다. 예를 들어, 제 1 외부 전자 장치(400)의 보안 모듈(430)에 저장된 AID 리스트의 전송은 SELECT PVKSE로 정의된 명령어를 이용할 수 있다. PVKSE(510)는 SELECT PVKKE로 정의된 명령어를 수신함에 대응하여 AID 리스트의 생성 및 전송을 수행할 수 있다.

[106] 본 발명의 다양한 실시예에 따르면, PVKSE(510)는 전자 장치(300)의 요청에 대응해서, AID 리스트를 전자 장치(300)로 전송할 수 있다. 전자 장치(300)의 키 쉐어링 애플릿(333)은 제 1 외부 전자 장치(400)로부터 AID 리스트를 수신하고,

공유 키에 대응하는 AID가 AID 리스트에 포함되는지 확인할 수 있다. 키 쉐어링 애플릿(333)은 공유 키에 대응하는 AID가 수신한 AID 리스트에 포함된 경우, 공유 키에 대응하는 AID 정보를 제 1 외부 전자 장치(400)에 전송하는 동작을 수행할 수 있다.

[107] 본 발명의 다양한 실시예에 따르면, PVKSE(510)는 키 쉐어링 애플릿(333)이 전송하는 선택된 AID 정보를 수신하고, 선택된 AID 에 대응하는 애플릿과 관련된 정보(예를 들면, 제 2 외부 전자 장치(1401)와 관련된 정보, 키 쉐어링 애플릿(431)의 정보(키 쉐어링 애플릿의 버전))를 전송할 수 있다.

[108] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(530, 540, 550, 560, 또는 570)들 각각은 SSD(582)에 저장될 수 있다. SSD(582)는 제 2 외부 전자 장치(1401)의 제조사별로 구별된 상태로, 제조사 각각에 대응하는 애플릿을 대응하는 제조사별로 구별된 SSD(582)에 저장할 수 있다. 예를 들면, 제조사 1에 대응하는 애플릿들(550, 560)은 제조사 1에 대응하는 SSD 공간(584)에 저장될 수 있고, 제조사 2에 대응하는 애플릿 (570)은 제조사 2에 대응하는 SSD 공간(585)에 저장될 수 있다. SSD(582)는 다양한 사용자가 이용 가능한 제 2 외부 전자 장치(1401) (예를 들면, 카 쉐어링의 공유 대상이 되는 운송 수단)을 위한 공유 키를 위한 애플릿(530, 540)을 별도로 저장할 수 있는 SSD 공간(583)을 더 포함할 수 있다.

[109] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(530, 540, 550, 560, 또는 570)들 각각은 애플릿의 활성화 여부를 지시하는 데이터를 포함할 수 있다. 활성화된 애플릿은 제 2 외부 전자 장치(1401)와 전자 장치(300) 의 인증을 수행 가능한 애플릿을 의미하며, 비활성화된 애플릿은 제 2 외부 전자 장치(1401)와 전자 장치(300) 의 인증이 수행될 수 없는 애플릿을 의미할 수 있다.

[110] 본 발명의 다양한 실시예에 따르면, 도 5는 전자 장치(300)의 보안 모듈(330)의 실시예를 중심으로 기재되었으나, 제 1 외부 전자 장치(400)가 전자 장치(300)가 전송한 키를 수신한 경우, 제 1 외부 전자 장치(400)의 보안 모듈(430)은 도 5의 실시예와 동일한 방법으로 전자 장치(300)가 전송한 키를 저장할 수 있다.

[111]

[112] 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))는 프로세서(예: 도 3의 프로세서(310)), 무선 통신을 지원하는 적어도 하나의 통신 모듈(예: 도 3의 통신 모듈(320)) 및 제 1 외부 전자 장치(예: 도 4의 제1 외부 전자 장치(400))로 전송될 공유 키 및 제 2 외부 전자 장치와의 인증에 이용되는 인증 키의 저장 및 관리를 수행하는 애플릿이 설치된 보안 모듈(예: 도 3의 보안 모듈(330))을 포함하고, 상기 프로세서(310)는 상기 인증 키의 제 1 외부 전자 장치로의 전송의 요청을 제 1 외부 전자 장치(400)로부터 수신하고, 상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 상기 보안 모듈(330)에 전송하고, 상기 공유 키 생성을 위한 정보에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈(330)을 제어하고, 상기 생성된 공유 키 및 생성된

공유 키와 관련된 정보를 제 1 외부 전자 장치(400)로 전송하도록 상기 보안 모듈(330)을 제어하도록 설정될 수 있다.

[113] 본 발명의 다양한 실시예에 따르면, 상기 공유 키와 관련된 정보는 상기 인증 키에 기반하여 생성됨을 지시하는 정보를 포함할 수 있다.

[114] 본 발명의 다양한 실시예에 따르면, 상기 공유 키와 관련된 정보는 상기 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))가 제공 가능한 기능 중 적어도 일부의 기능을 활성화 할 것을 지시하는 정보를 포함할 수 있다.

[115] 본 발명의 다양한 실시예에 따르면, 상기 입력된 공유 키 생성을 위한 정보는 상기 제 2 외부 전자 장치(1401)의 이용 허용 시간, 상기 제 2 외부 전자 장치(1401)의 이용 가능한 지역 범위 정보(geofencing limitation data)을 포함할 수 있다.

[116] 본 발명의 다양한 실시예에 따르면, 상기 프로세서(310)는 상기 공유 키의 암호화를 위한 암호 키를 상기 공유 키의 생성을 위한 정보와 함께 상기 보안 모듈(330)로 전송하도록 설정될 수 있다.

[117] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(330)은 상기 제 1 외부 전자 장치(400)의 보안 모듈(예: 도 4의 보안 모듈(430))에 설치된 상기 공유 키를 관리할 애플릿(예: 도 4의 키 쉐어링 애플릿(431))과 관련된 정보를 수신하고, 상기 수신한 애플릿과 관련된 정보에 기반하여 상기 공유 키를 상기 제 1 외부 전자 장치(400)에 전송할지 여부를 결정하도록 설정될 수 있다.

[118] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(330)은 상기 애플릿과 관련된 정보에 포함된 애플릿 식별자가 상기 공유 키에 대응하는 식별자와 동일한지 확인하고, 상기 애플릿 식별자와 상기 공유 키에 대응하는 식별자가 동일한지 여부에 기반하여 상기 공유 키를 상기 제 1 외부 전자 장치(400)에 전송할지 여부를 결정하도록 설정될 수 있다.

[119] 본 발명의 다양한 실시예에 따르면, 상기 애플릿과 관련된 정보는 상기 애플릿이 저장된 주소, 애플릿 식별자, 상기 제 1외부 전자 장치(400)의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(applet - specific data) 중 적어도 하나 이상을 포함할 수 있다.

[120] 본 발명의 다양한 실시예에 따르면, 상기 인증 키는 마스터 키 또는 상기 마스터 키에 기반하여 생성된 키 중 하나이며, 상기 인증 키가 상기 마스터 키에 기반하여 생성된 키인 경우, 상기 보안 모듈(330)은 상기 공유 키가 상기 인증 키에 기반하여 생성되었음을 지시하는(indicating) 토큰을 생성하고, 상기 토큰 및 상기 공유 키와 관련된 정보를 상기 제 1외부 전자 장치(400)로 전송하도록 설정될 수 있다.

[121] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)는 상기 통신 모듈(320)을 이용하여 상기 공유 키 및 상기 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치(400)에 전송하도록 설정될 수 있다.

[122]

[123] 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 4의 제 1 외부 전자 장치(400)는 프로세서(예: 도 4의 프로세서(410)), 무선 통신을 지원하는 적어도 하나의 통신 모듈(예: 도 4의 통신 모듈(420)) 및 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))의 인증에 이용되는 인증 키를 관리하는 애플릿과 관련된 정보를 관리하고, 애플릿 식별자(applet identification, AID) 리스트 및 상기 애플릿을 저장하는 보안 모듈(430)을 포함하고, 상기 보안 모듈(430)은 상기 애플릿과 관련된 정보를 요청하는 신호를 상기 제 1 외부 전자 장치(예: 도 3의 전자 장치(300))로부터 수신하고, 상기 애플릿과 관련된 정보를 상기 제 1 외부 전자 장치(300)로 전송하고, 상기 제 1 외부 전자 장치(300)로부터 상기 공유 키 및 상기 공유 키와 관련된 정보를 수신하고, 상기 수신한 공유 키 및 상기 공유 키와 관련된 정보를 상기 보안 모듈(430) 상에 설치하도록 설정될 수 있다.

[124] 본 발명의 다양한 실시예에 따르면, 상기 프로세서(420)는 상기 제 2 외부 전자 장치(1401) 의 정보를 상기 제 1 외부 전자 장치(300)로부터 수신하고, 상기 제 2 외부 전자 장치(1401)의 정보에 기반하여 상기 공유 키를 관리할 애플릿 식별자를 확인하고, 상기 애플릿을 설치하는 명령을 상기 보안 모듈(430)에 전송하도록 설정될 수 있다.

[125] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(430)은 상기 보안 모듈에 설치된 애플릿이 복수인 경우, 상기 공유 키를 관리할 애플릿을 제외한 나머지 애플릿을 비활성화하고, 상기 공유 키의 설치가 완료됨에 대응하여, 상기 나머지 애플릿을 활성화하도록 설정될 수 있다.

[126] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(430)은 상기 애플릿과 관련된 정보를 관리하는 PVKSE(proximity vehicle key system environment)(예: 도 5의 PVKSE(510))를 포함하고, 상기 PVKSE(510) 는 상기 보안 모듈의 발급된 보안 도메인(issued security domain)(예: 도 5의 ISD(581))에 저장되며, 상기 애플릿은 추가 보안 도메인(supplementary security domain)(예: 도 5의 SSD(582))에 저장되도록 설정될 수 있다.

[127] 본 발명의 다양한 실시예에 따르면, 상기 공유키와 관련된 정보는 상기 제 1 외부 전자 장치(300)에 저장되고, 상기 제 2 외부 전자 장치(1401)의 인증에 이용되는 인증 키에 기반하여 생성됨을 지시하는 정보를 포함할 수 있다.

[128] 본 발명의 다양한 실시예에 따르면, 상기 제 1 외부 전자 장치(300)에 저장된 인증 키는 마스터 키 또는 상기 마스터 키에 기반하여 생성된 키 중 하나이며, 상기 인증키가 상기 마스터 키에 기반하여 생성된 키인 경우, 상기 보안 모듈(430)은 상기 공유 키가 상기 인증 키에 기반하여 생성되었음을 지시하는(indicating) 토큰을 상기 제 1 외부 전자 장치(300)로부터 수신하고, 상기 제 2 외부 전자 장치(1401)에 상기 토큰을 전송하고, 상기 제 2 외부 전자 장치(1401)가 상기 토큰에 기반하여 생성한 공유 키를 수신하도록 설정될 수 있다.

[129]

[130] 도 6은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법의 동작 흐름도이다. 도 6은 전자 장치(예: 도 3의 전자 장치(300))와 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400)) 간 공유 키를 생성하고, 생성된 공유 키를 공유하는 구체적인 동작에 대해서 서술하고 있다.

[131] 도 6을 참조하면, 동작 610에서, 전자 장치(300)는 공유 키를 보안 모듈(예: 도 3의 보안 모듈(330))에서 생성할 수 있다. 공유 키를 생성하는 동작은 보안 모듈(330)에 설치된 운송 수단 키 애플릿(예: 도 3의 키 매니징 애플릿(331))에 의해 수행될 수 있다. 키 매니징 애플릿(331)이 생성한 공유 키는, 제 1 외부 전자 장치(400)로 전송하기 위해, 보안 모듈(330)에 설치된 키 쉐어링 애플릿(예: 도 3의 키 쉐어링 애플릿(333))에 전송될 수 있다. 공유 키를 생성하는 구체적인 동작은 도 7에서 후술한다.

[132] 동작 620에서, 제 1 외부 전자 장치(400)는 공유 키를 수신하기 위한 키 쉐어링 애플릿(예: 도 4의 키 쉐어링 애플릿(431))을 보안 모듈(예: 도 4의 보안 모듈(430))에 설치할 수 있다. 키 쉐어링 애플릿(431)을 설치하는 구체적인 동작은 도 9에서 서술한다.

[133] 동작 630에서, 전자 장치(300)와 제 1 외부 전자 장치(400)는 동작 610에서 생성한 공유 키를 송/수신할 수 있다. 공유 키의 공유 프로세스는 전자 장치(300)의 보안 모듈(330)에 설치된 키 쉐어링 애플릿(333)과 제 1 외부 전자 장치(400)의 보안 모듈(430)에 설치된 키 쉐어링 애플릿(431) 사이에서 수행될 수 있다. 공유 키를 송/수신하는 구체적인 동작에 대해서는 도 10 내지 도 13에서 후술한다.

[134]

[135] 도 7은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 제 2 외부 전자 장치의 인증에 이용되는 공유 키를 생성하는 방법을 도시한 동작 흐름도이다.

[136] 도 7은 도 6의 공유키 생성 동작(동작 610)에 대한 구체적인 내용을 도시하고 있다.

[137] 도 7을 참조하면, 동작 710에서, 전자 장치(예: 도 3의 전자 장치(300))의 프로세서(310)는 사용자 입력에 대응하여 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401) 키 관리 어플리케이션을 실행할 수 있다. 제 2 외부 전자 장치(1401) 키 관리 어플리케이션은 메모리(예: 도 3의 메모리(340)) 상에 설치된 어플리케이션으로, 보안 모듈(예: 도 3의 보안 모듈(330))에 저장된 운송 수단 키 관리 애플릿에 대한 제어를 수행할 수 있다.

[138] 본 발명의 다양한 실시예에 따르면, 프로세서(310)는 운송 수단과 전자 장치(300)의 인증에 이용되는 인증 키를 제 1 외부 전자 장치(400)로 전송할 것을 요청하는 신호를 수신할 수 있다. 예를 들면, 전자 장치(300)의 사용자가 운송 수단의 키 관리 어플리케이션의 사용자 인터페이스를 이용하여 제 1 외부 전자

장치(400)로 인증 키를 전송할 것을 요청할 수 있다.

[139] 동작 720에서, 프로세서(310)는 공유 키의 생성을 위한 정보를 포함하는 사용자 입력을 수신할 수 있다. 본 발명의 다양한 실시예에 다르면, 프로세서(310)는 제 2 외부 전자 장치 키 관리 어플리케이션이 제공하는 사용자 인터페이스를 이용하여, 공유 키의 생성을 위한 정보를 입력하는 사용자 입력을 수신할 수 있다.

[140] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성을 위한 정보는 제 1 외부 전자 장치(400)의 사용자의 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화할 기능에 대한 정보를 포함할 수 있다. 제 2 외부 전자 장치(1401)가 제공 가능한 기능들은 제 2 외부 전자 장치(1401)가의 이용 허용 시간(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 운행이 가능한 시간), 제 2 외부 전자 장치(1401)의 이용 가능한 지역 범위 정보(geofencing limitation data, 예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 운행이 허용되는 지역적인 범위), 제 2 외부 전자 장치(1401)의 성능 제약(예를 들면, 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 최대 허용 속도), 제 2 외부 전자 장치(1401)에 포함된 다양한 장치(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 트렁크, 또는 콘솔 박스) 또는 제 2 외부 전자 장치(1401)가 수행 가능한 다양한 기능(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 차선 유지 보조, 차선 이탈 알림, 크루즈 컨트롤, 어댑티브 크루즈 컨트롤, 또는 엔진 사용 가능 여)의 허용 여부를 지시하는 정보 중 적어도 일부를 포함할 수 있다. 공유 키의 생성을 위한 정보는 전자 장치(300)의 사용자가 제 2 외부 전자 장치(1401)의 키 관리 어플리케이션의 사용자 인터페이스를 이용한 사용자 입력(제 1 외부 전자 장치(400)의 사용자 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화된 기능을 선택하는 사용자 입력)에 의해 생성될 수 있다.

[141] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성을 위한 정보는 생성된 공유키를 암호화하여 제 1 외부 전자 장치(400)로 전송하기 위해 요구되는 데이터를 포함할 수 있다. 예를 들면, 공유 키의 생성을 위한 정보는 생성된 공유키를 대칭 암호화 방식 또는 비대칭 암호화 방식을 이용하여 암호화를 수행하는데 필요한 암호 키를 포함할 수 있다.

[142] 본 발명의 다양한 실시예에 따르면, 동작 720 이후, 동작 730을 수행하기 위한 전자 장치(300)의 인증 동작이 추가될 수 있다. 사용자 인증이 성공한 경우, 프로세서(310)는 공유 키 생성을 위한 정보 및 공유 키 생성 명령을 보안 모듈(330)에 전송할 수 있다. 사용자 인증 방식은 다양한 방식(예를 들면, 핀 번호 입력하는 방식, 사용자의 생체 정보(예를 들면, 지문 입력, 홍채 인식, 또는 얼굴 인식)를 입력하는 방식을 포함할 수 있다)이 이용될 수 있다.

[143] 동작 730에서, 프로세서(310)는 공유 키 생성을 위한 정보 및 공유 키 생성 명령어를 보안 모듈(330)에 전송할 수 있다.

[144] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성은 보안 모듈(330)에 설치된 키 매니징 애플릿(key managing applet, 331)에 의해 구현될 수 있다. 키 매니징 애플릿(331)은 공유 키의 생성을 위한 정보를 이용하여 공유 키를 생성할 수 있다.

[145] 동작 740에서, 키 매니징 애플릿(331)은 공유 키 생성을 위한 정보에 기반하여 공유 키 및 공유 키와 관련된 정보를 생성할 수 있다.

[146] 본 발명의 다양한 실시예에 따르면, 공유 키는 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)의 다양한 기능을 활성화하기 위해서, 제 2 외부 전자 장치(1401)와 인증을 수행하기 위해 요구되는 키를 의미할 수 있다.

[147] 본 발명의 다양한 실시예에 따르면, 공유 키와 관련된 정보는 공유 키가 전자 장치(300)에 저장된 인증 키에 기반하여 생성되었음을 지시하는 정보를 포함할 수 있다. 제 2 외부 전자 장치(1401)는 공유 키와 관련된 정보를 제 1 외부 전자 장치(400)로부터 수신하고, 전자 장치(300)에 저장된 인증 키에 기반하여 생성되었음을 지시하는 정보에 기반하여 유효한 공유 키인지 검증할 수 있다.

[148]

[149] 도 8은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 키 매니징 애플릿(331)에서 생성한 공유 키를 보안 모듈(330)의 키 쉐어링 애플릿(333)에 저장하는 방법을 도시한 동작 흐름도이다.

[150] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)의 키 매니징 애플릿(331)이 SE2SE(보안 모듈에서 다른 보안 모듈로 데이터를 전송하는 통신 규격)을 지원하는 경우, 키 쉐어링 애플릿(333)을 이용하지 않고, 키 매니징 애플릿(331)이 제 1 외부 전자 장치(400)의 키 쉐어링 애플릿(431)로 바로 공유 키 및 공유 키와 관련된 정보를 전송할 수 있다. 이 경우, 도 8에 도시된 동작은 생략될 수 있다.

[151] 동작 810에서, 전자 장치(300)의 제 2 외부 전자 장치(1401)의 키 관리 어플리케이션은 공유 키 생성이 성공했음을 알리는 신호를 키 매니징 애플릿(331)으로부터 수신함에 대응하여, 공유 키 생성 동작이 성공했음을 알리는 신호를 전자 장치(300)의 키 쉐어링 어플리케이션에 전송할 수 있다. 예를 들어, 키 쉐어링 어플리케이션은 전자 장치(300)의 메모리(예: 도 3의 메모리(340))에 설치되며, 보안 모듈(330) 상에 설치된 키 쉐어링 애플릿(333)의 동작을 관리하는 어플리케이션을 의미할 수 있다.

[152] 동작 820에서, 키 쉐어링 어플리케이션은 공유 키를 수신할 것을 지시하는 명령을 보안 모듈(330)에 설치된 키 쉐어링 애플릿(333)에 전송할 수 있다.

[153] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 어플리케이션은 공유 키에 대응하는 AID에 매칭되는 키 쉐어링 애플릿(333)에 공유 키를 수신할 것을 지시하는 명령을 전송할 수 있다.

[154] 동작 830에서, 키 쉐어링 애플릿(333)은 키 쉐어링 어플리케이션이 전송한 공유 키를 수신할 것을 지시하는 명령을 수신함에 대응하여, 키 매니징 애플릿(331)이

전송한 공유 키 및 공유 키 관련 정보를 수신할 수 있다. 일 실시예에 따르면, 키 쉐어링 애플릿(333)은 키 매니징 애플릿(331)에 공유 키 및 공유 키 관련 정보를 요청할 수 있다. 예를 들어, 키 매니징 애플릿(331)은 키 쉐어링 애플릿(333)이 전송한 공유 키 및 공유 키 관련 정보의 요청을 수신함에 대응하여, 키 쉐어링 애플릿(333)으로, 공유 키 및 공유 키 관련 정보를 전송할 수 있다.

[155] 동작 840에서, 키 쉐어링 애플릿(333)은 공유 키 및 공유 키 관련 정보의 수신이 성공했음을 알리는 정보를 키 쉐어링 어플리케이션에 전송할 수 있다.

[156]

[157] 도 9는 본 발명의 다양한 실시예에 따른 제 1 외부 전자 장치((400)에서 공유 키를 수신하기 위한 애플릿을 설치하는 방법(동작 620)을 도시한 동작 흐름도이다.

[158] 도 9를 참조하면, 동작 910에서, 프로세서(예: 도 4의 프로세서(410))는 키 쉐어링 어플리케이션을 실행할 수 있다. 키 쉐어링 어플리케이션은 제 1 외부 전자 장치(400)의 메모리(예: 도 1의 메모리(440)) 상에 설치될 수 있으며, 전자 장치(예: 도 3의 전자 장치(300))로부터 공유 키 및 공유 키와 관련된 정보를 수신하기 위한 키 쉐어링 애플릿(예: 도 4의 키 쉐어링 애플릿(431))을 설치하기 위한 어플리케이션을 의미할 수 있다. 예를 들어, 키 쉐어링 어플리케이션은 설치된 공유 키의 우선 순위에 대한 상태, 활성화 여부에 대한 상태, 운송 수단의 이용 가능한 기능에 대한 정보를 제공 및 변경할 수 있다.

