

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020 년 3 월 26 일 (26.03.2020) **WIPO | PCT**



(10) 국제공개번호
WO 2020/060101 A1

- (51) 국제특허분류: **G06F 21/56** (2013.01) **G06F 21/60** (2013.01)
- (21) 국제출원번호: PCT/KR2019/011774
- (22) 국제출원일: 2019 년 9 월 11 일 (11.09.2019)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보: 10-2018-0112989 2018 년 9 월 20 일 (20.09.2018) KR
- (71) 출원인: 삼성전자 주식회사 (**SAMSUNG ELECTRONICS CO., LTD.**) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).
- (72) 발명자: 이택기 (**LEE, Taekki**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 김종수 (**KIM, Jongsu**); 16677 경기도 수원시 영통구 삼성로 129,

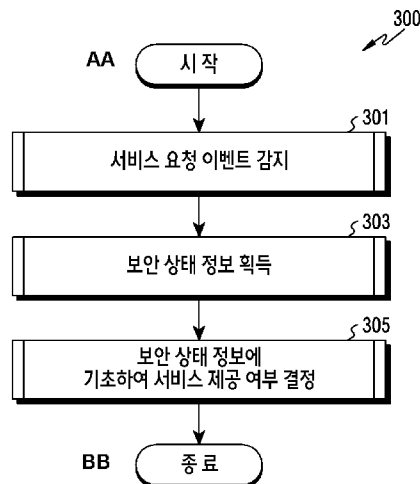
Gyeonggi-do (KR). 권은영 (**KWON, Eunyoung**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 이다솜 (**LEE, Dasom**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 조대행 (**CHO, Daehaeng**); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(74) 대리인: 권혁록 등 (**KWON, Hyuk-Rok et al.**); 03175 서울시 종로구 경희궁길 28, 2층, 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,

(54) Title: ELECTRONIC DEVICE FOR PROVIDING SERVICE BY USING SECURE ELEMENT, AND OPERATING METHOD THEREOF

(54) 발명의 명칭: 보안 엘리먼트를 이용하여 서비스를 제공하는 전자 장치 및 그의 동작 방법



301 ... Sense service request event

303 ... Acquire secure state information

305 ... Determine whether to provide service on basis of secure state information

AA ... Start

BB ... End

(57) Abstract: Various embodiments of the present invention relate to an electronic device for providing a service by using a secure element, and an operating method thereof. The electronic device comprises: a processor for acquiring secure state information of the electronic device; and a secure element operating under the control of the processor, receiving the secure state information of the electronic device from the processor, and including a repository for storing the received secure state information of the electronic device, wherein the secure element senses a security-related service request command, acquires the secure state information about the electronic device from the repository, and can process or ignore the sensed security-related service request command on the basis of whether the acquired secure state information of the electronic device satisfies a designated condition. Other embodiments are also possible.

SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (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))

(57) 요약서: 본 발명의 다양한 실시예는 보안 엘리먼트를 이용하여 서비스를 제공하는 전자 장치 및 그의 동작 방법에 관한 것이다. 이때 전자 장치는 상기 전자 장치의 보안 상태 정보를 획득하는 프로세서, 및 상기 프로세서의 제어에 의해 동작하고, 상기 프로세서로부터 상기 전자 장치의 보안 상태 정보를 수신하고, 수신된 전자 장치의 보안 상태 정보를 저장하는 저장소를 포함하는 보안 엘리먼트를 포함하고, 상기 보안 엘리먼트는, 보안 관련 서비스 요청 명령을 감지하고, 상기 저장소에서 상기 전자 장치의 보안 상태 정보를 획득하고, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시할 수 있다. 다른 실시예들도 가능할 수 있다.

명세서

발명의 명칭: 보안 엘리먼트를 이용하여 서비스를 제공하는 전자 장치 및 그의 동작 방법

기술분야

- [1] 본 발명의 다양한 실시예들은 보안 엘리먼트(secure element)를 이용하여 서비스를 제공하는 전자 장치 및 그의 동작 방법에 관한 것이다.

배경기술

- [2] 전자 장치는 보안 엘리먼트를 이용하여 다양한 보안 관련 서비스를 제공할 수 있다. 보안 엘리먼트는 크리덴셜(credential)과 같은 보안에 민감한 정보를 생성, 저장, 및/또는 관리하는 하드웨어 모듈이다. 보안 엘리먼트는, 신용 결제 서비스나 교통 카드와 같은 서비스 어플리케이션 프로그램을 저장하고, 개인의 신분 또는 자격 증명과 관련된 증명서(예: 신분증명서, 주민등록 증명서, 운전면허 증명서, 출입 증명서, 여권, eID(electronic identification))를 저장 및/또는 관리한다.
- [3] 보안 엘리먼트는 보안 엘리먼트에 접근하는 다른 엘리먼트(예: OCE(off card entity))의 보안 수준과 무관하게 보안 엘리먼트 칩 자체적으로 독립적인 보안성을 갖도록 설계된다. 예를 들어, 보안 엘리먼트는 하드웨어 및 소프트웨어적으로 다양한 불법적인 공격을 감지하고, 감지된 불법적인 공격으로부터 보안 엘리먼트에 저장된 정보를 안전하게 보호하도록 설계된다.

발명의 상세한 설명

기술적 과제

- [4] 보안 엘리먼트(secure element)는 모바일 기기나 IoT 장치 등과 같이 보안을 필요로 하는 전자 장치에 탑재되어 종속적으로 사용된다. 예를 들어, 보안 엘리먼트는 전자 장치의 호스트 프로세서로부터 유효한 명령이 수신되는 경우, 별다른 제약 없이 수신된 명령에 대응되는 기능을 처리한다. 즉, 보안 엘리먼트는 호스트 프로세서에 대해 종속적으로 동작하므로, 호스트 프로세서로부터 입력되는 유효한 모든 명령을 여과 없이 처리한다. 따라서, 전자 장치에 보안적인 위협이 발생할 경우, 전자 장치에 포함된 보안 엘리먼트의 보안성이 취약해질 수 있다. 예를 들어, 전자 장치가 루팅되거나 위변조되는 경우, 전자 장치에 포함된 보안 엘리먼트로의 접근 제어가 무력화됨으로써, 보안 관련 정보들이 불법적인 공격에 노출될 수 있다.
- [5] 따라서, 본 발명의 다양한 실시예들은 전자 장치의 보안 상태에 기초하여, 보안 엘리먼트를 통한 보안 서비스를 제공하는 전자 장치 및 그의 동작 방법에 관한 것이다.