[159] 동작 920에서, 프로세서(410)는 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))와 관련된 정보에 대한 사용자 입력을 수신할 수 있다. 제 2 외부 전자 장치(1401)와 관련된 정보는 제 1 외부 전자 장치(400)의 사용자가 키 쉐어링 어플리케이션의 인터페이스를 이용하여 입력한 정보를 의미할 수 있다. 제 2 외부 전자 장치(1401)와 관련된 정보는 제 2 외부 전자 장치(1401)의 제조사 이름(예를 들면, BMX), 제 2 외부 전자 장치(1401)의 모델 이름(예를 들면, X5)을 포함할 수 있다.

[160] 본 발명의 다양한 실시예에 따르면, 프로세서(410)는 제 1 외부 전자 장치(400)의 사용자가 키 쉐어링 어플리케이션의 인터페이스를 이용하여 입력하는 공유 키의 종류와 관련된 정보를 수신할 수 있다. 공유 키의 종류와 관련된 정보는 전자 장치(300)에 저장된 제 2 외부 전자 장치(1401)의 키와 동일한 공유 키 또는 복수의 이용자가 이용하는 쉐어링 카를 위한 일반적인 공유 키 중 어느 하나를 지정하는 정보를 의미할 수 있다.

[161] 동작 930에서, 프로세서(410)는 수신한 제 2 외부 전자 장치(1401)와 관련된 정보 또는 공유 키의 종류와 관련된 정보 및 키 쉐어링 애플릿(431)을 설치하는 명령을 보안 모듈(430)에 전송할 수 있다.

[162] 본 발명의 다양한 실시예에 따르면, 동작 930 이후, 동작 940을 수행하기 위한 제 1 외부 전자 장치(400)의 인증 동작이 추가될 수 있다. 사용자 인증이 성공한 경우, 프로세서(410)는 키 쉐어링 애플릿(431)을 설치하는 명령을 보안

모듈(430)에 전송할 수 있다. 사용자 인증 방식은 다양한 방식(예를 들면, 핀 번호 입력하는 방식, 사용자의 생체 정보(예를 들면, 지문 입력, 홍채 인식, 또는 얼굴 인식)를 입력하는 방식을 포함할 수 있다)이 이용될 수 있다.

[163] 동작 940에서, 보안 모듈(430)은 제 2 외부 전자 장치(1401)와 관련된 정보에 포함된 제 2 외부 전자 장치(1401)와의 제조사의 식별자(AID)에 대응하는 키 쉐어링 애플릿(431)을 설치할 수 있다.

[164] 본 발명의 다양한 실시예에 다르면, 생성된 키 쉐어링 애플릿(431)은 사용자 정보, 제 2 외부 전자 장치(1401)의 정보, 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)간 송수신되는 암호화에 이용되는 복수의 암호 키에 대한 정보를 포함할 수 있다. 키 쉐어링 애플릿(431)은 수신한 공유 키의 상태를 지시하는 정보를 포함할 수 있으며, 수신한 공유 키의 상태는 표 1에 정의되어 있다.

[165] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(431)은 운송 수단의 제조사의 식별자에 대응하는 공유 키를 수신하기 위해, 제조사의 식별자를 전자 장치(300)의 키 쉐어링 애플릿(333)에 전송할 수 있다. 전자 장치(300) 상에 저장된 공유 키가 제조사의 식별자와 대응하지 않는 경우, 공유 키의 송/수신 동작이 종료될 수 있다.

[166]

[167] 도 10은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 공유 키를 송/수신하는 구체적인 방법을 도시한 동작 흐름도이다.

[168] 도 10을 참조하면, 동작 1001에서, 전자 장치(예: 도 3의 전자 장치(300))는 공유 키를 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400))로 전송하기 위한 공유 키 전송 모드로 진입할 수 있다. 공유 키를 근거리 통신(예: NFC)를 이용하여 송/수신하는 경우, 전자 장치(300)는 NFC 리더 모드로 동작할 수 있다. 공유 키 전송 모드는 전자 장치(300)의 통신 모듈(320)을 NFC 리더 모드로 전환하는 구체적인 동작을 포함할 수 있다. 전자 장치(300)는 공유 키 전송 모드로 진입하고, 제 1 외부 전자 장치(400)에 AID 리스트를 전송할 것을 요청하는 신호를 전송할 수 있다. 공유 키 전송 모드로 진입하는 구체적인 내용에 대해서는 도 11에서 후술한다.

[169] 동작 1003에서, 제 1 외부 전자 장치(400)는 전자 장치(300)가 전송하는 공유 키를 수신하기 위한 공유 키 수신 모드로 진입할 수 있다. 공유 키를 근거리 통신(예: NFC)를 이용하여 송/수신하는 경우, 제 1 외부 전자 장치(400)는 NFC 카드 모드로 동작하면서, 공유 키를 수신할 수 있다.

[170] 동작 1005에서, 전자 장치(300)와 제 1 외부 전자 장치(400)는 SE2SE(secure module to secure module) 리더/카드 에뮬레이션 모드를 이용해서 공유 키를 공유할 수 있다. 전자 장치(300)는 NFC 리더(reader) 모드로 동작할 수 있으며, 제 1 외부 전자 장치(400)는 NFC 카드(card) 모드로 동작할 수 있다. 동작 1005에 대한 구체적인 내용에 대해서는 도 12에서 후술한다.

[171] 동작 1007에서, 공유 키 전송을 완료한 전자 장치(300)는 공유 키 전송 모드에서

일반 모드로 진입할 수 있다. 일반 모드는 통신 채널을 수립하기 위해서 다른 외부 전자 장치가 전송하는 신호를 수신할 수 있도록 하는 listening mode 및 다른 외부 전자 장치가 전자 장치(300)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 모두 지원하는 모드를 의미할 수 있다. 동작 1007에 대한 구체적인 내용에 대해서는 도 13에서 후술한다.

[172] 동작 1009에서, 공유 키 수신을 완료한 제 1 외부 전자 장치(400)는 공유 키 수신 모드에서 일반 모드로 진입할 수 있다. 일반 모드는 통신 채널을 수립하기 위해서 다른 외부 전자 장치가 전송하는 신호를 수신할 수 있도록 하는 listening mode 및 다른 외부 전자 장치가 제 1 외부 전자 장치(400)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 모두 지원하는 모드를 의미할 수 있다.

[173] 동작 1011에서, 전자 장치(300)는 공유 키의 공유 결과(실패 또는 성공)를 지시하는 알림을 수신하고, 공유 키의 공유 결과를 제 2 외부 전자 장치 키 관리 어플리케이션의 이력 정보에 업데이트할 수 있다.

[174] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)는 공유 키의 공유 결과를 전자 장치(300)의 사용자가 인지할 수 있도록 정보를 제공할 수 있다. 예를 들어, 제1 전자 장치(300)의 표시 장치(예: 도 1의 표시 장치(160)) 또는 음향 출력 장치(예: 도 1의 음향 출력 장치(155))를 통해 사용자에게 정보를 제공할 수 있다.

[175] 동작 1013에서, 제 1 외부 전자 장치(400)는 공유 키의 공유 결과(실패 또는 성공)를 지시하는 알림을 수신하고, 공유 결과를 제 1 외부 전자 장치(400)의 사용자가 인지할 수 있도록 출력할 수 있다. 예를 들어, 제 1 외부 전자 장치(400)의 표시 장치(예: 도 1의 표시 장치(160)) 또는 음향 출력 장치(예: 도 1의 음향 출력 장치(155))를 통해 사용자에게 정보를 제공할 수 있다.

[176] 본 발명의 다양한 실시예에 따르면, 공유 키의 수신을 성공한 제 1 외부 전자 장치(400)에 저장된 공유 키는 아직 비활성화 상태일 수 있다. 예를 들어, 공유 키는 제 2 외부 전자 장치(1401)와의 통신 연결시 제 2 외부 전자 장치(1401)의 공유 키에 대한 검증 후, 활성화될 수 있다.

[177]

[178] 도 11은 공유 키를 전송하는 전자 장치가 공유 키를 전송하는 전송 모드를 도시한 도면이다. 도 11에 도시된 실시예는, 도 10에 도시된 실시예 중, 공유 키를 전송하는 모드로 진입하는 실시예(동작 1001)에 대한 설명이다.도 11을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))는 제 2 외부 전자 장치의 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107)(예: 도 3의 보안 모듈(330))을 포함할 수 있다. 도 11에 도시된 실시예는 전자 장치(예: 도 3의 전자 장치(300)제 2 외부 전자 장치 키 관리 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107) 의 동작 주체들 간에 수행될 수 있다.

[179] 본 발명의 다양한 실시예에 따르면, NFC 서비스(1103)는 통신 모듈(예: 도 3의

통신 모듈(320))에 포함된 제어 회로를 의미할 수 있다. CLF(1105)는 NFC 통신을 수행하는 안테나를 포함하는 프론트 엔드 회로를 의미할 수 있다.

[180] 동작 1109에서, 제 2 외부 전자 장치의 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션(1101)은 NFC 서비스(1103)를 지정된 NFC 리더 모드로 설정(SET dedicated reader mode)하도록 제어할 수 있다. NFC 서비스(1103)는 제 2 외부 전자 장치의 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션(1101)에서 전송한 신호를 수신함에 대응하여, NFC 리더 모드로 동작하도록 CLF(1105)를 제어할 수 있다.

[181] 동작 1111에서, NFC 서비스(1103)는 CLF(1105)를 비활성화하는 명령(RF_DEACTIVATE_CMD)을 CLF(1105)로 전송할 수 있다.

[182] 본 발명의 다양한 실시예에 따르면, CLF(1105)는 기존에 수행하는 모드를 비활성화 후, NFC 리더 모드로 동작할 수 있다. 동작 1113에서, CLF(1105)는 비활성화 명령의 응답 신호(RF_DEACTIVATE_RSP)를 NFC 서비스(1103)에 전송할 수 있다.

[183] 동작 1115에서, NFC 서비스(1103)는 호스트(보안 모듈)를 선택하는 신호(SELECT_HOST_CMD)를 CLF(1105)로 전송할 수 있다. 예를 들어, 호스트는 수신한 데이터를 수신하는 구성 요소 또는 송신하는 데이터가 존재하는 구성 요소를 의미할 수 있다. 본 실시예에서는, 공유 키는 보안 모듈(1107)에 존재하기 때문에, 호스트는 보안 모듈(1107)에 해당될 수 있다. 동작 1117에서, CLF(1105)는 동작 1115에서 전송한 호스트 선택 신호의 응답 신호(SELECT_HOST_RSP)를 NFC 서비스(1103)에 전송할 수 있다.

[184] 동작 1119에서, NFC 서비스(1103)는 리더 모드를 활성화 하는 명령(READER_MODE_CMD)을 CLF(1105)로 전송할 수 있다. 동작 1121에서, CLF(1105)는 리더 모드를 활성화 하는 명령의 응답 신호(READER_MODE_RSP)를 NFC 서비스(1103)에 전송할 수 있다. 동작 1123에서, NFC 서비스(1103)은 결과를 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)에 전송할 수 있다.

[185] 동작 1125에서, 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)은 AID를 선택하는 명령(SELECT AID APDU CMD)을 보안 모듈(1107)에 전송할 수 있다. 동작 1127에서, 보안 모듈(1107)은 AID 선택하는 명령의 응답 신호(SELECT AID APDU RSP)를 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)에 전송할 수 있다.

[186] 동작 1129에서, 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)은 리더 게이트를 활성화 하는 명령(ENABLE READER GATE CMD)을 보안 모듈(1107)에 전송할 수 있다. 리더 게이트를 활성화 하는 명령은 보안 모듈(1107)이 공유 키 및 공유 키 관련 데이터를 전송하는 준비 동작을 수행하는 것을 의미한다. 동작 1131에서, 보안 모듈(1107)은 리더 게이트를 활성화 하는 명령의 응답 신호(ENABLE READER GATE RSP)를 제 2

외부 전자 장치 키 관리 어플리케이션(1101)에 전송할 수 있다.

[187] 동작 1133에서, 보안 모듈(1107)은 리더 모드로 동작할 것을 요청(EVT_READER_REQUESTED)하는 신호를 CLF(1105)로 전송할 수 있다. 동작 1135에서, CLF(1105)는 보안 모듈(1107)이 전송한 리더 모드로 동작할 것을 요청(READER_MODE_NTF)하는 신호를 NFC 서비스(1103)로 전송할 수 있다.

[188] 동작 1137에서, NFC 서비스(1103)은 리더 모드로 동작하는 명령(READER_MODE_CMD)을 CLF(1105)로 전송할 수 있다. 동작 1139에서, CLF(1105)는 리더 모드로 동작하는 명령의 응답 신호(READER_MODE_RSP)를 NFC 서비스(1103)으로 전송하고, 동작 1141에서, CLF(1105)는 공유 키 전송 모드로 진입할 수 있다. 공유 키 전송 모드는 제 1 외부 전자 장치(400)가 전자 장치(300)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 지원하는 모드를 의미할 수 있다.

[189]

[190] 도 12는 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 공유 키를 송/수신하는 동작을 도시한 흐름도이다. 도 12에 도시된 실시예는, 도 10에 도시된 실시예 중, 공유 키를 공유하는 동작(동작 1005)에 대한 실시예에 관한 것이다.

[191] 도 12에 도시된 실시예는, 전자 장치(예: 도 3의 전자 장치(300)) 및 제 1 외부 전자 장치(예: 도 4의 전자 장치(400))간 공유 키 및 공유 키와 관련된 정보를 송/수신하는 동작(예: 도 10의 1005)의 실시예이다.

[192] 도 12를 참조하면, 일 실시예에 따르면, 공유 키 및 공유 키와 관련된 정보를 전송하는 전자 장치(300)는 리더 모드로 동작하고, 공유 키 및 공유 키와 관련된 정보를 수신하는 제 1 외부 전자 장치(400)는 카드 모드로 동작할 수 있다.

[193] 전자 장치(300) 및 제 1 외부 전자 장치(400)가 송 수신하는 데이터는 1 개의 APDU(application protocol data unit)으로 정의된 데이터 규격을 따를 수 있다. 전자 장치(300)가 제 1 외부 전자 장치(400)로 명령을 전송하면서, 전송되는 데이터는 C-APDU(command- application protocol data unit)으로 정의되며, 제 1 외부 전자 장치(400)가 전자 장치(300)에 응답하면서, 전송되는 데이터는 R-APDU(response - application protocol data unit)으로 정의될 수 있다. 본 발명의 다양한 실시예에 따르면, 전자 장치(300) 및 제 1 외부 전자 장치(400)는 C-APDU, R-APDU 포맷으로 정의된 데이터 규격을 이용하여 아래에 기재된 동작을 수행할 수 있다.

[194] 먼저, 전자 장치(300)의 보안 모듈(330)은 통신 모듈(320)을 이용하여 AID 리스트를 전송할 것을 제 1 외부 전자 장치(400)에 요청할 수 있다. 제 1 외부 전자 장치(400)의 보안 모듈(430)은 통신 모듈(420)을 통해 AID 리스트를 전자 장치(300)로 전송할 수 있다.

[195] 전자 장치(300)의 보안 모듈(330)은 수신한 AID 리스트에서 전송될 공유키에 대응하는 AID를 선택하고, 선택된 AID를 지시하는 정보와 선택된 AID에

대응하는 키 쉐어링 애플릿과 관련된 정보를 전송할 것을 제 1 외부 전자 장치(400)에게 요청할 수 있다. 제 1 외부 전자 장치(400)의 보안 모듈(430)은 키 쉐어링 애플릿과 관련된 정보(예를 들면, 키 쉐어링 애플릿의 버전 정보, 사용자 정보)를 통신 모듈(420)을 통해 전자 장치(300)로 전송할 수 있다.

[196] 전자 장치(300)의 보안 모듈(330)은 키 쉐어링 애플릿과 관련된 정보를 확인하고, 키 쉐어링 애플릿의 상태(표 1에 정의된 상태)를 확인할 수 있다.

[197] 전자 장치(300)의 보안 모듈(330)과 제 1 외부 전자 장치(400)의 보안 모듈(430)은 암호 키를 이용하여 상호 인증을 수행하고, 상호 인증이 완료된 경우, 보안 모듈(330)은 제 1 외부 전자 장치(400)의 보안 모듈(430)로 통신 모듈(320)을 이용하여 생성된 공유 키 및 공유 키와 관련된 정보를 전송할 수 있다.

[198] 제 1 외부 전자 장치(400)의 보안 모듈(430)은 공유 키 및 공유 키와 관련된 정보를 전자 장치(300)로부터 수신하고, 공유 키와 관련된 정보에 포함된 공유 키 상태를 비활성화로 변경할 수 있다.

[199] 본 발명의 다양한 실시예에 따르면, 상기에 기재된 전자 장치(300)와 제 1 외부 전자 장치(400) 사이의 데이터 교환은 동작 1201, 1203, 1205, 1207에 도시된 C-APDU, R-APDU의 데이터 규격을 통해 송/수신될 수 있다.

[200]

[201] 도 13은 공유 키를 전송하는 전자 장치가 공유 키를 전송하는 전송 모드에서 일반 모드로 전환되는 실시예를 도시한 도면이다.

[202] 도 13을 참조하면, 전자 장치(예: 도 3의 전자 장치(300))가 공유 키 및 공유 키와 관련된 정보를 제 1 외부 전자 장치(예: 도 4의 전자 장치(400))에 전송한 후, 일반 모드로 전환하는 실시예를 도시하고 있다. 도 13에 도시된 실시예는 도 10에 도시된 실시예 중, 공유 키를 공유하는 동작이 완료된 후, 공유 키 전송 모드에서 일반 모드로 전환하는 동작(동작 1007)의 실시예와 관련된 것이다.

[203] 도 13을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))는 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))의 키 관리 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107)(예: 도 3의 보안 모듈(330))을 포함할 수 있다. 도 13에 도시된 실시예는 제 2 외부 전자 장치 키 관리 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107)의 동작 주체들 간에 수행될 수 있다.

[204] 본 발명의 다양한 실시예에 따르면, NFC 서비스(1103)는 통신 모듈(예: 도 3의 통신 모듈(320))에 포함된 제어 회로를 의미할 수 있다. CLF(1105)는 NFC 통신을 수행하는 안테나를 포함하는 프론트 엔드 회로를 의미할 수 있다.

[205] 동작 1301에서, 보안 모듈(1107)은 공유 키의 공유가 완료되었음을 알리는 신호(EVT_TRANSACION)를 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 전송할 수 있다.

[206] 동작 1303에서, 제 2 외부 전자 장치 키 관리 어플리케이션(1101)은 리더 게이트를 비활성화 하는 명령(DISABLE READER GATE CMD)를 보안 모듈(1107)에 전송하고, 보안 모듈(1107)은 동작 1305에서, 리더 게이트를 비활성화 하는 명령의 응답 신호(DISABLE READER GATE RSP)를 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 전송할 수 있다.

[207] 동작 1307에서, 보안 모듈(1107)은, 리더 모드를 종료하는 신호(EVT_END_OPERATION)를 CLF(1105)에 전송할 수 있다. 동작 1309에서, CLF(1105)는 리더 모드가 종료되었음을 알리는 신호(READER_MODE_NTF)를 NFC 서비스(1103)에 전송할 수 있다.

[208] 동작 1311에서, 제 2 외부 전자 장치 키 관리 어플리케이션(1101)은 지정된 리더 모드를 비활성화 하는 신호(disable dedicated reader mode)를 NFC 서비스(1103)에 전송할 수 있다.

[209] 동작 1313에서, NFC 서비스(1103)는 리더 모드를 종료하는 명령(READER_MODE_CMD)을 CLF(1105)에 전송하고, CLF(1105)는 리더 모드를 종료할 수 있다. 동작 1315에서, CLF(1105)는 리더 모드가 종료되었음을 알리는 응답 메시지(READER_MODE_RSP)를 NFC 서비스(1103)에 전송할 수 있다.

[210] 동작 1317에서, NFC 서비스(1103)는 일반 모드로 동작할 것을 명령하는 신호(RF_DISCOVERY_CMD)를 CLF(1105)에 전송할 수 있다. 동작 1319에서, CLF(1105)는 일반 모드로의 동작을 수행할 수 있다. 예를 들어, RF 디스커버리 프로세스를 수행할 수 있다. 동작 1321에서, CLF(1105)는 일반 모드로의 동작을 알리는 응답 메시지(RF_DISCOVERY_RSP)를 NFC 서비스에 전송할 수 있다.

[211] 동작 1323에서, NFC 서비스(1103)는 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 일반 모드로의 동작을 알리는 메시지를 전송할 수 있다.

[212] 본 발명의 다양한 실시예에 따르면, 일반 모드는 통신 채널을 수립하기 위해서 다른 외부 전자 장치가 전송하는 신호를 수신할 수 있도록 하는 listening mode 및 다른 외부 전자 장치가 제 1 외부 전자 장치(400)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 모두 지원하는 모드를 의미할 수 있다.

[213] 본 발명의 다양한 실시예에 따르면, 도 11 및 도 13에 개시된 실시예들은 순차적으로 동작하는 것처럼 도시하였으나, 반드시 순차적으로 동작하지 않고, 각 동작이 동시에 동작할 수 있으며(예를 들면, 동작 1303과 동작 1311은 동시에 구현될 수도 있다), 일부 동작은 다른 동작보다 더 먼저 동작할 수도 있다.

[214] 본 발명의 다양한 실시예에 따르면, 도 11 및 도 13에 개시된 실시예들은, 전자 장치(300)에서 수행되는 실시예들이지만, 제 1 외부 전자 장치(400)의 모드 변경 역시, 도 11 및 도 13에 개시된 동작을 이용하여 구현될 수 있다.

[215]

[216] 도 14는 제 2 외부 전자 장치(1401)가 제 1 외부 전자 장치(400)가 전송한 공유 키의 유효성을 검증하는 실시예를 도시한 도면이다.

[217] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(예: 도 4의 전자 장치(400))는 전자 장치(예: 도 3의 전자 장치(300))로부터 공유 키 및 공유 키와 관련된 정보를 수신할 수 있다. 공유 키와 관련된 정보에는 공유 키의 상태를 지시하는 정보가 포함될 수 있다. 공유 키의 상태는 공유 키를 수신하지 못한 상태(예: 표 1의 index 1), 공유 키를 수신했으나, 아직 제 2 외부 전자 장치(1401)가 권한을 허용하지 않은 상태(예: 표 1의 index 2), 공유 키를 수신했고, 제 2 외부 전자 장치(1401)가 권한을 허용한 상태(예: 표 1의 index 3), 공유 키가 유효하지 않은 상태(예: 표 1의 index 4)로 구성될 수 있다.

[218] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)가 공유 키를 수신한 경우, 공유 키의 상태는 공유 키를 수신했고, 제 2 외부 전자 장치(1401)가 권한을 허용 하지 않은 상태(index 2)에 해당될 수 있다. 공유 키는 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)와 공유 키 수신 후 첫 연결시 수행되는 제 2 외부 전자 장치(1401)의 검증 결과에 따라서 제 2 외부 전자 장치가 권한을 허용한 상태(index 3)로 변경될 수 있다. 이하, 제 2 외부 전자 장치가 제 1 외부 전자 장치(400)가 수신한 공유 키를 검증하는 실시예에 대해서 서술한다.

[219] 동작 1411에서, 제 1 외부 전자 장치(400)와 제 2 외부 전자 장치(1401)는 통신 채널을 설립할 수 있다.

[220] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)와 제 2 외부 전자 장치(1401)는 근거리 통신 방식을 이용하여 통신 채널을 설립할 수 있다. 제 2 외부 전자 장치(1401)에 포함된 근거리 통신 모듈이 리더 모드로 동작하고, 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)에 근접(또는, 태그)하는 경우, 제 1 외부 전자 장치(400)와 제 2 외부 전자 장치(1401) 사이의 통신 채널이 생성될 수 있다.

[221] 동작 1413에서, 제 1 외부 전자 장치(400)는 공유 키와 공유 키 관련 정보를 제 2 외부 전자 장치(1401)에 전송할 수 있다.

[222] 동작 1415에서, 제 2 외부 전자 장치(1401)는 제 1 외부 전자 장치(400)가 전송한 공유 키의 검증을 수행할 수 있다.

[223] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)에 저장된 인증 키가 마스터 키인 경우, 제 1 외부 전자 장치(400)는 마스터 키에 기반하여 생성된 공유 키를 전자 장치(300)로부터 수신할 수 있다. 이 경우, 제 2 외부 전자 장치(1401)는 공유 키가 마스터 키에 기반하여 생성되었는지 확인한 결과에 기반하여 공유 키의 유효성을 검증할 수 있다.

[224] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)에 저장된 인증 키가 마스터 키에 기반하여 생성된 1차 공유 키인 경우, 제 1 외부 전자 장치(400)는 1차 공유 키에 기반하여 생성된 토큰을 전자 장치(300)로부터 수신할 수 있다. 제 1 외부 전자 장치(400)는 전자 장치(300)로부터 수신한 토큰을 제 2 외부 전자 장치(1401)로 전송할 수 있다. 이 경우, 제 2 외부 전자 장치(1401)는 토큰이 1차 공유 키에 기반하여 생성되었는지 확인한 결과에 기반하여 토큰의 유효성을

검증할 수 있다.

[225] 동작 1417에서, 제 2 외부 전자 장치(1401)는 공유 키 또는 토큰의 검증 결과에 기반하여 공유 키 및 공유 키와 관련된 정보를 등록할 수 있다.

[226] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)에 저장된 인증 키가 마스터 키인 경우, 제 1 외부 전자 장치(400)는 1차 공유 키 및 공유 키와 관련된 정보를 전자 장치(300)로부터 수신할 수 있다. 이 경우, 제 2 외부 전자 장치(1401)는 1차 공유 키를 확인한 결과에 기반하여 유효성을 검증하고, 유효한 공유 키 및 인 경우, 새로운 사용자의 1차 공유 키 및 공유 키와 관련된 정보를 등록할 수 있다.

[227] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)은 프로세서(410) 또는 메모리(440)(예: 도 1의 메모리(130))와 물리적으로 분리된 모듈로써, 보안 모듈(430) 상에 저장된 데이터를 암호화하여 저장할 수 있다. 본 발명의 다른 실시예에 따르면, 보안 모듈(430)은 메모리(440)의 일 영역에 포함될 수 있으며, 보안 모듈(430)은 메모리(440) 상에 저장된 데이터를 암호화하여 저장된 부분을 의미할 수 있다. 보안 모듈(430)은 보안 모듈(430) 상의 데이터의 접근 요청을 수신함에 대응하여, 데이터의 접근 요청의 주체(예를 들면, 메모리(440) 상에 설치된 다양한 어플리케이션 등)의 접근 권한, 무결성 검증을 수행하고, 수행한 결과에 따라 보안 모듈(430) 상에 저장된 데이터의 접근/편집을 허가 또는 저장된 데이터를 전송할 수 있다.

[228] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)은 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)와 인증을 수행하는데 이용되는 제 2 외부 전자 장치(1401)의 키 애플릿을 관리하는 CRS(Contactless register service)를 포함할 수 있다. CRS(미도시)는 사용자의 요청에 기반하여 애플릿에 할당된 데이터의 수정, 추가, 또는 삭제를 수행할 수 있다.

[229] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)은 PVKSE(proximity vehicle key system environment)를 포함할 수 있다. PVKSE(예: 도 5의 PVKSE(510))는 보안 모듈(430)에 설치된 키 매니징 애플릿에 할당된 데이터의 수정, 추가, 또는 삭제에 대한 모니터링을 수행하고, 운송 수단 키 애플릿과 관련된 데이터의 변경을 감지하면, 운송 수단 키 애플릿과 관련된 정보를 생성 또는 생성된 애플릿과 관련된 정보를 변경할 수 있다. PVKSE(510)는 보안 모듈(430)에 저장된 데이터를 관리하는 CRS(contactless registry service)와는 소프트웨어적으로 별도로 구현된 구성 요소를 의미할 수 있다. PVKSE(510) 및 CRS(520)를 이용하여 공유 키를 수신하는 구체적인 동작에 대해서는 도 5에서 서술한다.

[230] 본 발명의 다양한 실시예에 따르면, 보안 모듈(430)에 설치된 키 쉐어링 애플릿(431)은 전자 장치(300)의 보안 모듈(330)에 설치된 키 쉐어링 애플릿(333)과의 상호 동작을 통하여 전자 장치(300)의 보안 모듈(330)에 설치된 공유 키 및 공유 키와 관련된 정보를 수신할 수 있다.

[231] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(431)를 이용하여 수신한

공유 키는 공유 키를 수신한 후 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)가 서로 처음으로 연결되는 경우 활성화될 수 있다. 제 2 외부 전자 장치(1401)는 제 1 외부 전자 장치(400)가 연결되면서 전송하는 공유 키를 검증하고, 검증 결과에 기반하여 공유 키의 활성화 여부를 결정할 수 있다. 활성화 이전의 공유 키는 표 1의 2 상태(PRIVILEGE DEACTIVE)와 같이 유지되며, 활성화 후의 공유 키는 표 1의 3 상태(PRIVILEGE ACTIVE)로 변화될 수 있다.

[232] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(431)은 2차 공유 키의 생성을 위한 토큰을 수신한 경우, 2차 공유 키의 생성을 위한 토큰을 제 2 외부 전자 장치(1401)에 전송할 수 있다. 제 2 외부 전자 장치(1401)는 2차 공유 키의 생성을 위한 토큰이 전자 장치(300)에 저장된 1차 공유 키에 기반하여 생성되었는지 확인하면서, 2차 공유 키의 생성을 위한 토큰의 유효성을 검증하고, 2차 공유 키를 생성할 수 있다. 생성된 공유 키는 키 쉐어링 애플릿(431)으로 전송될 수 있다. 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)간의 상호 동작에 대해서는 도 14에서 후술한다.

[233]

[234] 도 5는 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))에서, 보안 모듈(330)을 도시한 블록도이다.

[235] 도 5를 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(300)의 보안 모듈(330)은 발급된 보안 도메인(issued security domain, ISD, 581)과 추가 보안 도메인(supplementary security domain, SSD, 582)로 구분될 수 있다.

[236] 본 발명의 다양한 실시예에 따르면, ISD(581)에는 PVKSE(510) 및 CRS(520)가 설치될 수 있다. PVKSE(510)는 SSD(582)에 설치된 적어도 하나 이상의 제 2 외부 전자 장치(1401)의 키 관리 애플릿(530, 540, 550, 560, 또는 570)과 관련된 데이터를 관리할 수 있는 소프트웨어적 요소를 의미할 수 있다. PVKSE(510)는 적어도 하나 이상의 제 2 외부 전자 장치(1401)의 키 관리 애플릿(530, 540, 550, 560, 또는 570)과 관련된 데이터의 변경을 모니터링하고, 변경을 감지한 경우, 데이터 변경을 반영한 애플릿과 관련된 정보를 생성 또는 변경할 수 있다.

[237] 본 발명의 다양한 실시예에 따르면, PVKSE(510)는 적어도 하나 이상의 제 2 외부 전자 장치(1401)의 키 관리 애플릿(530, 540, 550, 560, 또는 570)과 관련된 정보를 관리할 수 있다. 애플릿과 관련된 정보는 제 2 외부 전자 장치(1401)의 제조사의 식별자를 의미하는 애플릿 식별자, 제 2 외부 전자 장치(1401)의 모델을 지시하는 애플릿 라벨, 애플릿의 우선 순위를 지시하는 우선 순위 정보, 또는 애플릿의 구체적인 데이터를 포함할 수 있다.

[238] 본 발명의 다양한 실시예에 따른 보안 모듈(330)은 적어도 하나 이상의 운송 수단 키 관리 애플릿(530, 540, 550, 560, 또는 570)을 관리하는 CRS(520)를 포함하고, CRS(520)의 제어에 기반하여 적어도 하나 이상의 애플릿(530, 540, 550, 560, 또는 570)의 관리를 수행할 수 있다.

[239] 본 발명의 다양한 실시예에 따르면, CRS(520)는 보안 모듈(330) 상에 설치되는 파일을 관리하는 소프트웨어적인 요소를 의미할 수 있다. CRS(520)는 프로세서(예: 도 3의 프로세서(310))의 요청에 기반하여 보안 모듈(330)에 저장된 다양한 데이터의 관리(예를 들면, 데이터의 암호화, 암호화된 데이터의 복호화 등)를 수행할 수 있으며, 보안 모듈(330)에 저장된 데이터를 메모리(예: 도 3의 메모리(350))에 이동시킬 수 있다.

[240] 본 발명의 다양한 실시예에 따르면, 보안 모듈(330)의 PVKSE(510)는 보안 모듈(330)상에 저장된 운송 수단 키 애플릿들 각각의 애플릿 식별자(applet identification, AID)를 포함하는 AID 리스트를 생성할 수 있다. AID 리스트는 PVKSE(510)에서 생성 및 관리할 수 있다.

[241] 전자 장치(예: 도 3의 전자 장치(300))는 제 1 외부 전자 장치(400)로 공유 키의 전송을 수행하기 위해서, 제 1 외부 전자 장치(400)의 보안 모듈(430)에 저장된 AID 리스트의 전송을 제 1 외부 전자 장치(400)에 요청할 수 있다. 예를 들어, 제 1 외부 전자 장치(400)의 보안 모듈(430)에 저장된 AID 리스트의 전송은 SELECT PVKSE로 정의된 명령어를 이용할 수 있다. PVKSE(510)는 SELECT PVKKE로 정의된 명령어를 수신함에 대응하여 AID 리스트의 생성 및 전송을 수행할 수 있다.

[242] 본 발명의 다양한 실시예에 따르면, PVKSE(510)는 전자 장치(300)의 요청에 대응해서, AID 리스트를 전자 장치(300)로 전송할 수 있다. 전자 장치(300)의 키 쉐어링 애플릿(333)은 제 1 외부 전자 장치(400)로부터 AID 리스트를 수신하고, 공유 키에 대응하는 AID가 AID 리스트에 포함되는지 확인할 수 있다. 키 쉐어링 애플릿(333)은 공유 키에 대응하는 AID가 수신한 AID 리스트에 포함된 경우, 공유 키에 대응하는 AID 정보를 제 1 외부 전자 장치(400)에 전송하는 동작을 수행할 수 있다.

[243] 본 발명의 다양한 실시예에 따르면, PVKSE(510)는 키 쉐어링 애플릿(333)이 전송하는 선택된 AID 정보를 수신하고, 선택된 AID 에 대응하는 애플릿과 관련된 정보(예를 들면, 제 2 외부 전자 장치(1401)와 관련된 정보, 키 쉐어링 애플릿(431)의 정보(키 쉐어링 애플릿의 버전))를 전송할 수 있다.

[244] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(530, 540, 550, 560, 또는 570)들 각각은 SSD(582)에 저장될 수 있다. SSD(582)는 제 2 외부 전자 장치(1401)의 제조사별로 구별된 상태로, 제조사 각각에 대응하는 애플릿을 대응하는 제조사별로 구별된 SSD(582)에 저장할 수 있다. 예를 들면, 제조사 1에 대응하는 애플릿들(550, 560)은 제조사 1에 대응하는 SSD 공간(584)에 저장될 수 있고, 제조사 2에 대응하는 애플릿 (570)은 제조사 2에 대응하는 SSD 공간(585)에 저장될 수 있다. SSD(582)는 다양한 사용자가 이용 가능한 제 2 외부 전자 장치(1401) (예를 들면, 카 쉐어링의 공유 대상이 되는 운송 수단)을 위한 공유 키를 위한 애플릿(530, 540)을 별도로 저장할 수 있는 SSD 공간(583)을 더 포함할 수 있다.

[245] 본 발명의 다양한 실시예에 따르면, 적어도 하나 이상의 애플릿(530, 540, 550, 560, 또는 570)들 각각은 애플릿의 활성화 여부를 지시하는 데이터를 포함할 수 있다. 활성화된 애플릿은 제 2 외부 전자 장치(1401)와 전자 장치(300) 의 인증을 수행 가능한 애플릿을 의미하며, 비활성화된 애플릿은 제 2 외부 전자 장치(1401)와 전자 장치(300) 의 인증이 수행될 수 없는 애플릿을 의미할 수 있다.

[246] 본 발명의 다양한 실시예에 따르면, 도 5는 전자 장치(300)의 보안 모듈(330)의 실시예를 중심으로 기재되었으나, 제 1 외부 전자 장치(400)가 전자 장치(300)가 전송한 키를 수신한 경우, 제 1 외부 전자 장치(400)의 보안 모듈(430)은 도 5의 실시예와 동일한 방법으로 전자 장치(300)가 전송한 키를 저장할 수 있다.

[247]

[248] 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))는 프로세서(예: 도 3의 프로세서(310)), 무선 통신을 지원하는 적어도 하나의 통신 모듈(예: 도 3의 통신 모듈(320)) 및 제 1 외부 전자 장치(예: 도 4의 제1 외부 전자 장치(400))로 전송될 공유 키 및 제 2 외부 전자 장치와의 인증에 이용되는 인증 키의 저장 및 관리를 수행하는 애플릿이 설치된 보안 모듈(예: 도 3의 보안 모듈(330))을 포함하고, 상기 프로세서(310)는 상기 인증 키의 제 1 외부 전자 장치로의 전송의 요청을 제 1 외부 전자 장치(400)로부터 수신하고, 상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 상기 보안 모듈(330)에 전송하고, 상기 공유 키 생성을 위한 정보에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈(330)을 제어하고, 상기 생성된 공유 키 및 생성된 공유 키와 관련된 정보를 제 1 외부 전자 장치(400)로 전송하도록 상기 보안 모듈(330)을 제어하도록 설정될 수 있다.

[249] 본 발명의 다양한 실시예에 따르면, 상기 공유 키와 관련된 정보는 상기 인증 키에 기반하여 생성됨을 지시하는 정보를 포함할 수 있다.

[250] 본 발명의 다양한 실시예에 따르면, 상기 공유 키와 관련된 정보는 상기 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))가 제공 가능한 기능 중 적어도 일부의 기능을 활성화 할 것을 지시하는 정보를 포함할 수 있다.

[251] 본 발명의 다양한 실시예에 따르면, 상기 입력된 공유 키 생성을 위한 정보는 상기 제 2 외부 전자 장치(1401)의 이용 허용 시간, 상기 제 2 외부 전자 장치(1401)의 이용 가능한 지역 범위 정보(geofencing limitation data)을 포함할 수 있다.

[252] 본 발명의 다양한 실시예에 따르면, 상기 프로세서(310)는 상기 공유 키의 암호화를 위한 암호 키를 상기 공유 키의 생성을 위한 정보와 함께 상기 보안 모듈(330)로 전송하도록 설정될 수 있다.

[253] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(330)은 상기 제 1 외부 전자 장치(400)의 보안 모듈(예: 도 4의 보안 모듈(430))에 설치된 상기 공유 키를 관리할 애플릿(예: 도 4의 키 쉐어링 애플릿(431))과 관련된 정보를 수신하고, 상기 수신한 애플릿과 관련된 정보에 기반하여 상기 공유 키를 상기 제 1 외부

전자 장치(400)에 전송할지 여부를 결정하도록 설정될 수 있다.

[254] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(330)은 상기 애플릿과 관련된 정보에 포함된 애플릿 식별자가 상기 공유 키에 대응하는 식별자와 동일한지 확인하고, 상기 애플릿 식별자와 상기 공유 키에 대응하는 식별자가 동일한지 여부에 기반하여 상기 공유 키를 상기 제 1 외부 전자 장치(400)에 전송할지 여부를 결정하도록 설정될 수 있다.

[255] 본 발명의 다양한 실시예에 따르면, 상기 애플릿과 관련된 정보는 상기 애플릿이 저장된 주소, 애플릿 식별자, 상기 제 1외부 전자 장치(400)의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(applet - specific data) 중 적어도 하나 이상을 포함할 수 있다.

[256] 본 발명의 다양한 실시예에 따르면, 상기 인증 키는 마스터 키 또는 상기 마스터 키에 기반하여 생성된 키 중 하나이며, 상기 인증 키가 상기 마스터 키에 기반하여 생성된 키인 경우, 상기 보안 모듈(330)은 상기 공유 키가 상기 인증 키에 기반하여 생성되었음을 지시하는(indicating) 토큰을 생성하고, 상기 토큰 및 상기 공유 키와 관련된 정보를 상기 제 1외부 전자 장치(400)로 전송하도록 설정될 수 있다.

[257] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)는 상기 통신 모듈(320)을 이용하여 상기 공유 키 및 상기 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치(400)에 전송하도록 설정될 수 있다.

[258]

[259] 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 4의 제 1 외부 전자 장치(400)는 프로세서(예: 도 4의 프로세서(410)), 무선 통신을 지원하는 적어도 하나의 통신 모듈(예: 도 4의 통신 모듈(420)) 및 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))의 인증에 이용되는 인증 키를 관리하는 애플릿과 관련된 정보를 관리하고, 애플릿 식별자(applet identification, AID) 리스트 및 상기 애플릿을 저장하는 보안 모듈(430)을 포함하고, 상기 보안 모듈(430)은 상기 애플릿과 관련된 정보를 요청하는 신호를 상기 제 1 외부 전자 장치(예: 도 3의 전자 장치(300))로부터 수신하고, 상기 애플릿과 관련된 정보를 상기 제 1 외부 전자 장치(300)로 전송하고, 상기 제 1 외부 전자 장치(300)로부터 상기 공유 키 및 상기 공유 키와 관련된 정보를 수신하고, 상기 수신한 공유 키 및 상기 공유 키와 관련된 정보를 상기 보안 모듈(430) 상에 설치하도록 설정될 수 있다.

[260] 본 발명의 다양한 실시예에 따르면, 상기 프로세서(420)는 상기 제 2 외부 전자 장치(1401) 의 정보를 상기 제 1 외부 전자 장치(300)로부터 수신하고, 상기 제 2 외부 전자 장치(1401)의 정보에 기반하여 상기 공유 키를 관리할 애플릿 식별자를 확인하고, 상기 애플릿을 설치하는 명령을 상기 보안 모듈(430)에 전송하도록 설정될 수 있다.

[261] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(430)은 상기 보안 모듈에

설치된 애플릿이 복수인 경우, 상기 공유 키를 관리할 애플릿을 제외한 나머지 애플릿을 비활성화하고, 상기 공유 키의 설치가 완료됨에 대응하여, 상기 나머지 애플릿을 활성화하도록 설정될 수 있다.

[262] 본 발명의 다양한 실시예에 따르면, 상기 보안 모듈(430)은 상기 애플릿과 관련된 정보를 관리하는 PVKSE(proximity vehicle key system environment)(예: 도 5의 PVKSE(510))를 포함하고, 상기 PVKSE(510) 는 상기 보안 모듈의 발급된 보안 도메인(issued security domain)(예: 도 5의 ISD(581))에 저장되며, 상기 애플릿은 추가 보안 도메인(supplementary security domain)(예: 도 5의 SSD(582))에 저장되도록 설정될 수 있다.

[263] 본 발명의 다양한 실시예에 따르면, 상기 공유키와 관련된 정보는 상기 제 1 외부 전자 장치(300)에 저장되고, 상기 제 2 외부 전자 장치(1401)의 인증에 이용되는 인증 키에 기반하여 생성됨을 지시하는 정보를 포함할 수 있다.

[264] 본 발명의 다양한 실시예에 따르면, 상기 제 1 외부 전자 장치(300)에 저장된 인증 키는 마스터 키 또는 상기 마스터 키에 기반하여 생성된 키 중 하나이며, 상기 인증키가 상기 마스터 키에 기반하여 생성된 키인 경우, 상기 보안 모듈(430)은 상기 공유 키가 상기 인증 키에 기반하여 생성되었음을 지시하는(indicating) 토큰을 상기 제 1 외부 전자 장치(300)로부터 수신하고, 상기 제 2 외부 전자 장치(1401)에 상기 토큰을 전송하고, 상기 제 2 외부 전자 장치(1401)가 상기 토큰에 기반하여 생성한 공유 키를 수신하도록 설정될 수 있다.

[265]

[266] 도 6은 본 발명의 다양한 실시예에 따른 전자 장치의 동작 방법의 동작 흐름도이다. 도 6은 전자 장치(예: 도 3의 전자 장치(300))와 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400)) 간 공유 키를 생성하고, 생성된 공유 키를 공유하는 구체적인 동작에 대해서 서술하고 있다.