과제 해결 수단

- [6] 다양한 실시예에 따르면, 전자 장치는, 상기 전자 장치의 보안 상태 정보를

획득하는 프로세서, 및 상기 프로세서의 제어에 의해 동작하고, 상기 프로세서로부터 상기 전자 장치의 보안 상태 정보를 수신하고, 수신된 전자 장치의 보안 상태 정보를 저장하는 저장소를 포함하는 보안 엘리먼트를 포함하고, 상기 보안 엘리먼트는, 보안 관련 서비스 요청 명령을 감지하고, 상기 저장소에서 상기 전자 장치의 보안 상태 정보를 획득하고, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시할 수 있다.

- [7] 다양한 실시예에 따르면, 전자 장치의 동작 방법은, 프로세서에서, 상기 전자 장치의 보안 상태 정보를 획득하는 동작, 상기 프로세서의 제어에 의해 동작하는 보안 엘리먼트에서, 상기 전자 장치의 보안 상태 정보를 상기 보안 엘리먼트 내부의 저장소에 저장하는 동작, 상기 보안 엘리먼트에서, 보안 관련 서비스 요청 명령을 감지하는 동작, 상기 보안 엘리먼트에서 상기 내부의 저장소에 저장된 상기 전자 장치의 보안 상태 정보를 획득하는 동작, 및 상기 보안 엘리먼트에서, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작을 포함할 수 있다.

발명의 효과

- [8] 다양한 실시예들은, 전자 장치에서 전자 장치의 보안 상태에 기초하여, 보안 엘리먼트(secure element)를 통한 서비스 제공 여부를 결정함으로써, 전자 장치가 보안적으로 취약해진 상태에서 보안 엘리먼트에 저장된 보안 관련 정보가 불법적인 공격에 노출되는 것을 방지하고, 더 높은 수준의 보안 관련 서비스를 제공할 수 있다.

도면의 간단한 설명

- [9] 도 1은 다양한 실시예들에 따른, 네트워크 환경 내의 전자 장치의 블록도이다.
 [10] 도 2는 다양한 실시예들에 따른, 보안 엘리먼트와 다른 구성 요소들 사이의 통신 구조를 나타내는 블록도이다.
 [11] 도 3은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 서비스를 제공하는 흐름도이다.
 [12] 도 4는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보를 저장하는 흐름도이다.
 [13] 도 5는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보를 저장하는 예시도이다.
 [14] 도 6은 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 흐름도이다.
 [15] 도 7은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 예시도이다.
 [16] 도 8은 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에

기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 신호 흐름도이다.

- [17] 도 9는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 무선 인터페이스를 통한 서비스를 제공하는 흐름도이다.
- [18] 도 10은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 무선 인터페이스를 통한 서비스를 제공하는 예시도이다.
- [19] 도 11은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 통신 인터페이스를 이용한 보안 엘리먼트에 대한 접근을 제어하는 흐름도이다.
- [20] 도 12는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 통신 인터페이스를 이용한 보안 엘리먼트에 대한 접근을 제어하는 예시도이다.
- [21] 도 13은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 정보를 제공하는 흐름도이다.
- [22] 도 14는 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 정보를 제공하는 예시도이다.
- [23] 도 15는 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 정보를 제공하는 신호 흐름도이다.

발명의 실시를 위한 최선의 형태

- [24] 이하, 본 문서의 다양한 실시예들이 첨부된 도면을 참조하여 기재된다. 실시예 및 이에 사용된 용어들은 본 문서에 기재된 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 해당 실시예의 다양한 변경, 균등물, 및/또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다.
- [25] 도 1은, 다양한 실시예들에 따른, 네트워크 환경(100) 내의 전자 장치(101)의 블록도이다. 도 1을 참조하면, 네트워크 환경(100)에서 전자 장치(101)는 제1 네트워크(198)(예: 근거리 무선 통신 네트워크)를 통하여 전자 장치(102)와 통신하거나, 또는 제2 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), 보안 엘리먼트(172), 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.

- [26] 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)를 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)는 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.
- [27] 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.
- [28] 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.
- [29] 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.
- [30] 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.

- [31] 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.
- [32] 표시 장치(160)는 전자 장치(101)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 표시 장치(160)는, 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 발생하는 힘의 세기를 측정하도록 설정된 센서 회로(예: 압력 센서)를 포함할 수 있다.
- [33] 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.
- [34] 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.
- [35] 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.
- [36] 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)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.
- [37] 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.
- [38] 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.

- [39] 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.
- [40] 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.
- [41] 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.
- [42] 안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 안테나 모듈은, 일실시예에 따르면, 도전체 또는 도전성 패턴으로 형성될 수 있고, 어떤 실시예에 따르면, 도전체 또는 도전성 패턴 이외에 추가적으로 다른 부품(예: RFIC)을 더 포함할 수 있다. 일실시예에 따르면, 안테나 모듈(197)은 하나 이상의 안테나들을 포함할 수 있고, 이로부터, 제 1 네트워크(198) 또는 제 2 네트워크(199)와 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.
- [43] 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.
- [44] 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. 일 실시예에 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.

- [45] 보안 엘리먼트(172)는 보안에 민감한 정보를 생성, 저장, 및/또는 관리하는 모듈이다. 보안 엘리먼트(172)는, 예를 들어, 신용 결제 서비스나 교통 카드 서비스를 제공하는 어플리케이션 프로그램(또는 어플릿)을 저장 및/또는 관리할 수 있고, 개인의 신분 또는 자격 증명과 관련된 정보 및/또는 증명서(예: 신분증명서, 주민등록 증명서, 운전면허 증명서, 출입 증명서, 여권, eID(electronic identification))를 저장 및/또는 관리할 수 있다. 보안 엘리먼트(172)는 독립적인 회로로 구현될 수 있으며, 별도의 프로세서를 포함할 수 있다. 보안 엘리먼트(172)는 별도의 프로세서를 포함하나, 프로세서(120)의 제어에 따라 동작할 수 있다. 예를 들어, 보안 엘리먼트(172)는 프로세서(120)에 종속적으로 동작할 수 있다. 보안 엘리먼트(172)는 프로세서(120) 또는 무선 통신 모듈(190)에 의해 활성화 및/또는 비활성화될 수 있다.

- [46] 보안 엘리먼트(172)는 전자 장치(101)의 고정 칩 내에 내장된 내장형 보안 엘리먼트(eSE; embedded secure element)를 포함할 수 있다. 보안 엘리먼트(172)는 전자 장치(101)의 운영 체제와 다른 운영 체제를 기반으로 구동될 수 있다. 예를 들어, 보안 엘리먼트(172)는 독자적인 운영 체제를 기반으로 동작할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 보안 채널 프로토콜에 기반하여 프로세서(120), 및/또는 적어도 하나의 다른 구성 요소와 통신할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는, SWP(single wired protocol), ISO, 또는 SPI(serial peripheral interface)를 이용하여 프로세서(120) 및/또는 적어도 하나의 다른 구성 요소들과 통신할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 서비스 제공자로부터 제공되는 어플릿을 설치하고, 설치된 어플릿을 이용하여 보안 관련 서비스를 제공할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 가입자 식별 모듈(196)을 포함할 수 있다. 예를 들어, 도시된 도 1에는 보안

엘리먼트(172)와 가입자 식별 모듈(196)이 별도의 모듈로 구성되어 있으나, 설계 방식에 따라 보안 엘리먼트와 가입자 식별 모듈(196)은 하나의 모듈로 구성될 수 있다.