[267] 도 6을 참조하면, 동작 610에서, 전자 장치(300)는 공유 키를 보안 모듈(예: 도 3의 보안 모듈(330))에서 생성할 수 있다. 공유 키를 생성하는 동작은 보안 모듈(330)에 설치된 운송 수단 키 애플릿(예: 도 3의 키 매니징 애플릿(331))에 의해 수행될 수 있다. 키 매니징 애플릿(331)이 생성한 공유 키는, 제 1 외부 전자 장치(400)로 전송하기 위해, 보안 모듈(330)에 설치된 키 쉐어링 애플릿(예: 도 3의 키 쉐어링 애플릿(333))에 전송될 수 있다. 공유 키를 생성하는 구체적인 동작은 도 7에서 후술한다.

[268] 동작 620에서, 제 1 외부 전자 장치(400)는 공유 키를 수신하기 위한 키 쉐어링 애플릿(예: 도 4의 키 쉐어링 애플릿(431))을 보안 모듈(예: 도 4의 보안 모듈(430))에 설치할 수 있다. 키 쉐어링 애플릿(431)을 설치하는 구체적인 동작은 도 9에서 서술한다.

[269] 동작 630에서, 전자 장치(300)와 제 1 외부 전자 장치(400)는 동작 610에서 생성한 공유 키를 송/수신할 수 있다. 공유 키의 공유 프로세스는 전자

장치(300)의 보안 모듈(330)에 설치된 키 쉐어링 애플릿(333)과 제 1 외부 전자 장치(400)의 보안 모듈(430)에 설치된 키 쉐어링 애플릿(431) 사이에서 수행될 수 있다. 공유 키를 송/수신하는 구체적인 동작에 대해서는 도 10 내지 도 13에서 후술한다.

[270]

[271] 도 7은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 제 2 외부 전자 장치의 인증에 이용되는 공유 키를 생성하는 방법을 도시한 동작 흐름도이다.

[272] 도 7은 도 6의 공유키 생성 동작(동작 610)에 대한 구체적인 내용을 도시하고 있다.

[273] 도 7을 참조하면, 동작 710에서, 전자 장치(예: 도 3의 전자 장치(300))의 프로세서(310)는 사용자 입력에 대응하여 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401) 키 관리 어플리케이션을 실행할 수 있다. 제 2 외부 전자 장치(1401) 키 관리 어플리케이션은 메모리(예: 도 3의 메모리(340)) 상에 설치된 어플리케이션으로, 보안 모듈(예: 도 3의 보안 모듈(330))에 저장된 운송 수단 키 관리 애플릿에 대한 제어를 수행할 수 있다.

[274] 본 발명의 다양한 실시예에 따르면, 프로세서(310)는 운송 수단과 전자 장치(300)의 인증에 이용되는 인증 키를 제 1 외부 전자 장치(400)로 전송할 것을 요청하는 신호를 수신할 수 있다. 예를 들면, 전자 장치(300)의 사용자가 운송 수단의 키 관리 어플리케이션의 사용자 인터페이스를 이용하여 제 1 외부 전자 장치(400)로 인증 키를 전송할 것을 요청할 수 있다.

[275] 동작 720에서, 프로세서(310)는 공유 키의 생성을 위한 정보를 포함하는 사용자 입력을 수신할 수 있다. 본 발명의 다양한 실시예에 다르면, 프로세서(310)는 제 2 외부 전자 장치 키 관리 어플리케이션이 제공하는 사용자 인터페이스를 이용하여, 공유 키의 생성을 위한 정보를 입력하는 사용자 입력을 수신할 수 있다.

[276] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성을 위한 정보는 제 1 외부 전자 장치(400)의 사용자의 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화할 기능에 대한 정보를 포함할 수 있다. 제 2 외부 전자 장치(1401)가 제공 가능한 기능들은 제 2 외부 전자 장치(1401)가의 이용 허용 시간(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 운행이 가능한 시간), 제 2 외부 전자 장치(1401)의 이용 가능한 지역 범위 정보(geofencing limitation data, 예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 운행이 허용되는 지역적인 범위), 제 2 외부 전자 장치(1401)의 성능 제약(예를 들면, 2 외부 전자 장치(1401)가 운송 수단인 경우, 운송 수단의 최대 허용 속도), 제 2 외부 전자 장치(1401)에 포함된 다양한 장치(예를 들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 트렁크, 또는 콘솔 박스) 또는 제 2 외부 전자 장치(1401)가 수행 가능한 다양한 기능(예를

들면, 제 2 외부 전자 장치(1401)가 운송 수단인 경우, 차선 유지 보조, 차선 이탈 알림, 크루즈 컨트롤, 어댑티브 크루즈 컨트롤, 또는 엔진 사용 가능 여)의 허용 여부를 지시하는 정보 중 적어도 일부를 포함할 수 있다. 공유 키의 생성을 위한 정보는 전자 장치(300)의 사용자가 제 2 외부 전자 장치(1401)의 키 관리 어플리케이션의 사용자 인터페이스를 이용한 사용자 입력(제 1 외부 전자 장치(400)의 사용자 이름, 제 2 외부 전자 장치(1401)가 제공 가능한 기능들 중 활성화된 기능을 선택하는 사용자 입력)에 의해 생성될 수 있다.

[277] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성을 위한 정보는 생성된 공유키를 암호화하여 제 1 외부 전자 장치(400)로 전송하기 위해 요구되는 데이터를 포함할 수 있다. 예를 들면, 공유 키의 생성을 위한 정보는 생성된 공유키를 대칭 암호화 방식 또는 비대칭 암호화 방식을 이용하여 암호화를 수행하는데 필요한 암호 키를 포함할 수 있다.

[278] 본 발명의 다양한 실시예에 따르면, 동작 720 이후, 동작 730을 수행하기 위한 전자 장치(300)의 인증 동작이 추가될 수 있다. 사용자 인증이 성공한 경우, 프로세서(310)는 공유 키 생성을 위한 정보 및 공유 키 생성 명령을 보안 모듈(330)에 전송할 수 있다. 사용자 인증 방식은 다양한 방식(예를 들면, 핀 번호 입력하는 방식, 사용자의 생체 정보(예를 들면, 지문 입력, 홍채 인식, 또는 얼굴 인식)를 입력하는 방식을 포함할 수 있다)이 이용될 수 있다.

[279] 동작 730에서, 프로세서(310)는 공유 키 생성을 위한 정보 및 공유 키 생성 명령어를 보안 모듈(330)에 전송할 수 있다.

[280] 본 발명의 다양한 실시예에 따르면, 공유 키의 생성은 보안 모듈(330)에 설치된 키 매니징 애플릿(key managing applet, 331)에 의해 구현될 수 있다. 키 매니징 애플릿(331)은 공유 키의 생성을 위한 정보를 이용하여 공유 키를 생성할 수 있다.

[281] 동작 740에서, 키 매니징 애플릿(331)은 공유 키 생성을 위한 정보에 기반하여 공유 키 및 공유 키와 관련된 정보를 생성할 수 있다.

[282] 본 발명의 다양한 실시예에 따르면, 공유 키는 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)의 다양한 기능을 활성화하기 위해서, 제 2 외부 전자 장치(1401)와 인증을 수행하기 위해 요구되는 키를 의미할 수 있다.

[283] 본 발명의 다양한 실시예에 따르면, 공유 키와 관련된 정보는 공유 키가 전자 장치(300)에 저장된 인증 키에 기반하여 생성되었음을 지시하는 정보를 포함할 수 있다. 제 2 외부 전자 장치(1401)는 공유 키와 관련된 정보를 제 1 외부 전자 장치(400)로부터 수신하고, 전자 장치(300)에 저장된 인증 키에 기반하여 생성되었음을 지시하는 정보에 기반하여 유효한 공유 키인지 검증할 수 있다.

[284]

[285] 도 8은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 키 매니징 애플릿(331)에서 생성한 공유 키를 보안 모듈(330)의 키 쉐어링 애플릿(333)에 저장하는 방법을 도시한 동작 흐름도이다.

[286] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)의 키 매니징 애플릿(331)이 SE2SE(보안 모듈에서 다른 보안 모듈로 데이터를 전송하는 통신 규격)을 지원하는 경우, 키 쉐어링 애플릿(333)을 이용하지 않고, 키 매니징 애플릿(331)이 제 1 외부 전자 장치(400)의 키 쉐어링 애플릿(431)로 바로 공유 키 및 공유 키와 관련된 정보를 전송할 수 있다. 이 경우, 도 8에 도시된 동작은 생략될 수 있다.

[287] 동작 810에서, 전자 장치(300)의 제 2 외부 전자 장치(1401)의 키 관리 어플리케이션은 공유 키 생성이 성공했음을 알리는 신호를 키 매니징 애플릿(331)으로부터 수신함에 대응하여, 공유 키 생성 동작이 성공했음을 알리는 신호를 전자 장치(300)의 키 쉐어링 어플리케이션에 전송할 수 있다. 예를 들어, 키 쉐어링 어플리케이션은 전자 장치(300)의 메모리(예: 도 3의 메모리(340))에 설치되며, 보안 모듈(330) 상에 설치된 키 쉐어링 애플릿(333)의 동작을 관리하는 어플리케이션을 의미할 수 있다.

[288] 동작 820에서, 키 쉐어링 어플리케이션은 공유 키를 수신할 것을 지시하는 명령을 보안 모듈(330)에 설치된 키 쉐어링 애플릿(333)에 전송할 수 있다.

[289] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 어플리케이션은 공유 키에 대응하는 AID에 매칭되는 키 쉐어링 애플릿(333)에 공유 키를 수신할 것을 지시하는 명령을 전송할 수 있다.

[290] 동작 830에서, 키 쉐어링 애플릿(333)은 키 쉐어링 어플리케이션이 전송한 공유 키를 수신할 것을 지시하는 명령을 수신함에 대응하여, 키 매니징 애플릿(331)이 전송한 공유 키 및 공유 키 관련 정보를 수신할 수 있다. 일 실시예에 따르면, 키 쉐어링 애플릿(333)은 키 매니징 애플릿(331)에 공유 키 및 공유 키 관련 정보를 요청할 수 있다. 예를 들어, 키 매니징 애플릿(331)은 키 쉐어링 애플릿(333)이 전송한 공유 키 및 공유 키 관련 정보의 요청을 수신함에 대응하여, 키 쉐어링 애플릿(333)으로, 공유 키 및 공유 키 관련 정보를 전송할 수 있다.

[291] 동작 840에서, 키 쉐어링 애플릿(333)은 공유 키 및 공유 키 관련 정보의 수신이 성공했음을 알리는 정보를 키 쉐어링 어플리케이션에 전송할 수 있다.

[292]

[293] 도 9는 본 발명의 다양한 실시예에 따른 제 1 외부 전자 장치((400)에서 공유 키를 수신하기 위한 애플릿을 설치하는 방법(동작 620)을 도시한 동작 흐름도이다.

[294] 도 9를 참조하면, 동작 910에서, 프로세서(예: 도 4의 프로세서(410))는 키 쉐어링 어플리케이션을 실행할 수 있다. 키 쉐어링 어플리케이션은 제 1 외부 전자 장치(400)의 메모리(예: 도 1의 메모리(440)) 상에 설치될 수 있으며, 전자 장치(예: 도 3의 전자 장치(300))로부터 공유 키 및 공유 키와 관련된 정보를 수신하기 위한 키 쉐어링 애플릿(예: 도 4의 키 쉐어링 애플릿(431))을 설치하기 위한 어플리케이션을 의미할 수 있다. 예를 들어, 키 쉐어링 어플리케이션은 설치된 공유 키의 우선 순위에 대한 상태, 활성화 여부에 대한 상태, 운송 수단의

이용 가능한 기능에 대한 정보를 제공 및 변경할 수 있다.

[295] 동작 920에서, 프로세서(410)는 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))와 관련된 정보에 대한 사용자 입력을 수신할 수 있다. 제 2 외부 전자 장치(1401)와 관련된 정보는 제 1 외부 전자 장치(400)의 사용자가 키 쉐어링 어플리케이션의 인터페이스를 이용하여 입력한 정보를 의미할 수 있다. 제 2 외부 전자 장치(1401)와 관련된 정보는 제 2 외부 전자 장치(1401)의 제조사 이름(예를 들면, BMX), 제 2 외부 전자 장치(1401)의 모델 이름(예를 들면, X5)을 포함할 수 있다.

[296] 본 발명의 다양한 실시예에 따르면, 프로세서(410)는 제 1 외부 전자 장치(400)의 사용자가 키 쉐어링 어플리케이션의 인터페이스를 이용하여 입력하는 공유 키의 종류와 관련된 정보를 수신할 수 있다. 공유 키의 종류와 관련된 정보는 전자 장치(300)에 저장된 제 2 외부 전자 장치(1401)의 키와 동일한 공유 키 또는 복수의 이용자가 이용하는 쉐어링 카를 위한 일반적인 공유 키 중 어느 하나를 지정하는 정보를 의미할 수 있다.

[297] 동작 930에서, 프로세서(410)는 수신한 제 2 외부 전자 장치(1401)와 관련된 정보 또는 공유 키의 종류와 관련된 정보 및 키 쉐어링 애플릿(431)을 설치하는 명령을 보안 모듈(430)에 전송할 수 있다.

[298] 본 발명의 다양한 실시예에 따르면, 동작 930 이후, 동작 940을 수행하기 위한 제 1 외부 전자 장치(400)의 인증 동작이 추가될 수 있다. 사용자 인증이 성공한 경우, 프로세서(410)는 키 쉐어링 애플릿(431)을 설치하는 명령을 보안 모듈(430)에 전송할 수 있다. 사용자 인증 방식은 다양한 방식(예를 들면, 핀 번호 입력하는 방식, 사용자의 생체 정보(예를 들면, 지문 입력, 홍채 인식, 또는 얼굴 인식)를 입력하는 방식을 포함할 수 있다)이 이용될 수 있다.

[299] 동작 940에서, 보안 모듈(430)은 제 2 외부 전자 장치(1401)와 관련된 정보에 포함된 제 2 외부 전자 장치(1401)와의 제조사의 식별자(AID)에 대응하는 키 쉐어링 애플릿(431)을 설치할 수 있다.

[300] 본 발명의 다양한 실시예에 다르면, 생성된 키 쉐어링 애플릿(431)은 사용자 정보, 제 2 외부 전자 장치(1401)의 정보, 제 2 외부 전자 장치(1401)와 제 1 외부 전자 장치(400)간 송수신되는 암호화에 이용되는 복수의 암호 키에 대한 정보를 포함할 수 있다. 키 쉐어링 애플릿(431)은 수신한 공유 키의 상태를 지시하는 정보를 포함할 수 있으며, 수신한 공유 키의 상태는 표 1에 정의되어 있다.

[301] 본 발명의 다양한 실시예에 따르면, 키 쉐어링 애플릿(431)은 운송 수단의 제조사의 식별자에 대응하는 공유 키를 수신하기 위해, 제조사의 식별자를 전자 장치(300)의 키 쉐어링 애플릿(333)에 전송할 수 있다. 전자 장치(300) 상에 저장된 공유 키가 제조사의 식별자와 대응하지 않는 경우, 공유 키의 송/수신 동작이 종료될 수 있다.

[302]

[303] 도 10은 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작

방법에서, 공유 키를 송/수신하는 구체적인 방법을 도시한 동작 흐름도이다.

[304] 도 10을 참조하면, 동작 1001에서, 전자 장치(예: 도 3의 전자 장치(300))는 공유 키를 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400))로 전송하기 위한 공유 키 전송 모드로 진입할 수 있다. 공유 키를 근거리 통신(예: NFC)를 이용하여 송/수신하는 경우, 전자 장치(300)는 NFC 리더 모드로 동작할 수 있다. 공유 키 전송 모드는 전자 장치(300)의 통신 모듈(320)을 NFC 리더 모드로 전환하는 구체적인 동작을 포함할 수 있다. 전자 장치(300)는 공유 키 전송 모드로 진입하고, 제 1 외부 전자 장치(400)에 AID 리스트를 전송할 것을 요청하는 신호를 전송할 수 있다. 공유 키 전송 모드로 진입하는 구체적인 내용에 대해서는 도 11에서 후술한다.

[305] 동작 1003에서, 제 1 외부 전자 장치(400)는 전자 장치(300)가 전송하는 공유 키를 수신하기 위한 공유 키 수신 모드로 진입할 수 있다. 공유 키를 근거리 통신(예: NFC)를 이용하여 송/수신하는 경우, 제 1 외부 전자 장치(400)는 NFC 카드 모드로 동작하면서, 공유 키를 수신할 수 있다.

[306] 동작 1005에서, 전자 장치(300)와 제 1 외부 전자 장치(400)는 SE2SE(secure module to secure module) 리더/카드 에뮬레이션 모드를 이용해서 공유 키를 공유할 수 있다. 전자 장치(300)는 NFC 리더(reader) 모드로 동작할 수 있으며, 제 1 외부 전자 장치(400)는 NFC 카드(card) 모드로 동작할 수 있다. 동작 1005에 대한 구체적인 내용에 대해서는 도 12에서 후술한다.

[307] 동작 1007에서, 공유 키 전송을 완료한 전자 장치(300)는 공유 키 전송 모드에서 일반 모드로 진입할 수 있다. 일반 모드는 통신 채널을 수립하기 위해서 다른 외부 전자 장치가 전송하는 신호를 수신할 수 있도록 하는 listening mode 및 다른 외부 전자 장치가 전자 장치(300)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 모두 지원하는 모드를 의미할 수 있다. 동작 1007에 대한 구체적인 내용에 대해서는 도 13에서 후술한다.

[308] 동작 1009에서, 공유 키 수신을 완료한 제 1 외부 전자 장치(400)는 공유 키 수신 모드에서 일반 모드로 진입할 수 있다. 일반 모드는 통신 채널을 수립하기 위해서 다른 외부 전자 장치가 전송하는 신호를 수신할 수 있도록 하는 listening mode 및 다른 외부 전자 장치가 제 1 외부 전자 장치(400)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 모두 지원하는 모드를 의미할 수 있다.

[309] 동작 1011에서, 전자 장치(300)는 공유 키의 공유 결과(실패 또는 성공)를 지시하는 알림을 수신하고, 공유 키의 공유 결과를 제 2 외부 전자 장치 키 관리 어플리케이션의 이력 정보에 업데이트할 수 있다.

[310] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)는 공유 키의 공유 결과를 전자 장치(300)의 사용자가 인지할 수 있도록 정보를 제공할 수 있다. 예를 들어, 제1 전자 장치(300)의 표시 장치(예: 도 1의 표시 장치(160)) 또는 음향 출력 장치(예: 도 1의 음향 출력 장치(155))를 통해 사용자에게 정보를 제공할 수 있다.

[311] 동작 1013에서, 제 1 외부 전자 장치(400)는 공유 키의 공유 결과(실패 또는

성공)를 지시하는 알림을 수신하고, 공유 결과를 제 1 외부 전자 장치(400)의 사용자가 인지할 수 있도록 출력할 수 있다. 예를 들어, 제 1 외부 전자 장치(400)의 표시 장치(예: 도 1의 표시 장치(160)) 또는 음향 출력 장치(예: 도 1의 음향 출력 장치(155))를 통해 사용자에게 정보를 제공할 수 있다.

[312] 본 발명의 다양한 실시예에 따르면, 공유 키의 수신을 성공한 제 1 외부 전자 장치(400)에 저장된 공유 키는 아직 비활성화 상태일 수 있다. 예를 들어, 공유 키는 제 2 외부 전자 장치(1401)와의 통신 연결시 제 2 외부 전자 장치(1401)의 공유 키에 대한 검증 후, 활성화될 수 있다.

[313]

[314] 도 11은 공유 키를 전송하는 전자 장치가 공유 키를 전송하는 전송 모드를 도시한 도면이다. 도 11에 도시된 실시예는, 도 10에 도시된 실시예 중, 공유 키를 전송하는 모드로 진입하는 실시예(동작 1001)에 대한 설명이다.도 11을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))는 제 2 외부 전자 장치의 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107)(예: 도 3의 보안 모듈(330))을 포함할 수 있다. 도 11에 도시된 실시예는 전자 장치(예: 도 3의 전자 장치(300)제 2 외부 전자 장치 키 관리 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107) 의 동작 주체들 간에 수행될 수 있다.

[315] 본 발명의 다양한 실시예에 따르면, NFC 서비스(1103)는 통신 모듈(예: 도 3의 통신 모듈(320))에 포함된 제어 회로를 의미할 수 있다. CLF(1105)는 NFC 통신을 수행하는 안테나를 포함하는 프론트 엔드 회로를 의미할 수 있다.

[316] 동작 1109에서, 제 2 외부 전자 장치의 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션(1101)은 NFC 서비스(1103)를 지정된 NFC 리더 모드로 설정(SET dedicated reader mode)하도록 제어할 수 있다. NFC 서비스(1103)는 제 2 외부 전자 장치의 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션(1101)에서 전송한 신호를 수신함에 대응하여, NFC 리더 모드로 동작하도록 CLF(1105)를 제어할 수 있다.

[317] 동작 1111에서, NFC 서비스(1103)는 CLF(1105)를 비활성화하는 명령(RF_DEACTIVATE_CMD)을 CLF(1105)로 전송할 수 있다.

[318] 본 발명의 다양한 실시예에 따르면, CLF(1105)는 기존에 수행하는 모드를 비활성화 후, NFC 리더 모드로 동작할 수 있다. 동작 1113에서, CLF(1105)는 비활성화 명령의 응답 신호(RF_DEACTIVATE_RSP)를 NFC 서비스(1103)에 전송할 수 있다.

[319] 동작 1115에서, NFC 서비스(1103)는 호스트(보안 모듈)를 선택하는 신호(SELECT_HOST_CMD)를 CLF(1105)로 전송할 수 있다. 예를 들어, 호스트는 수신한 데이터를 수신하는 구성 요소 또는 송신하는 데이터가 존재하는 구성 요소를 의미할 수 있다. 본 실시예에서는, 공유 키는 보안 모듈(1107)에 존재하기

때문에, 호스트는 보안 모듈(1107)에 해당될 수 있다. 동작 1117에서, CLF(1105)는 동작 1115에서 전송한 호스트 선택 신호의 응답 신호(SELECT_HOST_RSP)를 NFC 서비스(1103)에 전송할 수 있다.

[320] 동작 1119에서, NFC 서비스(1103)는 리더 모드를 활성화 하는 명령(READER_MODE_CMD)을 CLF(1105)로 전송할 수 있다. 동작 1121에서, CLF(1105)는 리더 모드를 활성화 하는 명령의 응답 신호(READER_MODE_RSP)를 NFC 서비스(1103)에 전송할 수 있다. 동작 1123에서, NFC 서비스(1103)은 결과를 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)에 전송할 수 있다.

[321] 동작 1125에서, 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)은 AID를 선택하는 명령(SELECT AID APDU CMD)을 보안 모듈(1107)에 전송할 수 있다. 동작 1127에서, 보안 모듈(1107)은 AID 선택하는 명령의 응답 신호(SELECT AID APDU RSP)를 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)에 전송할 수 있다.

[322] 동작 1129에서, 제 2 외부 전자 장치 키 관리 어플리케이션 또는 키 쉐어링 어플리케이션 (1101)은 리더 게이트를 활성화 하는 명령(ENABLE READER GATE CMD)을 보안 모듈(1107)에 전송할 수 있다. 리더 게이트를 활성화 하는 명령은 보안 모듈(1107)이 공유 키 및 공유 키 관련 데이터를 전송하는 준비 동작을 수행하는 것을 의미한다. 동작 1131에서, 보안 모듈(1107)은 리더 게이트를 활성화 하는 명령의 응답 신호(ENABLE READER GATE RSP)를 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 전송할 수 있다.

[323] 동작 1133에서, 보안 모듈(1107)은 리더 모드로 동작할 것을 요청(EVT_READER_REQUESTED)하는 신호를 CLF(1105)로 전송할 수 있다. 동작 1135에서, CLF(1105)는 보안 모듈(1107)이 전송한 리더 모드로 동작할 것을 요청(READER_MODE_NTF)하는 신호를 NFC 서비스(1103)로 전송할 수 있다.

[324] 동작 1137에서, NFC 서비스(1103)은 리더 모드로 동작하는 명령(READER_MODE_CMD)을 CLF(1105)로 전송할 수 있다. 동작 1139에서, CLF(1105)는 리더 모드로 동작하는 명령의 응답 신호(READER_MODE_RSP)를 NFC 서비스(1103)으로 전송하고, 동작 1141에서, CLF(1105)는 공유 키 전송 모드로 진입할 수 있다. 공유 키 전송 모드는 제 1 외부 전자 장치(400)가 전자 장치(300)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 지원하는 모드를 의미할 수 있다.

[325]

[326] 도 12는 본 발명의 다양한 실시예에 따른 전자 장치 및 전자 장치의 동작 방법에서, 공유 키를 송/수신하는 동작을 도시한 흐름도이다. 도 12에 도시된 실시예는, 도 10에 도시된 실시예 중, 공유 키를 공유하는 동작(동작 1005)에 대한 실시예에 관한 것이다.

[327] 도 12에 도시된 실시예는, 전자 장치(예: 도 3의 전자 장치(300)) 및 제 1 외부

전자 장치(예: 도 4의 전자 장치(400))간 공유 키 및 공유 키와 관련된 정보를 송/수신하는 동작(예: 도 10의 1005)의 실시예이다.

[328] 도 12를 참조하면, 일 실시예에 따르면, 공유 키 및 공유 키와 관련된 정보를 전송하는 전자 장치(300)는 리더 모드로 동작하고, 공유 키 및 공유 키와 관련된 정보를 수신하는 제 1 외부 전자 장치(400)는 카드 모드로 동작할 수 있다.

[329] 전자 장치(300) 및 제 1 외부 전자 장치(400)가 송 수신하는 데이터는 1 개의 APDU(application protocol data unit)으로 정의된 데이터 규격을 따를 수 있다. 전자 장치(300)가 제 1 외부 전자 장치(400)로 명령을 전송하면서, 전송되는 데이터는 C-APDU(command- application protocol data unit)으로 정의되며, 제 1 외부 전자 장치(400)가 전자 장치(300)에 응답하면서, 전송되는 데이터는 R-APDU(response - application protocol data unit)으로 정의될 수 있다. 본 발명의 다양한 실시예에 따르면, 전자 장치(300) 및 제 1 외부 전자 장치(400)는 C-APDU, R-APDU 포맷으로 정의된 데이터 규격을 이용하여 아래에 기재된 동작을 수행할 수 있다.

[330] 먼저, 전자 장치(300)의 보안 모듈(330)은 통신 모듈(320)을 이용하여 AID 리스트를 전송할 것을 제 1 외부 전자 장치(400)에 요청할 수 있다. 제 1 외부 전자 장치(400)의 보안 모듈(430)은 통신 모듈(420)을 통해 AID 리스트를 전자 장치(300)로 전송할 수 있다.

[331] 전자 장치(300)의 보안 모듈(330)은 수신한 AID 리스트에서 전송될 공유키에 대응하는 AID를 선택하고, 선택된 AID를 지시하는 정보와 선택된 AID에 대응하는 키 쉐어링 애플릿과 관련된 정보를 전송할 것을 제 1 외부 전자 장치(400)에게 요청할 수 있다. 제 1 외부 전자 장치(400)의 보안 모듈(430)은 키 쉐어링 애플릿과 관련된 정보(예를 들면, 키 쉐어링 애플릿의 버전 정보, 사용자 정보)를 통신 모듈(420)을 통해 전자 장치(300)로 전송할 수 있다.

[332] 전자 장치(300)의 보안 모듈(330)은 키 쉐어링 애플릿과 관련된 정보를 확인하고, 키 쉐어링 애플릿의 상태(표 1에 정의된 상태)를 확인할 수 있다.

[333] 전자 장치(300)의 보안 모듈(330)과 제 1 외부 전자 장치(400)의 보안 모듈(430)은 암호 키를 이용하여 상호 인증을 수행하고, 상호 인증이 완료된 경우, 보안 모듈(330)은 제 1 외부 전자 장치(400)의 보안 모듈(430)로 통신 모듈(320)을 이용하여 생성된 공유 키 및 공유 키와 관련된 정보를 전송할 수 있다.

[334] 제 1 외부 전자 장치(400)의 보안 모듈(430)은 공유 키 및 공유 키와 관련된 정보를 전자 장치(300)로부터 수신하고, 공유 키와 관련된 정보에 포함된 공유 키 상태를 비활성화로 변경할 수 있다.

[335] 본 발명의 다양한 실시예에 따르면, 상기에 기재된 전자 장치(300)와 제 1 외부 전자 장치(400) 사이의 데이터 교환은 동작 1201, 1203, 1205, 1207에 도시된 C-APDU, R-APDU의 데이터 규격을 통해 송/수신될 수 있다.

[336]

[337] 도 13은 공유 키를 전송하는 전자 장치가 공유 키를 전송하는 전송 모드에서 일반 모드로 전환되는 실시예를 도시한 도면이다.

[338] 도 13을 참조하면, 전자 장치(예: 도 3의 전자 장치(300))가 공유 키 및 공유 키와 관련된 정보를 제 1 외부 전자 장치(예: 도 4의 전자 장치(400))에 전송한 후, 일반 모드로 전환하는 실시예를 도시하고 있다. 도 13에 도시된 실시예는 도 10에 도시된 실시예 중, 공유 키를 공유하는 동작이 완료된 후, 공유 키 전송 모드에서 일반 모드로 전환하는 동작(동작 1007)의 실시예와 관련된 것이다.

[339] 도 13을 참조하면, 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))는 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))의 키 관리 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107)(예: 도 3의 보안 모듈(330))을 포함할 수 있다. 도 13에 도시된 실시예는 제 2 외부 전자 장치 키 관리 어플리케이션(1101), NFC 서비스(1103), 비 접촉 프론트엔드(contactless front-end, CLF, 1105) 및 보안 모듈(1107)의 동작 주체들 간에 수행될 수 있다.

[340] 본 발명의 다양한 실시예에 따르면, NFC 서비스(1103)는 통신 모듈(예: 도 3의 통신 모듈(320))에 포함된 제어 회로를 의미할 수 있다. CLF(1105)는 NFC 통신을 수행하는 안테나를 포함하는 프론트 엔드 회로를 의미할 수 있다.

[341] 동작 1301에서, 보안 모듈(1107)은 공유 키의 공유가 완료되었음을 알리는 신호(EVT_TRANSACION)를 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 전송할 수 있다.

[342] 동작 1303에서, 제 2 외부 전자 장치 키 관리 어플리케이션(1101)은 리더 게이트를 비활성화 하는 명령(DISABLE READER GATE CMD)를 보안 모듈(1107)에 전송하고, 보안 모듈(1107)은 동작 1305에서, 리더 게이트를 비활성화 하는 명령의 응답 신호(DISABLE READER GATE RSP)를 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 전송할 수 있다.

[343] 동작 1307에서, 보안 모듈(1107)은, 리더 모드를 종료하는 신호(EVT_END_OPERATION)를 CLF(1105)에 전송할 수 있다. 동작 1309에서, CLF(1105)는 리더 모드가 종료되었음을 알리는 신호(READER_MODE_NTF)를 NFC 서비스(1103)에 전송할 수 있다.

[344] 동작 1311에서, 제 2 외부 전자 장치 키 관리 어플리케이션(1101)은 지정된 리더 모드를 비활성화 하는 신호(disable dedicated reader mode)를 NFC 서비스(1103)에 전송할 수 있다.

[345] 동작 1313에서, NFC 서비스(1103)는 리더 모드를 종료하는 명령(READER_MODE_CMD)을 CLF(1105)에 전송하고, CLF(1105)는 리더 모드를 종료할 수 있다. 동작 1315에서, CLF(1105)는 리더 모드가 종료되었음을 알리는 응답 메시지(READER_MODE_RSP)를 NFC 서비스(1103)에 전송할 수 있다.

[346] 동작 1317에서, NFC 서비스(1103)는 일반 모드로 동작할 것을 명령하는

신호(RF_DISCOVERY_CMD)를 CLF(1105)에 전송할 수 있다. 동작 1319에서, CLF(1105)는 일반 모드로의 동작을 수행할 수 있다. 예를 들어, RF 디스커버리 프로세스를 수행할 수 있다. 동작 1321에서, CLF(1105)는 일반 모드로의 동작을 알리는 응답 메시지(RF_DISCOVERY_RSP)를 NFC 서비스에 전송할 수 있다.

[347] 동작 1323에서, NFC 서비스(1103)는 제 2 외부 전자 장치 키 관리 어플리케이션(1101)에 일반 모드로의 동작을 알리는 메시지를 전송할 수 있다.

[348] 본 발명의 다양한 실시예에 따르면, 일반 모드는 통신 채널을 수립하기 위해서 다른 외부 전자 장치가 전송하는 신호를 수신할 수 있도록 하는 listening mode 및 다른 외부 전자 장치가 제 1 외부 전자 장치(400)의 존재를 알 수 있도록 신호를 방송하는 polling mode를 모두 지원하는 모드를 의미할 수 있다.

[349] 본 발명의 다양한 실시예에 따르면, 도 11 및 도 13에 개시된 실시예들은 순차적으로 동작하는 것처럼 도시하였으나, 반드시 순차적으로 동작하지 않고, 각 동작이 동시에 동작할 수 있으며(예를 들면, 동작 1303과 동작 1311은 동시에 구현될 수도 있다), 일부 동작은 다른 동작보다 더 먼저 동작할 수도 있다.

[350] 본 발명의 다양한 실시예에 따르면, 도 11 및 도 13에 개시된 실시예들은, 전자 장치(300)에서 수행되는 실시예들이지만, 제 1 외부 전자 장치(400)의 모드 변경 역시, 도 11 및 도 13에 개시된 동작을 이용하여 구현될 수 있다.

[351]

[352] 도 14는 제 2 외부 전자 장치(1401)가 제 1 외부 전자 장치(400)가 전송한 공유 키의 유효성을 검증하는 실시예를 도시한 도면이다.

[353] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(예: 도 4의 전자 장치(400))는 전자 장치(예: 도 3의 전자 장치(300))로부터 공유 키 및 공유 키와 관련된 정보를 수신할 수 있다. 공유 키와 관련된 정보에는 공유 키의 상태를 지시하는 정보가 포함될 수 있다. 공유 키의 상태는 공유 키를 수신하지 못한 상태(예: 표 1의 index 1), 공유 키를 수신했으나, 아직 제 2 외부 전자 장치(1401)가 권한을 허용하지 않은 상태(예: 표 1의 index 2), 공유 키를 수신했고, 제 2 외부 전자 장치(1401)가 권한을 허용한 상태(예: 표 1의 index 3), 공유 키가 유효하지 않은 상태(예: 표 1의 index 4)로 구성될 수 있다.

[354] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)가 공유 키를 수신한 경우, 공유 키의 상태는 공유 키를 수신했고, 제 2 외부 전자 장치(1401)가 권한을 허용 하지 않은 상태(index 2)에 해당될 수 있다. 공유 키는 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)와 공유 키 수신 후 첫 연결시 수행되는 제 2 외부 전자 장치(1401)의 검증 결과에 따라서 제 2 외부 전자 장치가 권한을 허용한 상태(index 3)로 변경될 수 있다. 이하, 제 2 외부 전자 장치가 제 1 외부 전자 장치(400)가 수신한 공유 키를 검증하는 실시예에 대해서 서술한다.

[355] 동작 1411에서, 제 1 외부 전자 장치(400)와 제 2 외부 전자 장치(1401)는 통신 채널을 설립할 수 있다.

[356] 본 발명의 다양한 실시예에 따르면, 제 1 외부 전자 장치(400)와 제 2 외부 전자

장치(1401)는 근거리 통신 방식을 이용하여 통신 채널을 설립할 수 있다. 제 2 외부 전자 장치(1401)에 포함된 근거리 통신 모듈이 리더 모드로 동작하고, 제 1 외부 전자 장치(400)가 제 2 외부 전자 장치(1401)에 근접(또는, 태그)하는 경우, 제 1 외부 전자 장치(400)와 제 2 외부 전자 장치(1401) 사이의 통신 채널이 생성될 수 있다.

[357] 동작 1413에서, 제 1 외부 전자 장치(400)는 공유 키와 공유 키 관련 정보를 제 2 외부 전자 장치(1401)에 전송할 수 있다.

[358] 동작 1415에서, 제 2 외부 전자 장치(1401)는 제 1 외부 전자 장치(400)가 전송한 공유 키의 검증을 수행할 수 있다.

[359] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)에 저장된 인증 키가 마스터 키인 경우, 제 1 외부 전자 장치(400)는 마스터 키에 기반하여 생성된 공유 키를 전자 장치(300)로부터 수신할 수 있다. 이 경우, 제 2 외부 전자 장치(1401)는 공유 키가 마스터 키에 기반하여 생성되었는지 확인한 결과에 기반하여 공유 키의 유효성을 검증할 수 있다.

[360] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)에 저장된 인증 키가 마스터 키에 기반하여 생성된 1차 공유 키인 경우, 제 1 외부 전자 장치(400)는 1차 공유 키에 기반하여 생성된 토큰을 전자 장치(300)로부터 수신할 수 있다. 제 1 외부 전자 장치(400)는 전자 장치(300)로부터 수신한 토큰을 제 2 외부 전자 장치(1401)로 전송할 수 있다. 이 경우, 제 2 외부 전자 장치(1401)는 토큰이 1차 공유 키에 기반하여 생성되었는지 확인한 결과에 기반하여 토큰의 유효성을 검증할 수 있다.

[361] 동작 1417에서, 제 2 외부 전자 장치(1401)는 공유 키 또는 토큰의 검증 결과에 기반하여 공유 키 및 공유 키와 관련된 정보를 등록할 수 있다.

[362] 본 발명의 다양한 실시예에 따르면, 전자 장치(300)에 저장된 인증 키가 마스터 키인 경우, 제 1 외부 전자 장치(400)는 1차 공유 키 및 공유 키와 관련된 정보를 전자 장치(300)로부터 수신할 수 있다. 이 경우, 제 2 외부 전자 장치(1401)는 1차 공유 키를 확인한 결과에 기반하여 유효성을 검증하고, 유효한 공유 키 및 인 경우, 새로운 사용자의 1차 공유 키 및 공유 키와 관련된 정보를 등록할 수 있다.

[363] 동작 1419에서, 제 2 외부 전자 장치(1401)는 공유키의 검증 결과를 제 1 외부 전자 장치(400)에 전송할 수 있다.

[364] 동작 1421에서, 제 1 외부 전자 장치(400)는 공유 키와 관련된 정보를 업데이트할 수 있다. 본 발명의 다양한 실시예에 따르면, 공유 키에 관련된 정보에 포함된 공유 키의 상태를 변경할 수 있다. 상술하면, 공유 키와 관련된 정보에 포함된 공유 키의 상태는 공유 키를 수신했으나, 아직 제 2 외부 전자 장치(1401)가 권한을 허용하지 않은 상태(예: 표 1의 index 2)일 수 있다. 제 1 외부 전자 장치(400)는 제 2 외부 전자 장치(1401)의 검증 결과에 기반하여 공유 키의 상태를 공유 키를 수신하고, 제 2 외부 전자 장치(1401)가 권한을 허용한 상태(예: 표 1의 index 3)로 변경할 수 있다.

[365]

[366] 본 발명의 다양한 실시예에 따른 전자 장치(예: 도 3의 전자 장치(300))의 동작 방법은 제 2 외부 전자 장치(예: 도 14의 제 2 외부 전자 장치(1401))와의 인증에 이용되는 인증 키에 기반하여 생성되는 공유 키의 전송 요청을 제 1 외부 전자 장치(예: 도 4의 제 1 외부 전자 장치(400))로부터 수신하는 동작, 상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 보안 모듈(예: 도 3의 보안 모듈(330))에 전송하는 동작, 상기 정보 및 상기 명령에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈(330)을 제어하는 동작 및 상기 생성된 공유 키 및 상기 생성된 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치(400)로 전송하도록 상기 보안 모듈(300)을 제어하는 동작을 포함할 수 있다.

[367] 본 발명의 다양한 실시예에 따르면, 상기 공유 키와 관련된 정보는 상기 공유 키가 상기 인증 키에 기반하여 생성됨을 지시하는 정보를 포함할 수 있다.

[368] 본 발명의 다양한 실시예에 따르면, 상기 전자 장치(300)의 동작 방법은 상기 제 1 외부 전자 장치(400)의 보안 모듈(예: 도 4의 보안 모듈(430))에 설치된 상기 공유 키를 관리할 애플릿과 관련된 정보를 수신하는 동작 및 상기 수신한 애플릿과 관련된 정보에 기반하여 상기 공유 키를 상기 제 1 외부 전자 장치(400)에 전송할지 여부를 결정하는 동작을 더 포함할 수 있다.

[369] 본 발명의 다양한 실시예에 따르면, 상기 인증키는 마스터 키 또는 상기 마스터 키에 기반하여 생성된 키 중 하나이며, 상기 전자 장치의 동작 방법은 상기 인증키가 상기 마스터 키에 기반하여 생성된 키인 경우, 상기 공유 키가 상기 인증 키에 기반하여 생성되었음을 지시하는(indicating) 토큰을 생성하는 동작 및 상기 토큰 및 상기 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치(400)로 전송하는 동작을 더 포함할 수 있다.

[370]

[371] 본 문서에 개시된 다양한 실시예들에 따른 전자 장치는 다양한 형태의 장치가 될 수 있다. 전자 장치는, 예를 들면, 휴대용 통신 장치 (예: 스마트폰), 컴퓨터 장치, 휴대용 멀티미디어 장치, 휴대용 의료 기기, 카메라, 웨어러블 장치, 또는 가전 장치를 포함할 수 있다. 본 문서의 실시예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

[372] 본 문서의 다양한 실시예들 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시예들로 한정하려는 것이 아니며, 해당 실시예의 다양한 변경, 균등물, 또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 또는 관련된 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 아이템에 대응하는 명사의 단수 형은 관련된 문맥상 명백하게 다르게 지시하지 않는 한, 상기 아이템 한 개 또는 복수 개를 포함할 수 있다. 본 문서에서, "A 또는 B", "A 및 B 중 적어도 하나", “A 또는 B 중 적어도 하나,”"A, B 또는 C," "A, B 및 C 중 적어도 하나,”및 “A, B, 또는 C 중 적어도 하나"와 같은 문구들 각각은 그 문구들 중 해당하는 문구에 함께 나열된 항목들의 모든 가능한

조합을 포함할 수 있다. "제 1", "제 2", 또는 "첫째" 또는 "둘째"와 같은 용어들은 단순히 해당 구성요소를 다른 해당 구성요소와 구분하기 위해 사용될 수 있으며, 해당 구성요소들을 다른 측면(예: 중요성 또는 순서)에서 한정하지 않는다. 어떤(예: 제 1) 구성요소가 다른(예: 제 2) 구성요소에, "기능적으로" 또는 "통신적으로"라는 용어와 함께 또는 이런 용어 없이, "커플드" 또는 "커넥티드"라고 언급된 경우, 그것은 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로(예: 유선으로), 무선으로, 또는 제 3 구성요소를 통하여 연결될 수 있다는 것을 의미한다.

[373] 본 문서에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구현된 유닛을 포함할 수 있으며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로 등의 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는, 상기 부품의 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 일실시예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

[374] 본 문서의 다양한 실시예들은 기기(machine)(예: 전자 장치(101)) 의해 읽을 수 있는 저장 매체(storage medium)(예: 내장 메모리(136) 또는 외장 메모리(138))에 저장된 하나 이상의 명령어들을 포함하는 소프트웨어(예: 프로그램(140))로서 구현될 수 있다. 예를 들면, 기기(예: 전자 장치(101))의 프로세서(예: 프로세서(120))는, 저장 매체로부터 저장된 하나 이상의 명령어들 중 적어도 하나의 명령을 호출하고, 그것을 실행할 수 있다. 이것은 기기가 상기 호출된 적어도 하나의 명령어에 따라 적어도 하나의 기능을 수행하도록 운영되는 것을 가능하게 한다. 상기 하나 이상의 명령어들은 컴파일러에 의해 생성된 코드 또는 인터프리터에 의해 실행될 수 있는 코드를 포함할 수 있다. 기기로 읽을 수 있는 저장매체 는, 비일시적(non-transitory) 저장매체의 형태로 제공될 수 있다. 여기서, '비일시적'은 저장매체가 실재(tangible)하는 장치이고, 신호(signal)(예: 전자기파)를 포함하지 않는다는 것을 의미할 뿐이며, 이 용어는 데이터가 저장매체에 반영구적으로 저장되는 경우와 임시적으로 저장되는 경우를 구분하지 않는다.