- [47] 도 2는 다양한 실시예들에 따른, 보안 엘리먼트(172)와 적어도 하나의 다른 구성 요소 사이의 통신 구조를 나타내는 블록도(200)이다. 일실시예에 따르면, 적어도 하나의 다른 구성 요소는 도 1의 전자 장치(101)에 포함된 프로세서(120)일 수 있다.
- [48] 도 2를 참조하면, 다양한 실시예에 따른 프로세서(120)(예: 도 1의 프로세서(120))는 적어도 하나의 인터페이스를 통해 직접적 및/또는 간접적으로 보안 엘리먼트(172)(예: 도 1의 보안 엘리먼트(172))와 연결될 수 있다. 적어도 하나의 인터페이스는, 예를 들어, I2C, SWP, SPI, 또는 ISO 중 적어도 하나를 포함할 수 있다. 나열된 인터페이스들은 예시적인 것으로서, 본 발명의 다양한 실시예들은 이에 한정되지 않을 것이다. 예를 들어, 프로세서(120)는 나열된 인터페이스들 이외에 다른 통신 프로토콜을 따르는 인터페이스들을 통해 직접적 및/또는 간접적으로 보안 엘리먼트(172)와 연결될 수 있다. 일실시예에 따르면, 프로세서(120)는 별도의 접근 관리자(access rule enforcer)(또는 접근 관리 모듈)를 이용하여 적어도 하나의 다른 구성 요소(예: 근거리 통신 모듈(210)(예: 도 1의 무선 통신 모듈(192)))를 통해 간접적으로 보안 엘리먼트(172)와 통신할 수 있다. 일실시예에 따르면, 프로세서(120)는 접근 권한 감시자(또는 접근 권한 감시 모듈)를 이용하여 직접적으로 보안 엘리먼트(172)와 통신할 수 있다. 일실시예에 따르면, 접근 관리자는, I2C 인터페이스에 대한 접근 권한, 및/또는 근거리 통신 모듈(210)을 통한 보안 엘리먼트(172)로의 접근 권한을 관리하는 소프트웨어 모듈일 수 있다. 일실시예에 따르면, 접근 권한 감시자는, SPI 인터페이스에 대한 접근 권한, 및/또는 SPI 인터페이스를 통한 보안 엘리먼트(172)에 대한 접근 권한을 관리하는 소프트웨어 모듈일 수 있다.
- [49] 다양한 실시예들에 따르면, 프로세서(120)는 전자 장치(101)의 보안 상태를 감지할 수 있다. 일실시예에 따르면, 프로세서(120)는 전자 장치의 루팅 여부, 멀웨어(malware) 감지 여부, warranty bit의 변경(broken) 여부, 보안 엘리먼트(172)에 대한 접근 관리자의 위변조 여부, 전자 장치(101)의 시스템 영역에 대한 불법적 공격 감지 여부, 또는 전자 장치(101)에 설치된 어플리케이션에 대한 불법적 공격 감지 여부 중 적어도 하나를 감지할 수 있다. 프로세서(120)는 당업자에게 공지된 보안 상태 감지 기술을 이용하여 전자 장치(101)의 보안 상태를 감지할 수 있다. 예를 들어, 프로세서(120)는 warranty bit를 이용하여 전자 장치(101)의 보안 상태를 감지할 수 있다. 예컨대, 프로세서(120)는 전자 장치(101)의 부팅 시, warranty bit를 체크하여 부팅 이미지가 정상적인지 여부를 판단할 수 있다. 프로세서(120)는 warranty bit가 변경된 경우에 부팅 이미지가 비정상적인 것으로 결정하고, 전자 장치(101)의 보안 상태를 루팅(rooting)된 상태로 결정할 수 있다. 이는 예시적인 것으로서, 본

발명의 다양한 실시예에 따른 보안 상태를 감지하는 기법은 이에 한정되지 않는다. 예를 들어, 본 발명의 다양한 실시예에 따르면, 당업자에게 공지된 다양한 보안 상태 감지 기법들을 이용할 수 있다.

- [50] 다양한 실시예들에 따르면, 프로세서(120)는 감지된 전자 장치(101)의 보안 상태를 나타내는 보안 상태 정보를 보안 엘리먼트(172)로 제공할 수 있다. 전자 장치(101)의 보안 상태 정보는, 예를 들어, 전자 장치(101)의 시스템 영역에 대한 보안 상태를 나타내는 정보, 또는 전자 장치에 설치된 어플리케이션의 보안 상태를 나타내는 정보 중 적어도 하나를 포함할 수 있다. 보안 상태 정보는, 보안 레벨(또는 보안 수준)을 나타내거나, 보안 문제의 종류를 나타내는 형태로 구성될 수 있다. 예를 들어, 보안 레벨은 0레벨부터 N레벨까지의 단계로 차등적으로 미리 정의될 수 있고, 프로세서(120)는 미리 정의된 보안 레벨에 기초하여, 현재 감지된 전자 장치(101)의 보안 상태에 대응되는 보안 레벨을 결정할 수 있다. 예를 들어, "보안 레벨 N"은 보안 레벨이 가장 높은 단계이면서 전자 장치(101)가 안전한 상태이고, "보안 레벨 0"은 보안 레벨이 가장 낮은 단계이면서 전자 장치(101)의 보안 상태가 매우 취약한 상태로 정의될 수 있다. "보안 레벨 N-a"를 전자 장치(101)가 루팅되어 보안에 취약한 상태로 정의되고, "보안 레벨 N-b"를 전자 장치(102)가 루팅되었고, 보안 엘리먼트(172)에 대한 접근 관리자가 위변조되어, 보안에 취약한 상태로 정의될 수 있다. 다른 예로, 전자 장치(101)의 보안 상태 정보는, 루팅, 접근 관리자 위변조, 멀웨어(malware) 감지, 또는 워런티 비트 깨짐 중 적어도 하나의 보안 문제가 감지된 상태임을 나타내도록 정의될 수 있다. 프로세서(120)는 전자 장치(101)의 루팅이 감지된 경우, "보안 레벨 N-a", "루팅됨"을 나타내는 보안 상태 정보를 생성하고, 생성된 보안 상태 정보를 보안 엘리먼트(172)로 제공할 수 있다. 보안 상태 정보에 대한 정의는 사업자, 및/또는 설계자에 의해 결정 및/또는 변경될 수 있다.