[375] 일실시예에 따르면, 본 문서에 개시된 다양한 실시예들에 따른 방법은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only memory (CD-ROM))의 형태로 배포되거나, 또는 어플리케이션 스토어(예: 플레이 스토어TM)를 통해 또는 두개의 사용자 장치들(예: 스마트폰들) 간에 직접, 온라인으로 배포(예: 다운로드 또는 업로드)될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 기기로 읽을 수 있는 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다.

[376] 다양한 실시예들에 따르면, 상기 기술한 구성요소들의 각각의 구성요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있다. 다양한 실시예들에 따르면, 전술한 해당 구성요소들 중 하나 이상의 구성요소들 또는 동작들이 생략되거나, 또는 하나 이상의 다른 구성요소들 또는 동작들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성요소들(예: 모듈 또는 프로그램)은 하나의 구성요소로 통합될 수 있다. 이런 경우, 통합된 구성요소는 상기 복수의 구성요소들 각각의 구성요소의 하나 이상의 기능들을 상기 통합 이전에 상기 복수의 구성요소들 중 해당 구성요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 다양한 실시예들에 따르면, 모듈, 프로그램 또는 다른 구성요소에 의해 수행되는 동작들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 상기 동작들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 동작들이 추가될 수 있다.

청구범위

[청구항 1] 전자 장치에 있어서,
프로세서;
무선 통신을 지원하는 적어도 하나의 통신 모듈; 및
제 1 외부 전자 장치로 전송될 공유 키 및 제 2 외부 전자 장치와의 인증에 이용되는 인증 키의 저장 및 관리를 수행하는 애플릿이 설치된 보안 모듈을 포함하고,
상기 프로세서는
상기 인증 키의 제 1 외부 전자 장치로의 전송의 요청을 수신하고,
상기 공유 키의 생성을 위한 정보 및 상기 공유 키 생성 명령을 상기 보안 모듈에 전송하고,
상기 공유 키 생성을 위한 정보에 기반하여 상기 공유 키를 생성하도록 상기 보안 모듈을 제어하고,
상기 생성된 공유 키 및 생성된 공유 키와 관련된 정보를 제 1 외부 전자 장치로 전송하도록 상기 보안 모듈을 제어하도록 설정된 전자 장치.

[청구항 2] 제 1항에 있어서,
상기 공유 키와 관련된 정보는
상기 인증 키에 기반하여 생성됨을 지시하는 정보를 포함하는 전자 장치.

[청구항 3] 제 1항에 있어서,
상기 공유 키와 관련된 정보는
상기 제 2 외부 전자 장치가 제공 가능한 기능 중 적어도 일부의 기능을 활성화 할 것을 지시하는 정보를 포함하는 전자 장치.

[청구항 4] 제 1항에 있어서,
상기 입력된 공유 키 생성을 위한 정보는
상기 제 2 외부 전자 장치의 이용 허용 시간, 상기 제 2 외부 전자 장치의 이용 가능한 지역 범위 정보(geofencing limitation data)을 포함하는 전자 장치.

[청구항 5] 제 1항에 있어서,
상기 프로세서는
상기 공유 키의 암호화를 위한 암호 키를 상기 공유 키의 생성을 위한 정보와 함께 상기 보안 모듈로 전송하도록 설정된 전자 장치.

[청구항 6] 제 1항에 있어서,
상기 보안 모듈은
상기 제 1 외부 전자 장치의 보안 모듈에 설치된 상기 공유 키를 관리할 애플릿과 관련된 정보를 수신하고,
상기 수신한 애플릿과 관련된 정보에 기반하여 상기 공유 키를 상기 제 1 외부 전자 장치에 전송할지 여부를 결정하도록 설정된 전자 장치.

[청구항 7] 제 6항에 있어서,
상기 보안 모듈은
상기 애플릿과 관련된 정보에 포함된 애플릿 식별자가 상기 공유 키에 대응하는 식별자와 동일한지 확인하고,
상기 애플릿 식별자와 상기 공유 키에 대응하는 식별자가 동일한지 여부에 기반하여 상기 공유 키를 상기 제 1 외부 전자 장치에 전송할지 여부를 결정하도록 설정된 전자 장치.

[청구항 8] 제 6항에 있어서,
상기 애플릿과 관련된 정보는
상기 애플릿이 저장된 주소, 애플릿 식별자, 상기 외부 전자 장치의 모델 식별자, 상기 애플릿의 활성화 여부를 지시하는 데이터, 상기 애플릿 각각에 지정된 우선 순위, 또는 상기 애플릿의 구체적인 데이터(applet-specific data) 중 적어도 하나 이상을 포함하는 전자 장치.

[청구항 9] 제 1항에 있어서,
상기 인증 키는 마스터 키 또는 상기 마스터 키에 기반하여 생성된 키 중 하나이며,
상기 인증 키가 상기 마스터 키에 기반하여 생성된 키인 경우,
상기 보안 모듈은
상기 공유 키가 상기 인증 키에 기반하여 생성되었음을 지시하는(indicating) 토큰을 생성하고,
상기 토큰 및 상기 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치로 전송하도록 설정된 전자 장치.

[청구항 10] 제 1항에 있어서,
상기 전자 장치는
상기 통신 모듈을 이용하여 상기 공유 키 및 상기 공유 키와 관련된 정보를 상기 제 1 외부 전자 장치에 전송하도록 설정된 전자 장치.

[청구항 11] 제 1 외부 전자 장치로부터 공유 키를 수신하는 전자 장치에 있어서,
프로세서;
무선 통신을 지원하는 적어도 하나의 통신 모듈; 및
제 2 외부 전자 장치의 인증에 이용되는 인증 키를 관리하는 애플릿과 관련된 정보를 관리하고, 애플릿 식별자(applet identification, AID) 리스트 및 상기 애플릿을 저장하는 보안 모듈을 포함하고,
상기 보안 모듈은
상기 애플릿과 관련된 정보를 요청하는 신호를 상기 제 1 외부 전자 장치로부터 수신하고,
상기 애플릿과 관련된 정보를 상기 제 1 외부 전자 장치로 전송하고,
상기 제 1 외부 전자 장치로부터 상기 공유 키 및 상기 공유 키와 관련된 정보를 수신하고,

상기 수신한 공유 키 및 상기 공유 키와 관련된 정보를 상기 보안 모듈 상에 설치하도록 설정된 전자 장치.

[청구항 12] 제 11항에 있어서,
상기 프로세서는
상기 운송 수단의 정보를 상기 제 1 외부 전자 장치로부터 수신하고,
상기 운송 수단의 정보에 기반하여 상기 공유 키를 관리할 애플릿 식별자를 확인하고,
상기 애플릿을 설치하는 명령을 상기 보안 모듈에 전송하도록 설정된 전자 장치.

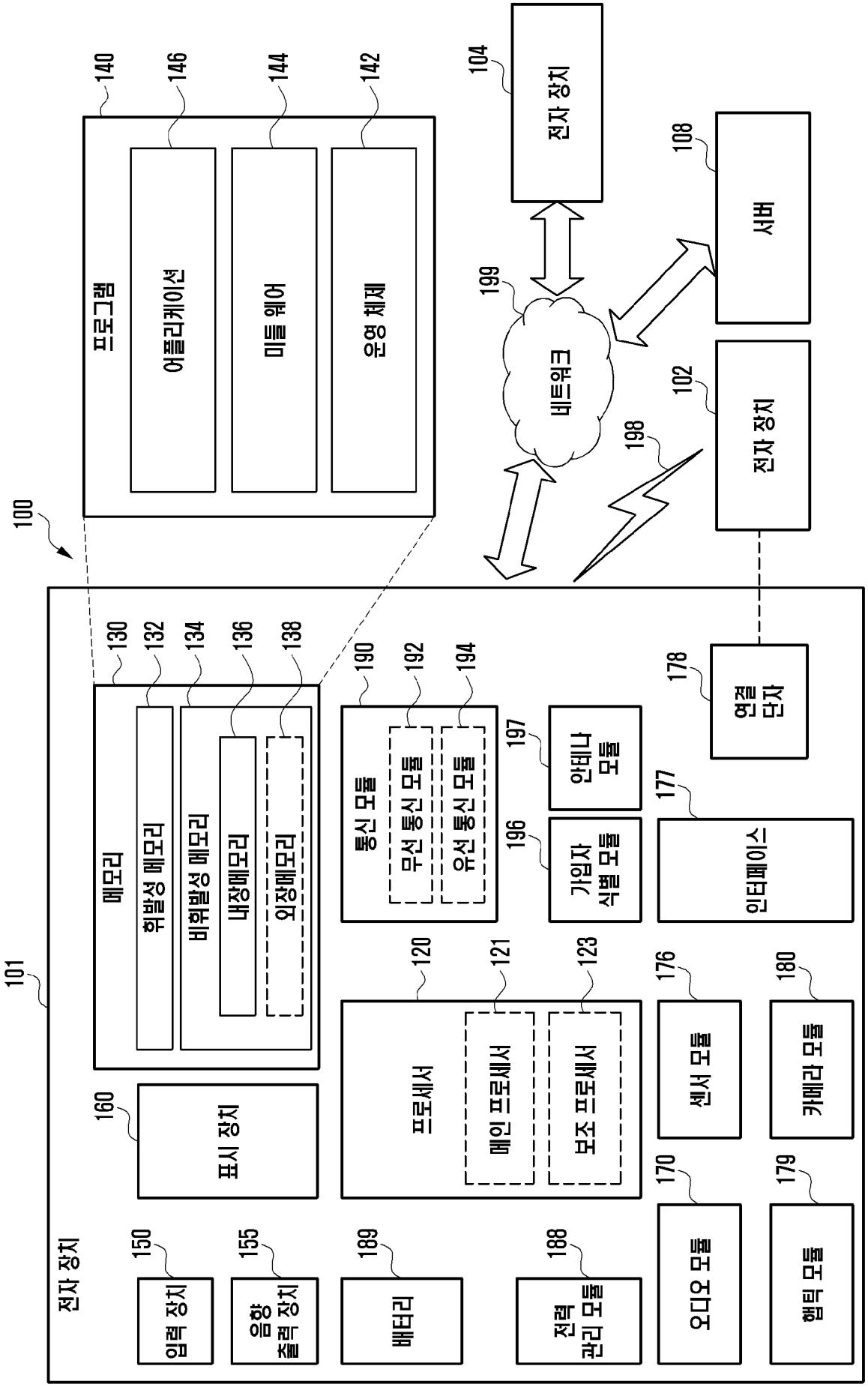
[청구항 13] 제 11항에 있어서,
상기 보안 모듈은
상기 보안 모듈에 설치된 애플릿이 복수인 경우, 상기 공유 키를 관리할 애플릿을 제외한 나머지 애플릿을 비활성화하고,
상기 공유 키의 설치가 완료됨에 대응하여, 상기 나머지 애플릿을 활성화하도록 설정된 전자 장치.

[청구항 14] 제 11항에 있어서,
상기 보안 모듈은
상기 애플릿과 관련된 정보를 관리하는 PVKSE(proximity vehicle key system environment)를 포함하고, 상기 PVKSE 는 상기 보안 모듈의 발급된 보안 도메인(issued security domain)에 저장되며, 상기 애플릿은 추가 보안 도메인(supplementary security domain)에 저장되도록 설정된 전자 장치.

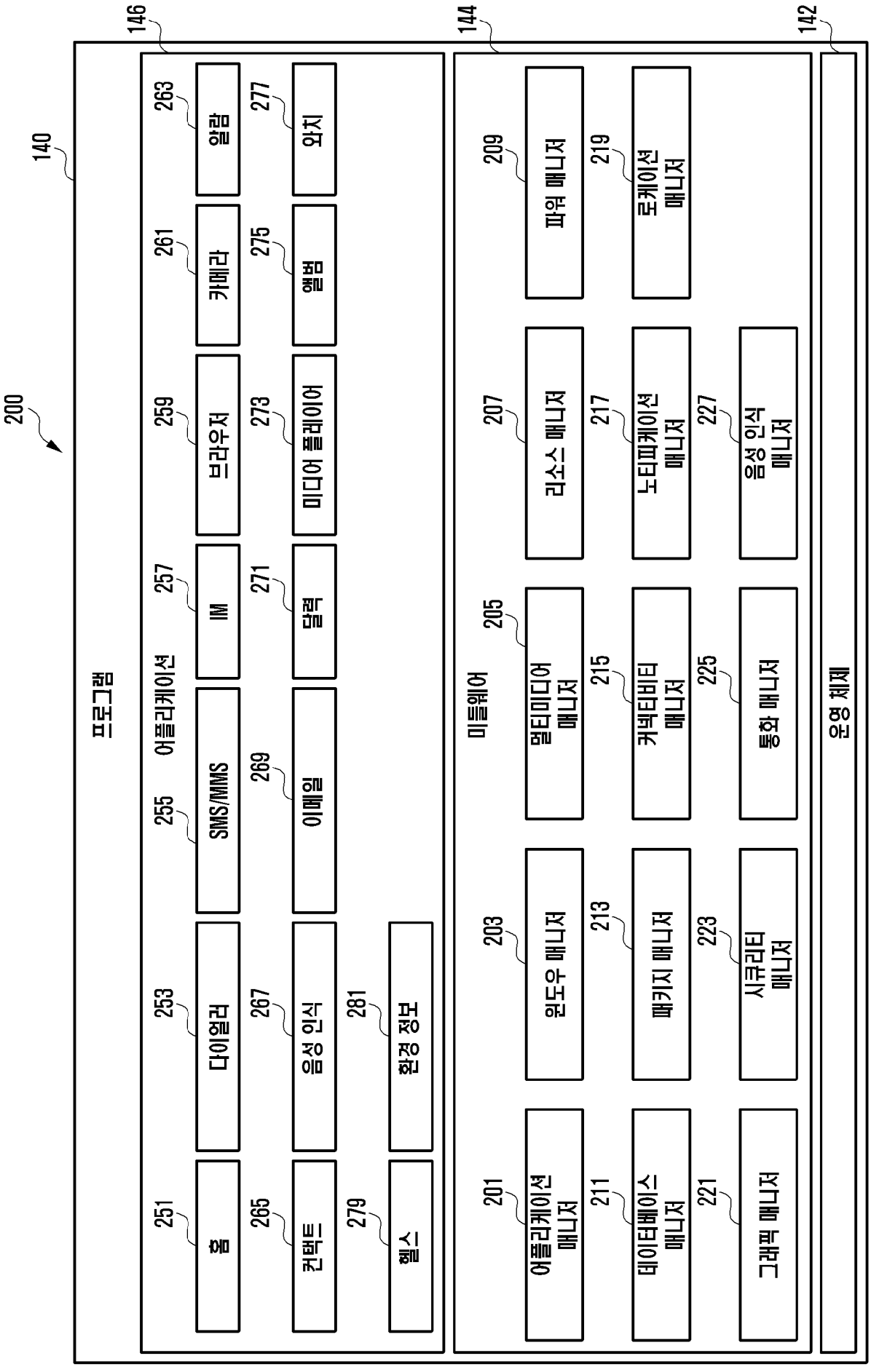
[청구항 15] 제 11항에 있어서,
상기 공유키와 관련된 정보는
상기 제 1 외부 전자 장치에 저장되고, 상기 제 2 외부 전자 장치의 인증에 이용되는 인증 키에 기반하여 생성됨을 지시하는 정보를 포함하는 전자 장치.

WO 2019/194428 PCT/KR2019/002946

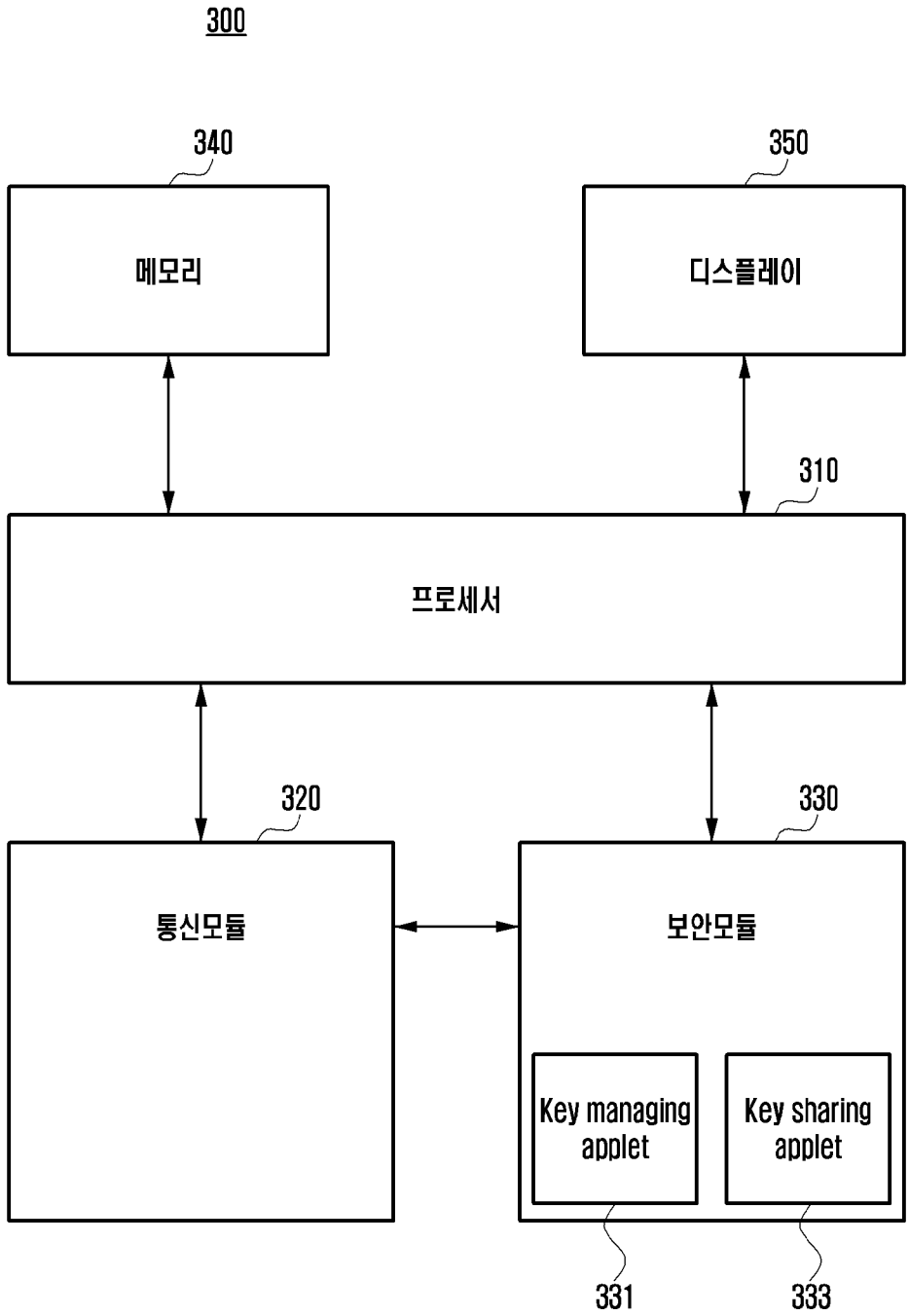
[도1]



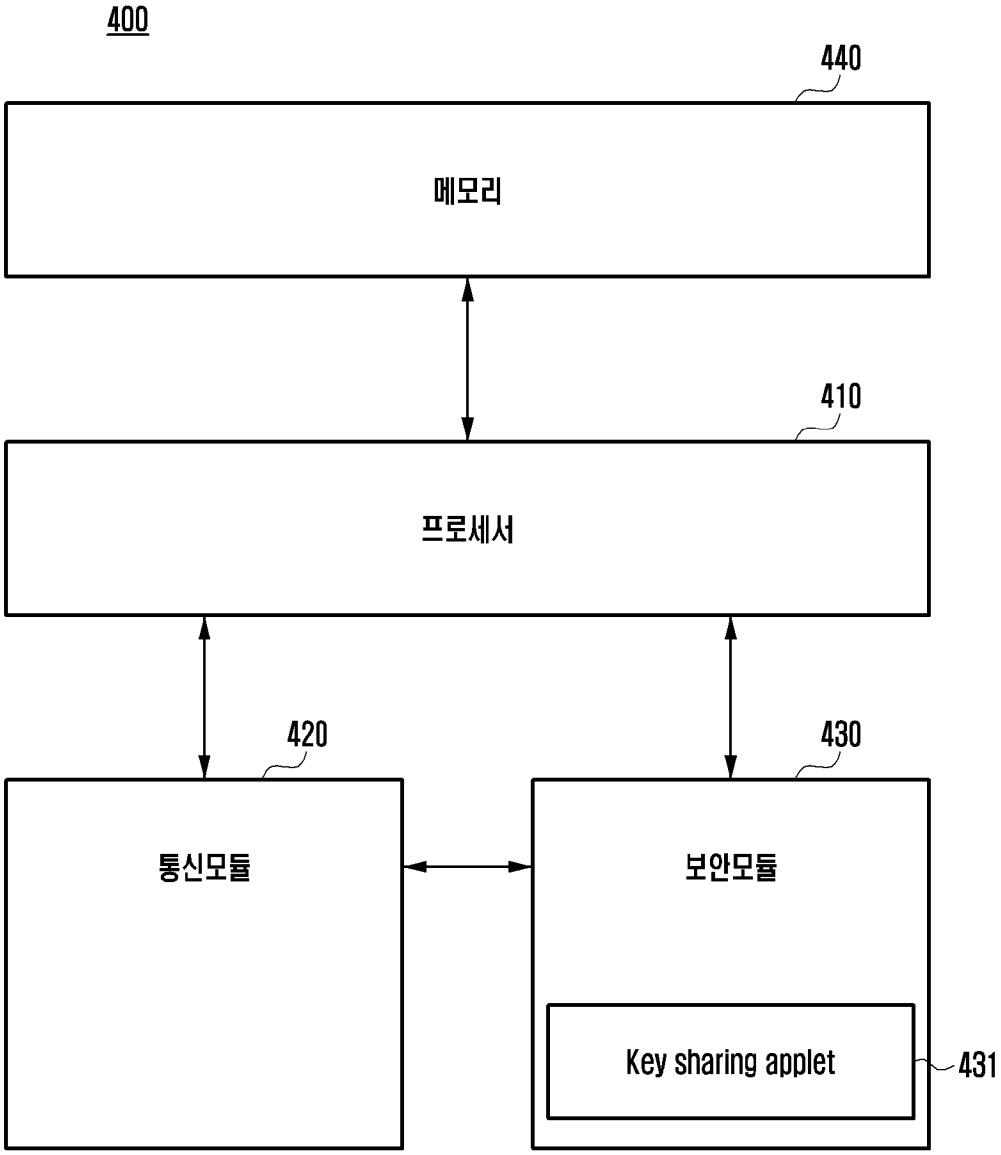
[도2]