- [51] 다양한 실시예들에 따르면, 프로세서(120)는 실시간, 주기적인 시점, 또는 지정된 이벤트 발생 시점 중 적어도 하나에 해당하는 시점에 전자 장치(101)의 보안 상태를 감지하고, 감지된 보안 상태를 나타내는 보안 상태 정보를 보안 엘리먼트(172)로 제공할 수 있다. 예를 들어, 프로세서(120)는 부팅 이벤트가 발생하는 시점, 어플리케이션 설치 시점, 소프트웨어 업데이트 시점, 또는 보안 관련 서비스 요청이 발생된 시점 중 적어도 하나의 시점에 전자 장치(101)의 보안 상태를 감지할 수 있다. 일 실시예에 따르면, 프로세서(120)는 보안 상태 감지 시점마다, 감지된 전자 장치(101)의 보안 상태를 나타내는 정보를 보안 엘리먼트(172)로 제공할 수 있다. 예를 들어, 프로세서(120)는 전자 장치(101)의 보안 상태가 감지되면, 보안 엘리먼트(172)를 활성화시키고, 활성화된 보안 엘리먼트(172)로 전자 장치(101)의 보안 상태 정보를 제공할 수 있다. 일 실시예에 따르면, 프로세서(120)는 전자 장치(101)의 보안 상태의 변경이 감지되면, 변경된 보안 상태를 나타내는 정보를 보안 엘리먼트(172)로 제공할 수 있다. 예를 들어, 프로세서(120)는 실시간, 주기적인 시점, 또는 지정된 이벤트 발생 시점마다 전자

장치(101)의 보안 상태를 감지하고, 현재 시점에 감지된 전자 장치(101)의 보안 상태와 이전 시점에 감지된 전자 장치(101)의 보안 상태의 적어도 일부가 상이하면, 보안 엘리먼트(172)를 활성화시키고, 현재 시점에 감지된 전자 장치(101)의 보안 상태를 나타내는 보안 상태 정보를 활성화된 보안 엘리먼트(172)로 제공할 수 있다. 일실시예에 따르면, 프로세서(120)는 보안 채널 프로토콜을 이용하여 보안 엘리먼트(172)로 보안 상태 정보를 제공할 수 있다. 예를 들어, 프로세서(120)는 신뢰할 수 있는 주체를 통해, 보안 상태 정보를 보안 엘리먼트(172)로 제공할 수 있고, 이를 통해 보안 상태 정보가 위변조되는 것을 방지할 수 있다.

[52] 다양한 실시예들에 따르면, 프로세서(120)는 사용자 입력에 기초하여 제1 어플리케이션을 실행하고, 실행 중인 제1 어플리케이션에 의해 보안 엘리먼트(172)를 이용하는 보안 관련 서비스가 요청됨을 감지할 수 있다. 프로세서(120)는 제1 어플리케이션을 이용하여 보안 엘리먼트(172)로 보안 관련 서비스를 요청하는 명령을 전송할 수 있다. 일실시예에 따르면, 프로세서(120)는 보안 관련 서비스를 요청하는 명령 전송 시, 제1 어플리케이션의 보안 상태 정보를 함께 보안 엘리먼트(172)로 전송할 수 있다. 일실시예에 따르면, 프로세서(120)는 제1 어플리케이션의 보안 상태 정보를 포함하면서, 보안 관련 서비스를 요청하는 명령 신호를 보안 엘리먼트(172)로 전송할 수 있다. 제1 어플리케이션의 보안 상태 정보는, 어플리케이션의 무결성(integrity) 및/또는 신뢰성 검증을 위해 필요한 정보(예: 어플리케이션 해시(hash) 정보)를 포함할 수 있다.

[53] 다양한 실시예에 따르면, 프로세서(120)는 보안 엘리먼트(172)로부터 보안 관련 서비스를 요청하는 명령에 대한 응답 신호를 수신할 수 있다. 프로세서(120)는 보안 엘리먼트(172)로부터의 응답 신호에 기초하여 보안 관련 서비스를 제공하거나, 보안 관련 서비스 제공 불가능함을 사용자에게 알릴 수 있다. 일 실시예에 따르면, 프로세서(120)는 응답 신호에 포함된 적어도 하나의 정보에 기초하여, 보안 엘리먼트(172)로부터 보안 관련 서비스가 허가(또는 승인)되었는지 여부를 결정할 수 있다. 프로세서(120)는 응답 신호에 보안 관련 서비스를 요청하는 명령에 대응하는 정보, 또는 보안 관련 서비스에 대한 허가(또는 승인)를 나타내는 정보가 포함된 경우, 적어도 하나의 정보에 기초하여 보안 관련 서비스를 제공할 수 있다. 프로세서(120)는 응답 신호에 보안 관련 서비스에 대한 비허가(또는 거부)를 나타내는 정보가 포함된 경우, 보안 관련 서비스를 제공할 수 없음을 나타내는 사용자 인터페이스가 제공되도록 표시 장치(160)를 제어할 수 있다. 보안 관련 서비스를 제공할 수 없음을 나타내는 사용자 인터페이스는, 보안 상태 정보를 포함할 수 있다. 예를 들어, 프로세서(120)는 보안 엘리먼트(172)로부터 수신된 응답 신호에 보안 관련 서비스에 대한 비허가(또는 거부)를 나타내는 정보와 보안 상태 정보가 포함된 경우, 보안 상태 정보를 포함하면서 보안 관련 서비스를 제공할 수 없음을

나타내는 사용자 인터페이스가 제공되도록 표시 장치(160)를 제어할 수 있다. 일 실시예에 따르면, 프로세서(120)는 보안 관련 서비스를 요청하는 명령에 대한 응답 신호가 지정된 시간 동안 수신되지 않는 경우, 보안 관련 서비스를 제공할 수 없음을 나타내는 사용자 인터페이스가 제공되도록 표시 장치(160)를 제어할 수 있다. 예를 들어, 프로세서(120)는 보안 엘리먼트(172)로 보안 관련 서비스를 요청하는 명령을 전송한 시점부터 지정된 시간 구간 이내에 보안 엘리먼트(172)로부터 응답 신호가 수신되지 않는 경우, 보안 관련 서비스를 제공할 수 없음을 나타내는 사용자 인터페이스가 제공되도록 표시 장치(160)를 제어할 수 있다. 일 실시예에 따르면, 보안 관련 서비스를 제공할 수 없음을 나타내는 사용자 인터페이스는, 보안 상태로 인해 보안 관련 서비스를 제공할 수 없음을 나타내는 정보를 포함할 수 있다.

[54] 다양한 실시예들에 따르면, 보안 엘리먼트(172)는 적어도 하나의 인터페이스를 통해 프로세서(120), 또는 근거리 통신 모듈(210)과 통신할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 프로세서(120), 또는 근거리 통신 모듈(210)에 의해 주기적, 또는 특정 시점에 활성화되어 동작할 수 있다.

[55] 다양한 실시예들에 따르면, 보안 엘리먼트(172)는 프로세서(120)로부터 보안 채널 프로토콜을 통해 보안 상태 정보를 수신하고, 수신된 보안 상태 정보를 보안 엘리먼트(172) 내부의 저장소에 저장할 수 있다. 예를 들어, 보안 상태 정보는, 보안 엘리먼트(172) 내부의 변경 불가능한(immutable) 영역에 저장될 수 있다. 보안 엘리먼트(172)는 이전 시점에 저장된 보안 상태 정보를 삭제하지 않고, 현재 시점에 프로세서(120)로부터 수신된 보안 상태 정보를 추가 저장할 수 있다. 예를 들어, 보안 엘리먼트(172)는 현재 시점의 보안 상태 정보와 과거 시점의 보안 상태 정보를 변경 불가능한 영역에 함께 저장할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 보안 상태 정보의 변경 이력 정보를 저장할 수 있다.

[56] 다양한 실시예들에 따르면, 보안 엘리먼트(172)는 보안 관련 서비스 요청 이벤트가 감지되면, 보안 엘리먼트(172) 내부의 저장소에 기 저장된 보안 상태 정보에 기반하여, 보안 관련 서비스를 제공할지 여부를 결정할 수 있다. 보안 엘리먼트(172)는 기 저장된 보안 상태 정보에 기초하여, 요청된 보안 관련 서비스에 대응하는 지정된 조건이 만족되는지 여부를 결정할 수 있다. 보안 엘리먼트(172)는 지정된 조건이 만족되는 경우, 보안 관련 서비스 제공하고, 지정된 조건이 만족되지 않는 경우, 보안 관련 서비스가 차단되도록 동작할 수 있다.

[57] 일 실시예에 따르면, 보안 엘리먼트(172)는 프로세서(120)로부터 보안 관련 서비스를 요청하는 명령과 제1 어플리케이션의 보안 상태 정보를 수신할 수 있다. 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 기반하여, 관련 어플릿을 실행할 수 있다. 예를 들어, 보안 관련 서비스 요청 명령은, 보안 관련 서비스 요청 명령을 생성한 제1 어플리케이션의 정보(예: 식별 정보), 또는 제1

어플리케이션에 대응되는 제1 어플릿의 정보(예: 식별 정보)를 포함할 수 있다. 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 포함된 정보에 기초하여, 제1 어플리케이션에 대응되는 제1 어플릿을 실행할 수 있다. 제1 어플리케이션이 결제 어플리케이션(payment application)인 경우, 제1 어플릿은 결제 어플릿(payment applet)일 수 있다. 보안 엘리먼트(172)는 제1 어플릿을 이용하여 보안 엘리먼트(172) 내부의 저장소에서 기 저장된 제1 어플리케이션의 보안 상태 정보를 획득할 수 있다. 기 저장된 제1 어플리케이션의 보안 상태 정보는, 제1 어플리케이션과 제1 어플리케이션에 대응되는 제1 어플릿이 전자 장치(101)에 저장되는 시점에 프로세서(120)로부터 보안 엘리먼트(172)에 제공됨으로써, 보안 엘리먼트(172) 내부의 저장소에 저장될 수 있다. 보안 엘리먼트(172)는 프로세서(120)로부터 수신된 제1 어플리케이션의 보안 상태 정보와 보안 엘리먼트(172) 내부의 저장소로부터 획득된 제1 어플리케이션의 보안 상태 정보를 비교할 수 있다. 보안 엘리먼트(172)는 프로세서(120)로부터 수신된 제1 어플리케이션의 보안 상태 정보와 보안 엘리먼트(172) 내부의 저장소로부터 획득된 제1 어플리케이션의 보안 상태 정보가 동일한 경우, 제1 어플릿을 이용하여 보안 관련 서비스를 요청하는 명령을 처리함으로써, 요청된 보안 관련 서비스가 제공되도록 제어할 수 있다. 보안 엘리먼트(172)는 프로세서(120)로부터 수신된 제1 어플리케이션의 보안 상태 정보와 보안 엘리먼트(172) 내부의 저장소로부터 획득된 제1 어플리케이션의 보안 상태 정보가 동일하지 않은 경우, 보안 관련 서비스 제공이 불가능한 것으로 결정하고 제1 어플릿에서 보안 관련 서비스를 요청하는 명령이 처리되지 않도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 프로세서(120)가 제1 어플리케이션을 이용하여 전송한 보안 관련 서비스 요청 명령을 정상적으로 처리하지 않고, 무시(또는 폐기)할 수 있다. 일실시에에 따르면, 제1 어플리케이션이 악의적인 목적으로 수정되거나 유사한 다른 어플리케이션으로 대체된 경우, 수신된 제1 어플리케이션의 보안 상태 정보와 보안 엘리먼트(172) 내부의 저장소로부터 획득된 제1 어플리케이션의 보안 상태 정보가 상이할 수 있다.

- [58] 일실시에에 따르면, 보안 엘리먼트(172)는 프로세서(120), 또는 근거리 통신 모듈(예: 도 2의 근거리 통신 모듈(210))을 통해 외부 전자 장치로부터 보안 관련 서비스를 요청하는 명령(또는 신호)을 수신할 수 있다. 보안 관련 서비스 요청 명령은, 보안 관련 서비스 요청 명령에 관련된 어플릿을 나타내는 정보(예: 식별 정보)를 포함할 수 있다. 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 포함된 정보에 기반하여, 관련된 어플릿인 제2 어플릿을 실행할 수 있다. 제2 어플릿은 교통 카드 어플릿(transit card applet)일 수 있다. 보안 엘리먼트(172)는 제2 어플릿을 이용하여 보안 엘리먼트(172) 내부의 저장소에서 기 저장된 보안 상태 정보를 획득할 수 있다. 보안 엘리먼트(172)는 제2 어플릿을 이용하여, 기 저장된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다. 예를 들어, 지정된 조건은, 전자 장치(101)에 멀웨어가 설치되지 않음을 나타내는

조건일 수 있다. 다른 예로, 지정된 조건은, 전자 장치(101)가 루팅되지 않고, 멀웨어가 설치되지 않음을 나타내는 조건일 수 있다. 또 다른 예로, 지정된 조건은, 보안 레벨 0을 포함할 수 있다. 이는 예시적인 것으로서, 본 발명의 다양한 실시예는 이에 한정되지 않는다. 보안 엘리먼트(172)는 기 저장된 보안 상태 정보가 지정된 조건을 만족하는 것으로 확인되는 경우, 제2 어플릿을 이용하여 보안 관련 서비스를 요청하는 명령을 처리함으로써, 요청된 보안 관련 서비스가 제공되도록 제어할 수 있다. 보안 엘리먼트(172)는 기 저장된 보안 상태 정보가 지정된 조건을 만족하지 않는 것으로 확인되는 경우, 보안 상태가 취약하여 보안 관련 서비스 제공이 불가능한 것으로 결정하고, 제2 어플릿에서 보안 관련 서비스를 요청하는 명령이 처리되지 않도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 2 어플릿을 이용하여 보안 관련 서비스 요청 명령을 무시(또는 폐기)할 수 있다.