200
140
프로그램
146
어플리케이션
251 홈
253 다이얼러
255 SMS/MMS
257 IM
259 브라우저
261 카메라
263 알람
265 컨택트
267 음성 인식
269 이메일
271 달력
273 미디어 플레이어
275 앨범
277 와치
279 헬스
281 환경 정보
144
미들웨어
201 어플리케이션 매니저
203 윈도우 매니저
205 멀티미디어 매니저
207 리소스 매니저
209 파워 매니저
211 데이터베이스 매니저
213 패키지 매니저
215 커넥티비티 매니저
217 노티피케이션 매니저
219 로케이션 매니저
221 그래픽 매니저
223 시큐리티 매니저
225 통화 매니저
227 음성 인식 매니저
142
운영 체제

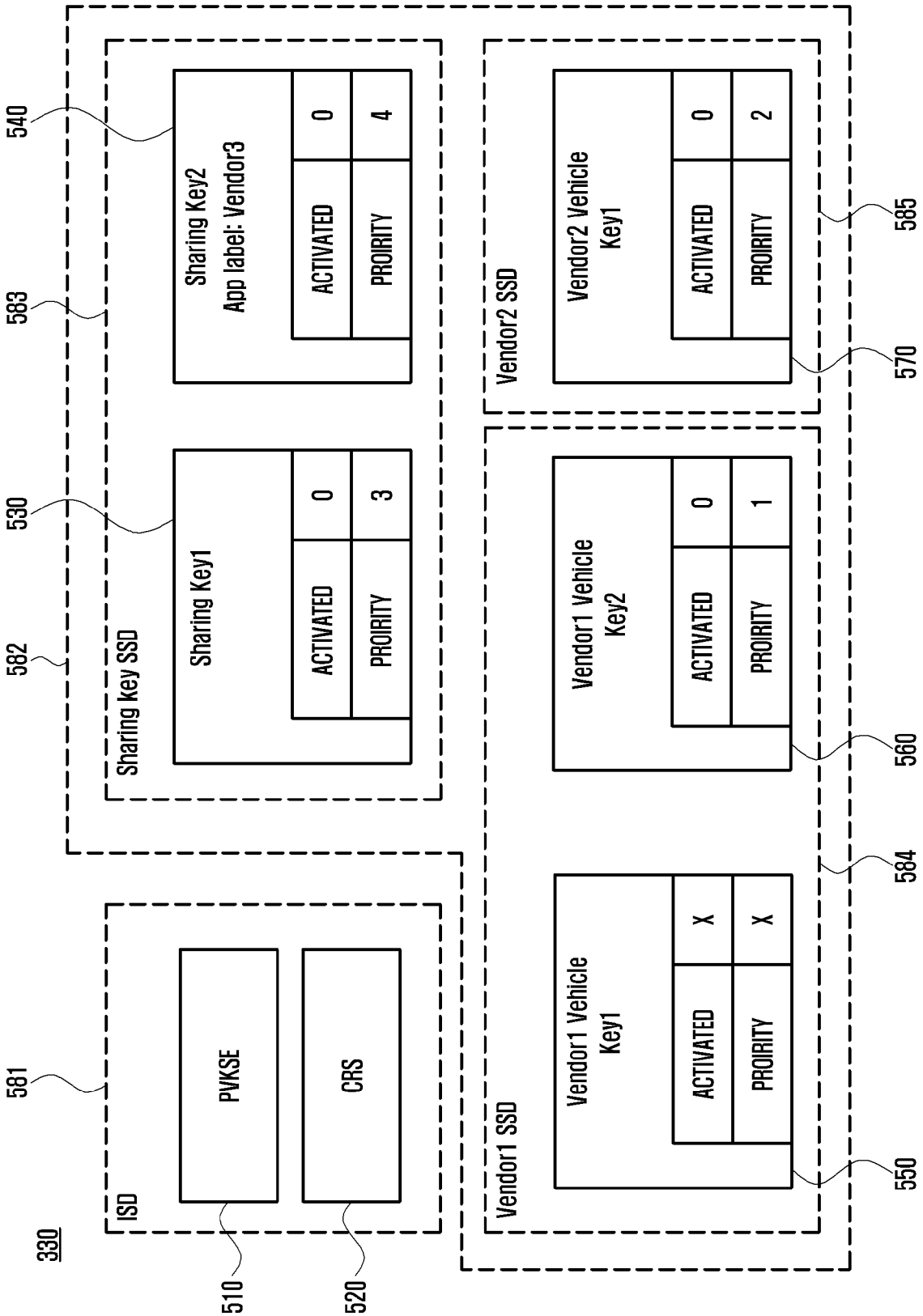
[도3]


300
340
메모리
350
디스플레이
310
프로세서
320
통신모듈
330
보안모듈
Key managing applet
Key sharing applet
331
333

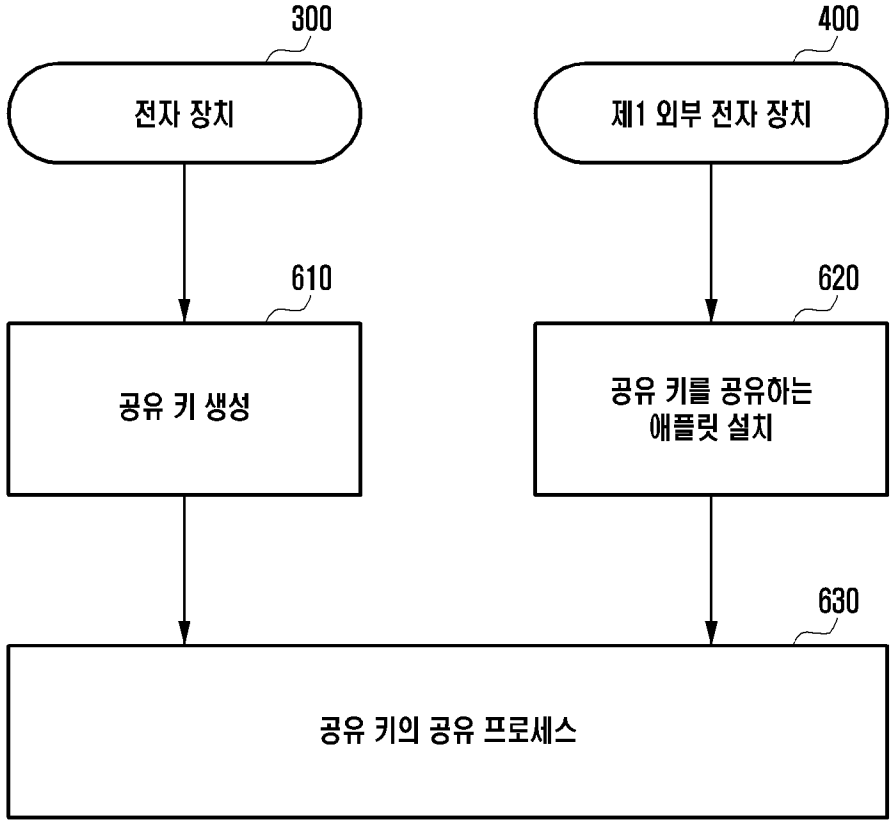
[도4]



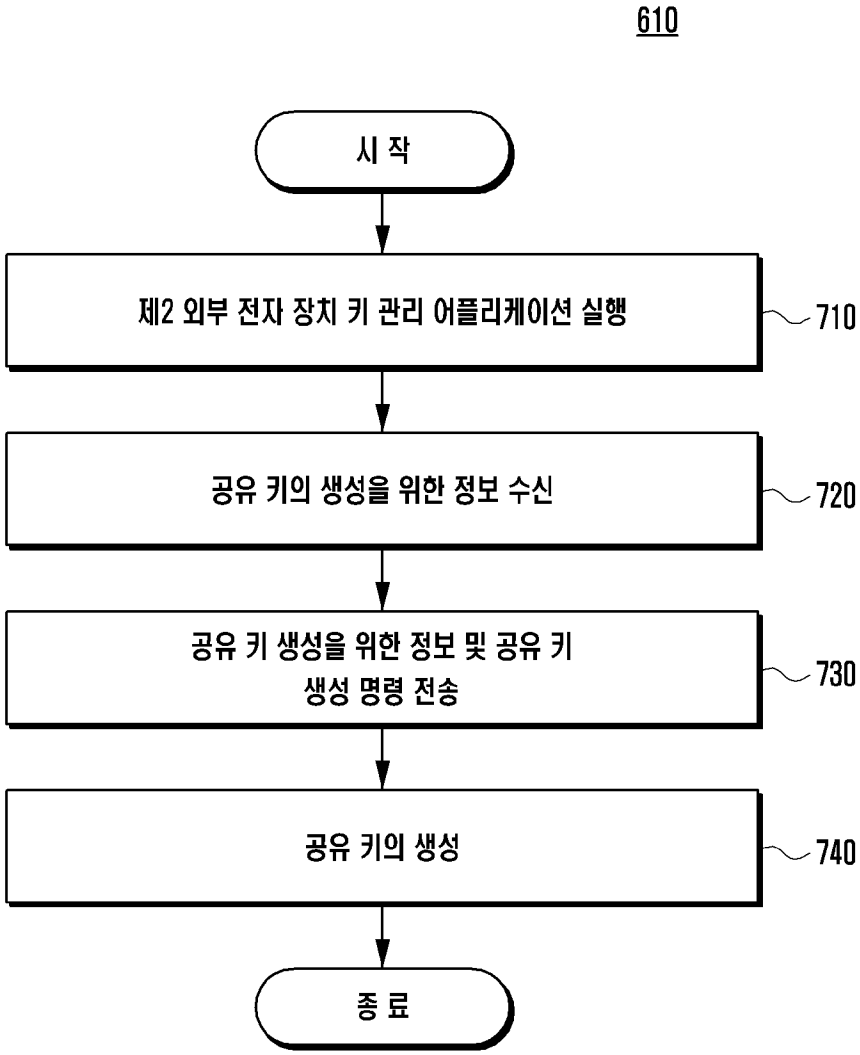
[도5]


330
ISD
581
PVKSE
CRS
510
520
Sharing key SSD
582
Sharing Key1
530
ACTIVATED
0
PRIORITY
3
Sharing Key2
App label: Vendor3
583
540
ACTIVATED
0
PRIORITY
4
Vendor1 SSD
584
Vendor1 Vehicle
Key1
550
ACTIVATED
X
PRIORITY
X
Vendor1 Vehicle
Key2
560
ACTIVATED
0
PRIORITY
1
Vendor2 SSD
585
Vendor2 Vehicle
Key1
570
ACTIVATED
0
PRIORITY
2

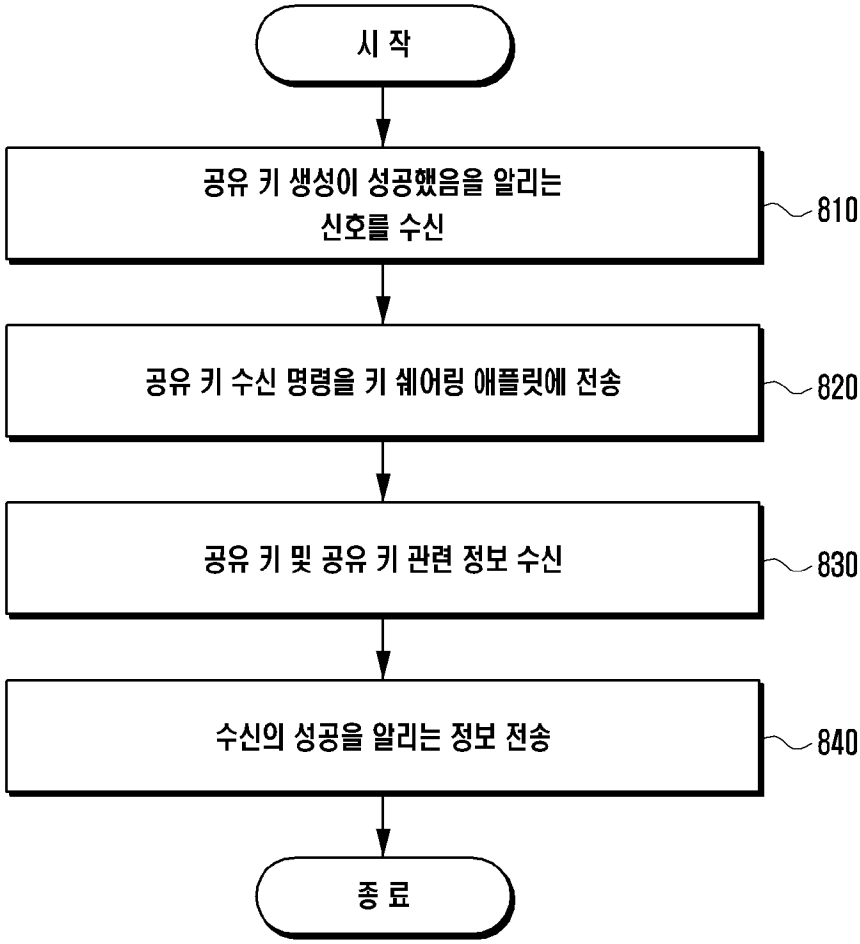
[도6]


300
전자 장치
400
제1 외부 전자 장치
610
공유 키 생성
620
공유 키를 공유하는
애플릿 설치
630
공유 키의 공유 프로세스

[도7]

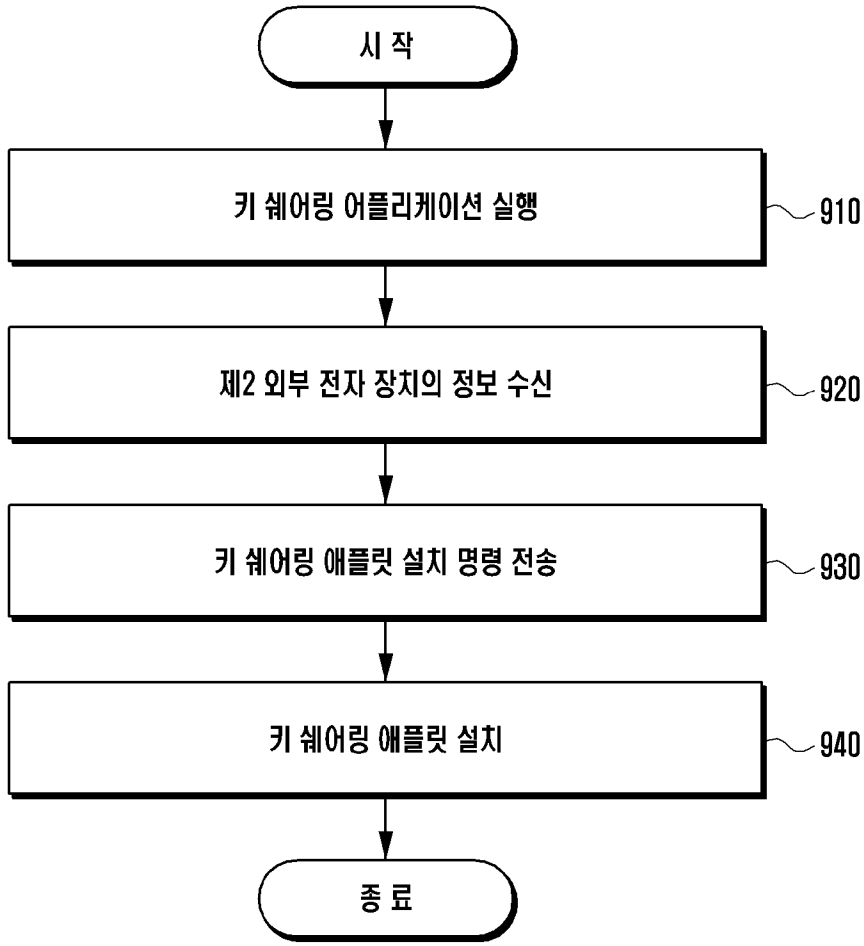

610
시 작
제2 외부 전자 장치 키 관리 어플리케이션 실행
710
공유 키의 생성을 위한 정보 수신
720
공유 키 생성을 위한 정보 및 공유 키 생성 명령 전송
730
공유 키의 생성
740
종 료

[도8]

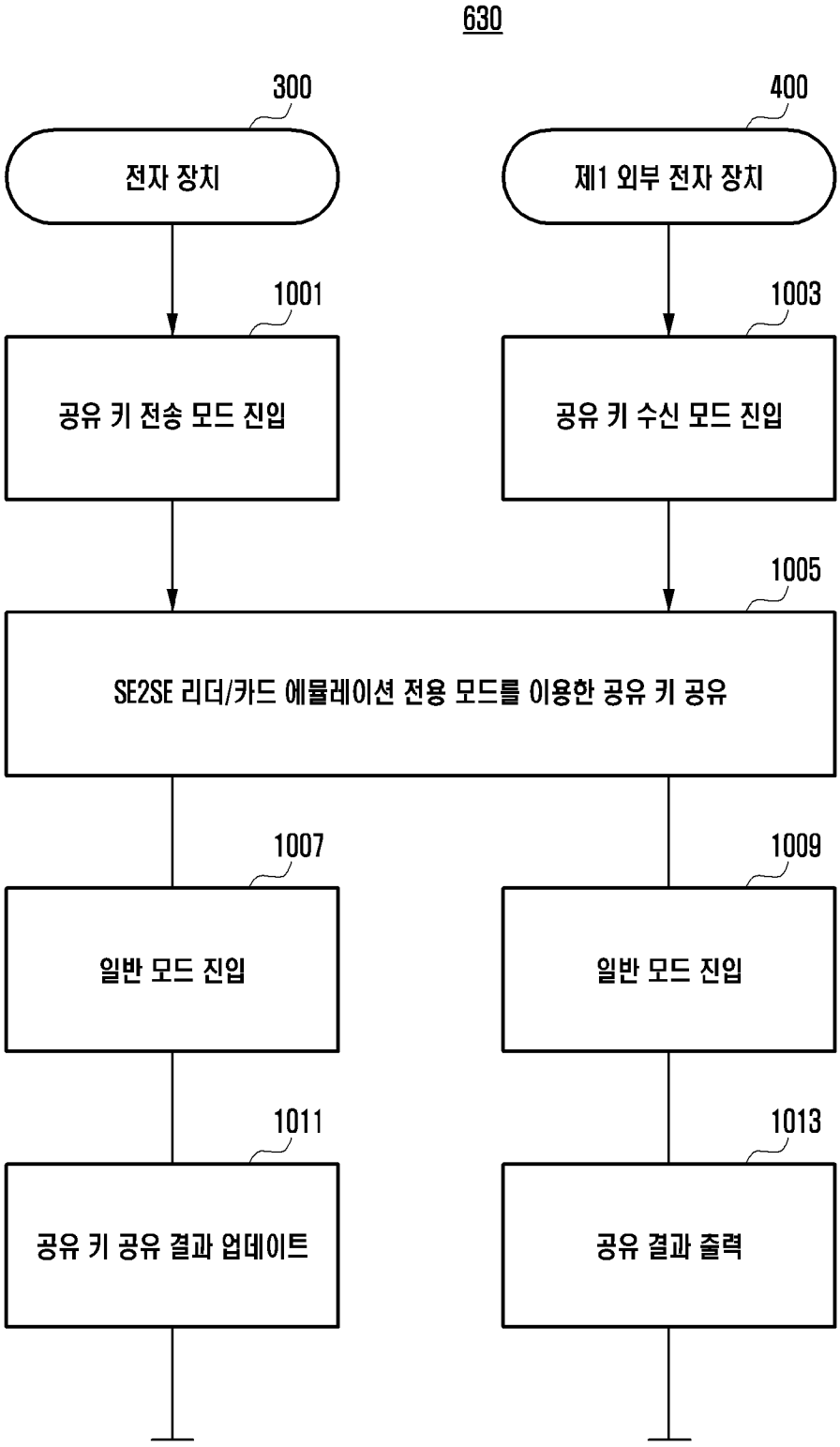

시 작
공유 키 생성이 성공했음을 알리는 신호를 수신
810
공유 키 수신 명령을 키 쉐어링 애플릿에 전송
820
공유 키 및 공유 키 관련 정보 수신
830
수신의 성공을 알리는 정보 전송
840
종 료

[도9]

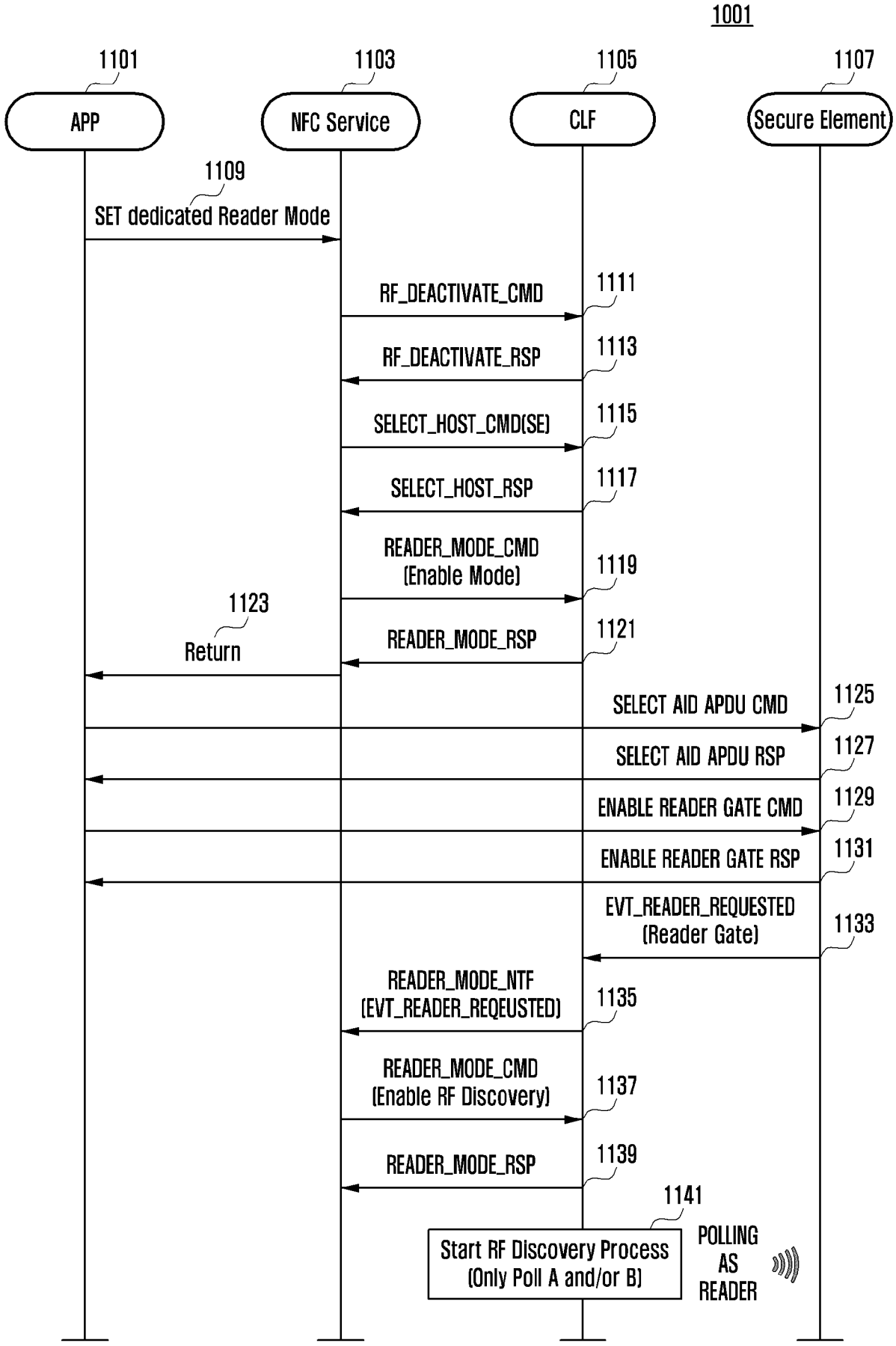
620


시 작
키 쉐어링 어플리케이션 실행
910
제2 외부 전자 장치의 정보 수신
920
키 쉐어링 애플릿 설치 명령 전송
930
키 쉐어링 애플릿 설치
940
종 료

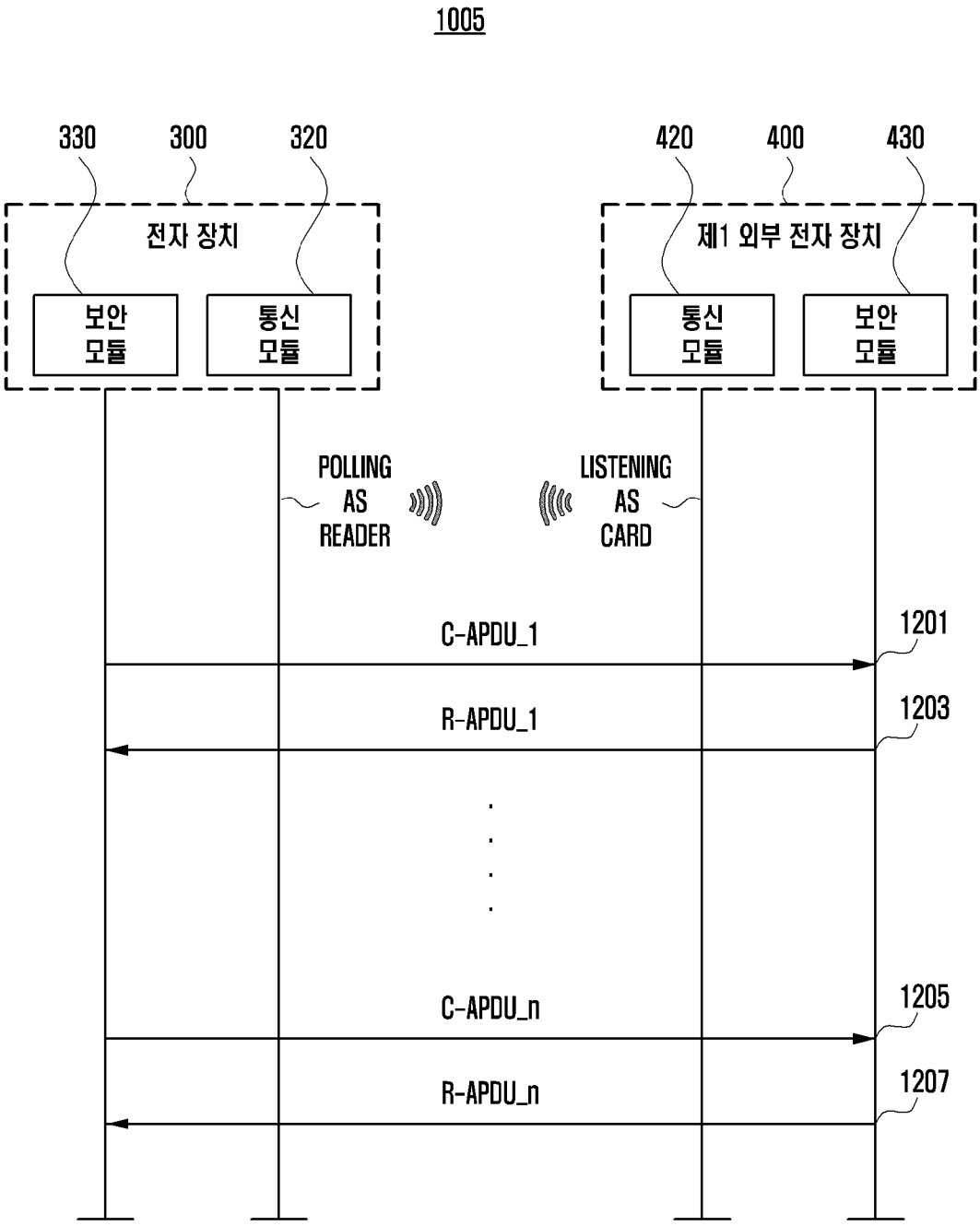
[도10]


630
300
전자 장치
400
제1 외부 전자 장치
1001
공유 키 전송 모드 진입
1003
공유 키 수신 모드 진입
1005
SE2SE 리더/카드 에뮬레이션 전용 모드를 이용한 공유 키 공유
1007
일반 모드 진입
1009
일반 모드 진입
1011
공유 키 공유 결과 업데이트
1013
공유 결과 출력

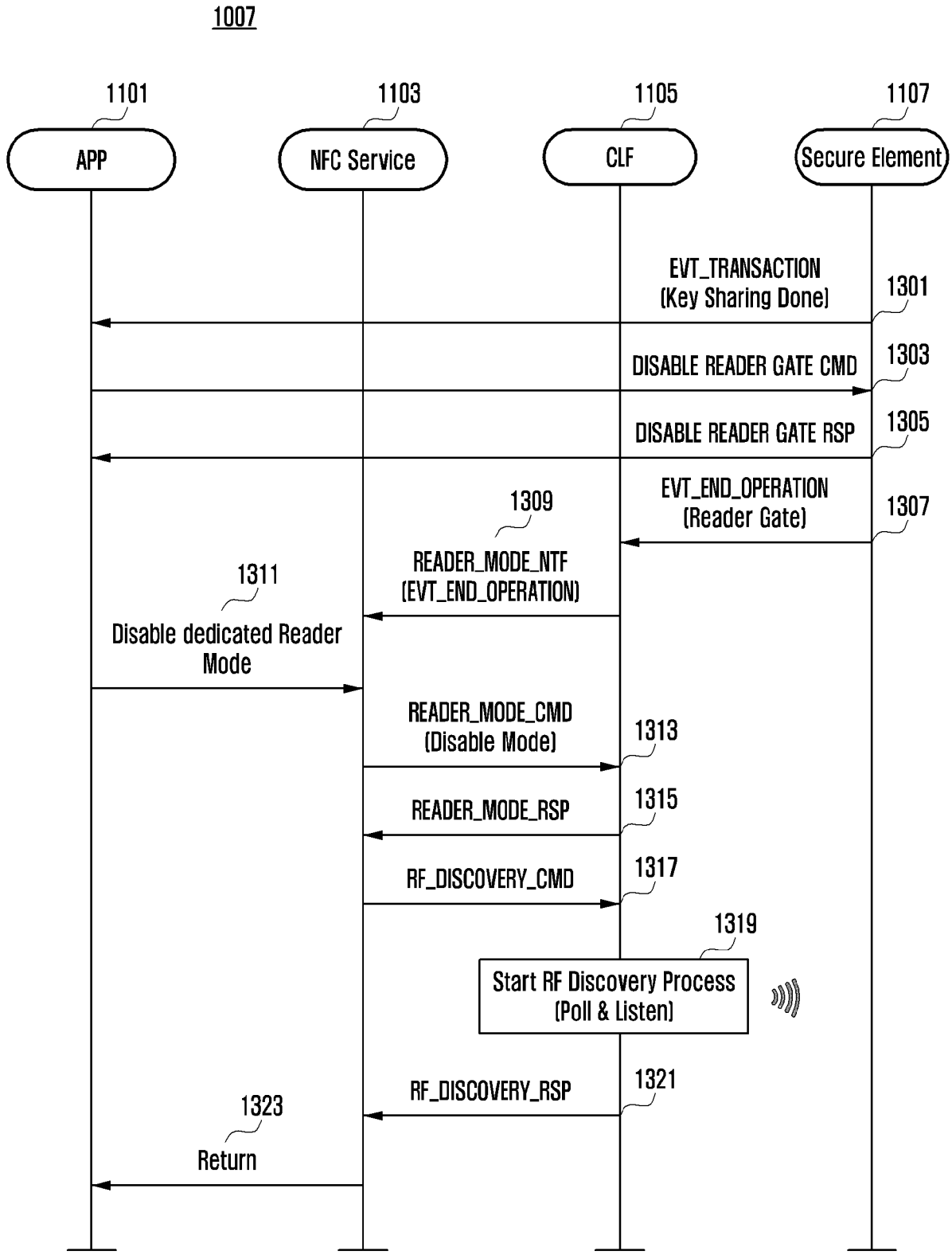
[도11]


1001
1101
APP
1103
NFC Service
1105
CLF
1107
Secure Element
1109
SET dedicated Reader Mode
RF_DEACTIVATE_CMD
1111
RF_DEACTIVATE_RSP
1113
SELECT_HOST_CMD(SE)
1115
SELECT_HOST_RSP
1117
READER_MODE_CMD
(Enable Mode)
1119
READER_MODE_RSP
1121
1123
Return
SELECT AID APDU CMD
1125
SELECT AID APDU RSP
1127
ENABLE READER GATE CMD
1129
ENABLE READER GATE RSP
1131
EVT_READER_REQUESTED
(Reader Gate)
1133
READER_MODE_NTF
(EVT_READER_REQEUSTED)
1135
READER_MODE_CMD
(Enable RF Discovery)
1137
READER_MODE_RSP
1139
1141
Start RF Discovery Process
(Only Poll A and/or B)
POLLING
AS
READER

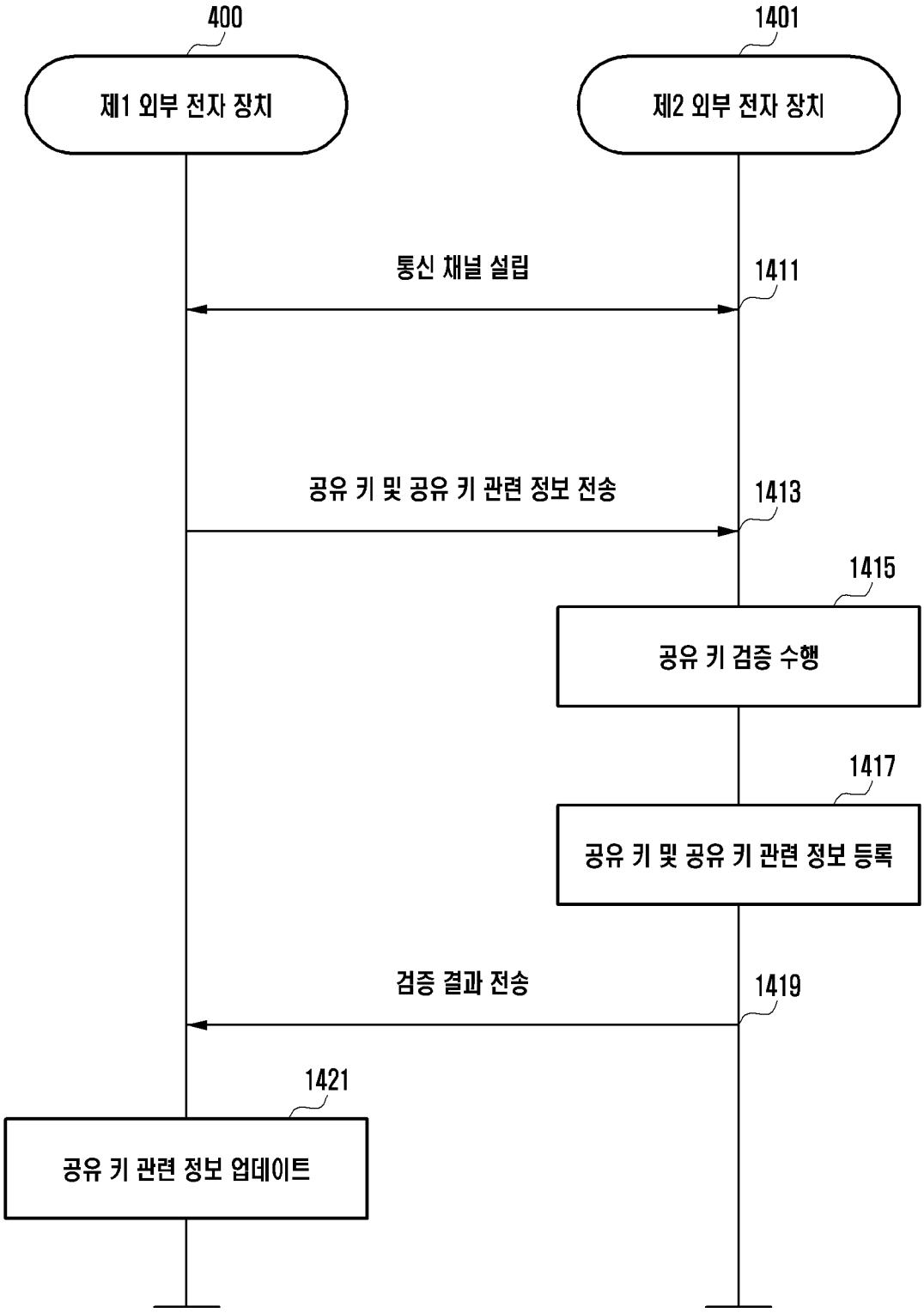
[도12]


1005
330
300
320
420
400
430
전자 장치
보안 모듈
통신 모듈
제1 외부 전자 장치
통신 모듈
보안 모듈
POLLING AS READER
LISTENING AS CARD
C-APDU_1
1201
R-APDU_1
1203
C-APDU_n
1205
R-APDU_n
1207

[도13]


1007
1101
APP
1103
NFC Service
1105
CLF
1107
Secure Element
EVT_TRANSACTION
(Key Sharing Done)
1301
DISABLE READER GATE CMD
1303
DISABLE READER GATE RSP
1305
EVT_END_OPERATION
(Reader Gate)
1307
1309
READER_MODE_NTF
(EVT_END_OPERATION)
1311
Disable dedicated Reader Mode
READER_MODE_CMD
(Disable Mode)
1313
READER_MODE_RSP
1315
RF_DISCOVERY_CMD
1317
1319
Start RF Discovery Process
(Poll & Listen)
RF_DISCOVERY_RSP
1321
1323
Return

[도14]


400
제1 외부 전자 장치
1401
제2 외부 전자 장치
통신 채널 설립
1411
공유 키 및 공유 키 관련 정보 전송
1413
1415
공유 키 검증 수행
1417
공유 키 및 공유 키 관련 정보 등록
검증 결과 전송
1419
1421
공유 키 관련 정보 업데이트

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2019/002946

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/33(2013.01)i, H04L 9/08(2006.01)i, H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/33; E05B 85/00; G06Q 20/16; G06Q 20/40; G06Q 50/30; H04W 12/04; H04W 4/02; H04W 4/04; H04W 88/02; H04L 9/08; H04L 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: electronic device, external, vehicle, authentication key, sharing key, applet, security module

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2016-0088880 A (QUALCOMM INCORPORATED) 26 July 2016 See paragraphs [0034]-[0058], [0073], [0111]; and figures 1-2.	1-13,15
Y		14
Y	KR 10-2014-0098872 A (NAMKOONG, Yongjoo) 08 August 2014 See claim 9.	14
A	KR 10-2015-0063198 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 09 June 2015 See paragraphs [0026]-[0040]; claim 1; and figure 1.	1-15
A	KR 10-2017-0138031 A (KOREA AUTOMOTIVE TECHNOLOGY INSTITUTE) 14 December 2017 See paragraphs [0027]-[0033]; claims 1-8; and figure 1.	1-15
A	KR 10-2015-0107591 A (SAMSUNG ELECTRONICS CO., LTD.) 23 September 2015 See paragraphs [0031]-[0063]; claims 1-2, 7-9; and figure 1.	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 JUNE 2019 (24.06.2019)	**24 JUNE 2019 (24.06.2019)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2019/002946

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2016-0088880 A	26/07/2016	CN 105830470 A	03/08/2016
		CN 105850159 A	10/08/2016
		CN 107005789 A	01/08/2017
		EP 3072316 A1	28/09/2016
		EP 3072317 A1	28/09/2016
		EP 3072317 B1	16/05/2018
		EP 3222068 A1	27/09/2017
		JP 2017-505253 A	16/02/2017
		JP 2017-509171 A	30/03/2017
		JP 2017-537545 A	14/12/2017
		JP 6194114 B2	06/09/2017
		JP 6246365 B2	13/12/2017
		KR 10-1752115 B1	28/06/2017
		KR 10-2016-0088879 A	26/07/2016
		US 2015-0148989 A1	28/05/2015
		US 2015-0149042 A1	28/05/2015
		US 2016-0142877 A1	19/05/2016
		US 9358940 B2	07/06/2016
		US 9428127 B2	30/08/2016
		US 9980090 B2	22/05/2018
		WO 2015-077662 A1	28/05/2015
		WO 2015-077664 A1	28/05/2015
		WO 2016-081607 A1	26/05/2016
KR 10-2014-0098872 A	08/08/2014	None	
KR 10-2015-0063198 A	09/06/2015	None	
KR 10-2017-0138031 A	14/12/2017	KR 10-2019-0004831 A	14/01/2019
KR 10-2015-0107591 A	23/09/2015	KR 10-2015-0108027 A	24/09/2015
		US 2015-0262441 A1	17/09/2015
		US 2018-0170308 A1	21/06/2018
		US 9896061 B2	20/02/2018
		WO 2015-142002 A1	24/09/2015

국 제 조 사 보 고 서

국제출원번호
PCT/KR2019/002946

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/33(2013.01)i, H04L 9/08(2006.01)i, H04L 9/32(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 21/33; E05B 85/00; G06Q 20/16; G06Q 20/40; G06Q 50/30; H04W 12/04; H04W 4/02; H04W 4/04; H04W 88/02; H04L 9/08; H04L 9/32

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 전자 장치(electronic device), 외부(external), 운송 수단(vehicle), 인증 키(authentication key), 공유 키(sharing key), 애플릿(applet), 보안 모듈(security module)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2016-0088880 A (퀄컴 인코포레이티드) 2016.07.26 단락 [0034]-[0058], [0073], [0111]; 및 도면 1-2 참조.	1-13,15
Y		14
Y	KR 10-2014-0098872 A (남궁용주) 2014.08.08 청구항 9 참조.	14
A	KR 10-2015-0063198 A (한국전자통신연구원) 2015.06.09 단락 [0026]-[0040]; 청구항 1; 및 도면 1 참조.	1-15
A	KR 10-2017-0138031 A (자동차부품연구원) 2017.12.14 단락 [0027]-[0033]; 청구항 1-8; 및 도면 1 참조.	1-15
A	KR 10-2015-0107591 A (삼성전자주식회사) 2015.09.23 단락 [0031]-[0063]; 청구항 1-2, 7-9; 및 도면 1 참조.	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2019년 06월 24일 (24.06.2019)	2019년 06월 24일 (24.06.2019)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
진상범
전화번호 +82-42-481-8398

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2019/002946

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2016-0088880 A	2016/07/26	CN 105830470 A	2016/08/03
		CN 105850159 A	2016/08/10
		CN 107005789 A	2017/08/01
		EP 3072316 A1	2016/09/28
		EP 3072317 A1	2016/09/28
		EP 3072317 B1	2018/05/16
		EP 3222068 A1	2017/09/27
		JP 2017-505253 A	2017/02/16
		JP 2017-509171 A	2017/03/30
		JP 2017-537545 A	2017/12/14
		JP 6194114 B2	2017/09/06
		JP 6246365 B2	2017/12/13
		KR 10-1752115 B1	2017/06/28
		KR 10-2016-0088879 A	2016/07/26
		US 2015-0148989 A1	2015/05/28
		US 2015-0149042 A1	2015/05/28
		US 2016-0142877 A1	2016/05/19
		US 9358940 B2	2016/06/07
		US 9428127 B2	2016/08/30
		US 9980090 B2	2018/05/22
		WO 2015-077662 A1	2015/05/28
		WO 2015-077664 A1	2015/05/28
		WO 2016-081607 A1	2016/05/26
KR 10-2014-0098872 A	2014/08/08	없음	
KR 10-2015-0063198 A	2015/06/09	없음	
KR 10-2017-0138031 A	2017/12/14	KR 10-2019-0004831 A	2019/01/14
KR 10-2015-0107591 A	2015/09/23	KR 10-2015-0108027 A	2015/09/24
		US 2015-0262441 A1	2015/09/17
		US 2018-0170308 A1	2018/06/21
		US 9896061 B2	2018/02/20
		WO 2015-142002 A1	2015/09/24