- [59] 일실시예에 따르면, 보안 엘리먼트(172)는 보안 상태 정보와 보안 관련 서비스 요청 명령(또는 신호)이 수신된 인터페이스에 기초하여, 보안 관련 서비스 제공 여부를 결정할 수 있다. 예를 들어, 보안 엘리먼트(172)는 적어도 하나의 다른 구성 요소(예: 프로세서(120)) 또는 근거리 통신 모듈(210)과의 인터페이스에 관련된 보안 상태 정보가 지정된 조건을 만족하지 못하는 경우, 해당 인터페이스로부터 입력된 보안 관련 서비스 요청 명령을 무시하거나, 해당 인터페이스로부터의 신호 수신을 차단할 수 있다. 예컨대, 보안 상태 정보가 전자 장치(101)가 루팅되었고, 근거리 통신 모듈(210)을 통한 보안 엘리먼트(172)로의 접근 권한을 관리하는 접근 관리자(Access Rule Enforcer)가 위변조되었음을 나타내는 경우, 보안 엘리먼트(172)는 근거리 무선 통신 모듈(210)과의 인터페이스인 SWP의 보안이 취약하여 보안 관련 서비스 제공이 불가능한 것으로 결정할 수 있다. 보안 엘리먼트(172)는 SWP의 보안이 취약하여 보안 관련 서비스 제공이 불가능한 경우, SWP로부터 수신되는 보안 관련 서비스 요청 명령을 무시하거나 SWP로부터 신호가 수신되지 않도록 차단할 수 있다. 다른 예로, 보안 엘리먼트(172)는 적어도 하나의 다른 구성 요소와의 인터페이스에 관련된 보안 상태 정보가 지정된 조건을 만족하는 경우, 해당 인터페이스로부터 입력된 보안 관련 서비스 요청 명령을 정상적으로 처리함으로써, 요청된 보안 관련 서비스가 제공되도록 제어할 수 있다. 예컨대, 보안 상태 정보가 전자 장치(101)가 루팅되지 않았고, 근거리 통신 모듈(210)을 통한 보안 엘리먼트(172)로의 접근 권한을 관리하는 접근 관리자가 위변조되지 않은 상태를 나타내는 경우, 보안 엘리먼트(172)는 근거리 무선 통신 모듈(210)과의 인터페이스인 SWP의 보안에 문제가 없는 것으로 결정하고, SWP로부터 수신된 보안 관련 서비스 요청 명령을 정상적으로 처리할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)의 운영 시스템(220)은 보안 관련 서비스 요청 명령이 입력(또는 수신)되는 인터페이스를 식별할 수 있다. 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령이 입력되는 시점마다 보안

엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보를 확인하고, 확인된 보안 상태 정보와 보안 관련 서비스 요청 명령(또는 신호)이 수신된 인터페이스에 기초하여, 보안 관련 서비스 제공 여부를 결정할 수 있다.

- [60] 일실시예에 따르면, 보안 엘리먼트(172)는 프로세서(120)로부터 보안 관련 서비스를 요청하는 명령을 수신할 수 있다. 보안 엘리먼트(172)는 보안 관련 서비스를 요청하는 명령에 관련된 어플릿이 존재하지 않는 경우, 보안 엘리먼트(172)는 내부 저장소에 저장된 전자 장치(101)의 보안 상태 정보를 직접 확인하여 보안 관련 서비스 제공 여부를 결정할 수 있다. 예를 들어, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 기반하여, 관련 어플릿이 존재 여부를 결정할 수 있다. 예컨대, 보안 관련 서비스 요청 명령은, 보안 관련 서비스 요청 명령을 생성한 제3 어플리케이션의 정보(예: 식별 정보)를 포함할 수 있다. 보안 엘리먼트(172)는 제3 어플리케이션의 정보에 기초하여, 제3 어플리케이션에 대응되는 어플릿의 존재 여부를 결정할 수 있다. 제3 어플리케이션이 금융 관련 어플리케이션인 경우, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 포함된 어플리케이션 정보에 기초하여, 보안 엘리먼트(172) 내에 금융 관련 어플리케이션에 대응되는 관련 어플릿이 존재하지 않음을 확인할 수 있다. 관련 어플릿이 존재하지 않는 경우, 보안 엘리먼트(172)는 운영 시스템을 통해 보안 엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보를 직접 확인하고, 확인된 보안 상태 정보에 기초하여 보안 관련 서비스 제공 여부를 결정할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 내부 저장소에 저장된 전자 장치(101)의 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 보안 관련 서비스 제공 여부를 결정할 수 있다. 지정된 조건은, 예를 들어, 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 모두 보안 레벨 0 인 조건을 나타낼 수 있다. 이는 예시적인 것으로서, 본 발명의 다양한 실시예들은 이에 한정되지 않는다. 보안 엘리먼트(172)는 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 지정된 조건을 만족하는 경우, 보안 관련 서비스 요청 명령을 처리함으로써, 요청된 보안 관련 서비스가 제공되도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 지정된 조건을 만족하는 경우, 보안 관련 서비스 요청 명령에 의해 요청된 보안 관련 정보(예: 인증서 정보)를 포함하는 응답 신호를 프로세서(120)로 제공할 수 있다. 보안 엘리먼트(172)는 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 지정된 조건을 만족하지 못하는 경우, 보안 상태가 취약하여 보안 관련 서비스 제공이 불가능한 것으로 결정하고, 보안 관련 서비스 요청 명령을 정상적으로 처리하지 않고, 무시(또는 폐기)할 수 있다.

- [61] 일실시예에 따르면, 보안 엘리먼트(172)는 보안 관련 서비스를 요청하는

명령에 대한 응답 신호를 전송할 수 있다. 예를 들어, 보안 엘리먼트(172)는 요청된 보안 관련 서비스가 허가(또는 승인)되거나, 비허가(또는 거부)되었음을 나타내는 응답 신호를 프로세서(120)로 제공할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 요청된 보안 관련 서비스의 제공이 불가능한 것으로 결정된 경우, 요청된 보안 관련 서비스가 비허가되었음을 나타내는 정보와 보안 상태 정보를 포함하는 응답 신호를 프로세서(120)로 제공할 수 있다.

[62] 다양한 실시예에 따르면, 근거리 통신 모듈(210)은 근거리 무선 통신망을 통해 외부 전자 장치(예: 전자 장치(102))로부터 신호를 수신하고, 수신된 신호에 기초하여 보안 엘리먼트(172)의 활성 상태를 제어할 수 있다. 근거리 통신 모듈(210)은 외부 전자 장치로부터 수신된 신호가 지정된 보안 관련 서비스를 요청하는 신호인지 여부를 결정할 수 있다. 근거리 통신 모듈(210)은 외부 전자 장치로부터 수신된 신호가 지정된 보안 관련 서비스 요청 신호인 경우, 보안 엘리먼트(172)를 활성화시키고, 외부 전자 장치로부터 수신된 신호를 보안 엘리먼트(172)로 전달할 수 있다. 근거리 통신 모듈(210)은 보안 엘리먼트(172)로부터 응답 신호가 제공되는 경우, 제공된 응답 신호를 근거리 무선 통신망을 통해 외부 전자 장치로 전송할 수 있다.

[63] 다양한 실시예에 따르면, 근거리 통신 모듈(210)은 프로세서(120)로부터 보안 엘리먼트(172)로 전달할 신호를 수신하고, 수신된 신호를 보안 엘리먼트(172)로 전달할 수 있다. 근거리 통신 모듈(210)은 보안 엘리먼트(172)로 전달할 신호가 프로세서(120)로부터 수신된 시점에 보안 엘리먼트(172)가 비활성(또는 슬립) 상태인 경우, 보안 엘리먼트(172)가 활성화되도록 제어한 후, 활성화된 보안 엘리먼트(172)로 프로세서(120)로부터의 신호를 전달할 수 있다. 근거리 통신 모듈(210)은 보안 엘리먼트(172)로부터의 응답 신호를 프로세서(120)로 전달할 수 있다.

[64] 다양한 실시예에 따르면, 전자 장치(예: 도 1의 전자 장치(101))는, 상기 전자 장치(101)의 보안 상태 정보를 획득하는 프로세서(예: 도 1의 프로세서(120)), 및 상기 프로세서(120)의 제어에 의해 동작하고, 상기 프로세서(120)로부터 상기 전자 장치(101)의 보안 상태 정보를 수신하고, 수신된 전자 장치의 보안 상태 정보를 저장하는 저장소를 포함하는 보안 엘리먼트(예: 도 1의 보안 엘리먼트(172))를 포함하고, 상기 보안 엘리먼트(172)는, 보안 관련 서비스 요청 명령을 감지하고, 상기 저장소에서 상기 전자 장치의 보안 상태 정보를 획득하고, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시할 수 있다.

[65] 다양한 실시예에 따르면, 상기 전자 장치(101)의 보안 상태 정보는, 상기 전자 장치(101)의 루팅 여부에 대한 정보, 멀웨어(malware) 감지 여부에 대한 정보, 워런티 비트(warranty bit) 변경 여부에 대한 정보, 접근 관리자의 위변조 여부에 대한 정보, 상기 전자 장치의 시스템 영역에 대한 보안 상태 정보, 또는 상기 전자

- 장치에 설치된 어플리케이션에 대한 보안 상태 정보 중 적어도 하나를 포함할 수 있다.
- [66] 다양한 실시예에 따르면, 상기 보안 상태 정보는, 보안 레벨, 또는 보안 문제의 종류 중 적어도 하나를 나타낼 수 있다.
- [67] 다양한 실시예에 따르면, 상기 지정된 조건은, 상기 보안 관련 서비스 요청 명령의 종류에 기초하여 결정될 수 있다.
- [68] 다양한 실시예에 따르면, 상기 보안 관련 서비스를 요청하는 명령은, 상기 프로세서(120), 또는 외부 전자 장치(예: 도 1의 전자 장치(102))로부터 수신될 수 있다.
- [69] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)는, 상기 획득된 전자 장치(101)의 보안 상태 정보가 지정된 조건을 만족하는 경우, 상기 감지된 보안 관련 서비스 요청 명령을 정상적으로 처리하여 상기 명령에 대응되는 기능을 수행하고, 상기 획득된 전자 장치(101)의 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 상기 감지된 보안 관련 서비스 요청 명령을 무시할 수 있다.
- [70] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)는, 상기 프로세서(120)로부터 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 수신하고, 상기 저장소에 저장된 상기 전자 장치(101)의 보안 상태 정보에서 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 획득하고, 상기 수신된 어플리케이션의 보안 상태 정보와 상기 획득된 어플리케이션의 보안 상태 정보가 일치하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시할 수 있다.
- [71] 다양한 실시예에 따르면, 상기 프로세서(120)는, 상기 전자 장치에 상기 어플리케이션이 설치된 시점에 상기 어플리케이션의 보안 상태 정보를 결정하고, 상기 결정된 어플리케이션의 보안 상태 정보를 상기 보안 엘리먼트(172)로 전송하여 상기 보안 엘리먼트의 저장소에 저장되도록 제어할 수 있다.
- [72] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)는, 상기 전자 장치(101)의 보안 상태 정보가 접근 관리자의 위변조에 관련된 조건을 만족하는지 여부를 결정하고, 상기 전자 장치(101)의 보안 상태 정보가 접근 관리자의 위변조에 관련된 조건을 만족하지 않는 경우, 상기 감지된 보안 관련 서비스 요청 명령에 대응되는 인터페이스를 확인하고, 상기 확인된 인터페이스가 상기 위변조된 접근 관리자에 대응되는 인터페이스인 경우, 상기 감지된 보안 관련 서비스 요청 명령을 무시하고, 상기 확인된 인터페이스가 상기 위변조된 접근 관리자에 대응되는 인터페이스가 아닌 경우, 상기 감지된 보안 관련 서비스 요청 명령에 대응되는 기능을 수행할 수 있다.
- [73] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)는, 상기 보안 관련 서비스 요청 명령에 대한 응답 신호를 상기 프로세서(120), 또는 외부 전자 장치(102)로 제공하고, 상기 응답 신호는, 상기 보안 관련 서비스 요청 명령에 의해 요청된

정보, 보안 관련 서비스 요청 명령에 의해 수행된 기능에 대한 결과를 나타내는 정보, 또는 보안 관련 서비스에 대한 승인 여부를 나타내는 정보 중 적어도 하나를 포함할 수 있다.

[74] 도 3은 다양한 실시예들에 따른 전자 장치에서 보안 관련 서비스를 제공하는 흐름도(300)이다. 이하 실시예에서 각 동작들은 순차적으로 수행될 수도 있으나, 반드시 순차적으로 수행되는 것은 아니다. 예를 들어, 각 동작들의 순서가 변경될 수도 있으며, 적어도 두 동작들이 병렬적으로 수행될 수도 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다.

[75] 도 3을 참조하면, 다양한 실시예에 따른 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 301에서 보안 관련 서비스 요청 이벤트를 감지할 수 있다. 보안 관련 서비스는, 보안 엘리먼트(172)에 저장된 정보, 또는 보안 엘리먼트(172)에 설치된 어플릿을 이용하는 서비스일 수 있다. 예를 들어, 보안 관련 서비스는, 보안 엘리먼트(172)에 설치된 결제 어플릿, 또는 교통 카드 어플릿을 이용하는 서비스일 수 있다. 다른 예로, 보안 관련 서비스는 보안 엘리먼트(172)에 저장된 사용자의 신분 또는 자격 증명과 관련된 증명서 또는 관련 정보를 이용하는 서비스일 수 있다. 예컨대, 보안 엘리먼트(172)는 프로세서(예: 도 1의 프로세서(120))로부터 결제 어플리케이션을 이용한 결제 요청 명령이 수신되거나, 외부 전자 장치(예: 도 1의 전자 장치(102))로부터 교통 요금 결제 요청 명령이 수신되는 경우, 보안 관련 서비스 요청 이벤트가 발생된 것으로 결정할 수 있다. 다른 예로, 보안 엘리먼트(172)는 적어도 하나의 다른 구성 요소(예: 도 1의 프로세서(120), 또는 도 2의 근거리 무선 통신 모듈(210))에 대한 인터페이스(예: SPI, 또는 SWP)로부터 보안 관련 서비스 요청 명령이 수신되는 경우, 보안 관련 서비스 요청 이벤트가 발생된 것으로 결정할 수 있다. 또 다른 예로, 보안 엘리먼트(172)는 프로세서(120)로부터 은행 어플리케이션을 이용한 사용자 인증 요청 명령이 수신되는 경우, 보안 관련 서비스 요청 이벤트가 발생된 것으로 결정할 수 있다.

[76] 다양한 실시예에 따른 전자 장치(예: 보안 엘리먼트(172))는 동작 303에서 전자 장치의 보안 상태를 나타내는 보안 상태 정보를 획득할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 보안 엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보를 획득할 수 있다. 보안 상태 정보는, 예를 들어, 전자 장치(101)의 루팅 여부, 멀웨어(malware) 감지 여부, warranty bit 변경(broken) 여부, 보안 엘리먼트(172)에 대한 접근 관리자의 위변조 여부, 전자 장치(101)의 시스템 영역에 대한 보안 상태 정보, 전자 장치(101)에 설치된 어플리케이션에 대한 보안 상태 정보 중 적어도 하나를 포함할 수 있다. 보안 상태 정보는, 보안 레벨(또는 보안 수준)을 나타내거나, 보안 문제의 종류를 나타내는 형태로 구성될 수 있다. 예를 들어, 보안 레벨은 0레벨부터 N레벨까지의 단계로 차등적으로 미리 정의될 수 있다. 예컨대, "보안 레벨 N"은 보안 레벨이 가장 높은 단계이면서 전자 장치(101)가 안전한 상태이고, "보안 레벨 0"은 보안 레벨이 가장 낮은

단계이면서 전자 장치(101)의 보안 상태가 매우 취약한 상태로 정의될 수 있다. "보안 레벨 N-a"를 전자 장치(101)가 루팅된 상태이고, "보안 레벨 N-b"를 전자 장치(102)가 루팅되었으면서 보안 엘리먼트(172)에 대한 접근 관리자가 위변조된 상태로 정의될 수 있다. 다른 예로, 보안 상태 정보는, 루팅, 접근 관리자 위변조, 멀웨어(malware) 감지, 또는 워런티 비트 깨짐 중 적어도 하나의 보안 문제가 감지된 상태임을 나타내도록 정의될 수 있다. 보안 상태 정보에 대한 정의는 사업자, 및/또는 설계자에 의해 결정 및/또는 변경될 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 보안 엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보는 현재 시점의 보안 상태 정보와 과거 시점의 보안 상태 정보를 나타내는 보안 이력 정보를 포함할 수 있다. 일실시예에 따르면, 보안 상태 정보는, 프로세서(120)에 의해 실시간, 주기적인 시점, 또는 지정된 이벤트 발생 시점 중 적어도 하나의 시점에 획득되어 보안 엘리먼트(172) 내부의 저장소에 저장될 수 있다.

- [77] 다양한 실시예에 따른 전자 장치(예: 보안 엘리먼트(172))는 동작 305에서 보안 상태 정보에 기초하여 서비스 제공 여부를 결정할 수 있다. 보안 엘리먼트(172)는 획득된 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여 서비스 제공 여부를 결정할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 획득된 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 요청된 보안 관련 서비스의 제공이 불가능한 상태로 결정하고, 요청된 보안 관련 서비스가 제공되지 않도록 동작할 수 있다. 예컨대, 보안 엘리먼트(172)는 적어도 하나의 다른 구성 요소로부터 입력된 보안 관련 서비스 요청 명령을 무시 또는 폐기할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 획득된 보안 상태 정보가 지정된 조건을 만족하는 경우, 요청된 보안 관련 서비스의 제공이 가능한 상태로 결정하고, 요청된 보안 관련 서비스가 제공되도록 동작할 수 있다. 예컨대, 보안 엘리먼트(172)는 적어도 하나의 다른 구성 요소로부터 입력된 보안 관련 서비스 요청 명령을 정상적으로 처리할 수 있다. 일실시예에 따르면, 지정된 조건은, 감지된 보안 관련 서비스 요청 이벤트(또는 명령)의 종류에 기초하여 상이하게 결정될 수 있다. 예를 들어, 결제 어플릿을 이용하는 결제 요청 명령에 의해 보안 관련 서비스 요청 이벤트가 감지된 경우, 지정된 조건은 보안 엘리먼트(172) 내부의 저장소에 저장된 결제 어플리케이션의 보안 상태 정보(예: 해시 정보)와 프로세서(120)로부터 수신되는 결제 어플리케이션의 보안 상태 정보가 일치하는 조건을 포함할 수 있다. 다른 예로, 교통 카드 어플릿을 이용하는 교통 요금 결제 명령에 의해 보안 관련 서비스 요청 이벤트가 감지된 경우, 지정된 조건은 "루팅되지 않음, 및 멀웨어 감지되지 않음"을 나타내는 조건을 포함할 수 있다. 또 다른 예로, SWP 인터페이스를 통해 보안 관련 서비스 요청 명령이 수신되어 보안 관련 서비스 요청 이벤트가 감지된 경우, 지정된 조건은 "루팅되지 않음, 접근 관리자 위변조되지 않음"을 나타내는 조건을 포함할 수 있다. 또 다른 예로, 프로세서(120)로부터 은행 어플리케이션을 이용하여 생성된 사용자 인증 요청

명령이 수신되어 보안 관련 서비스 요청 이벤트가 감지된 경우, 지정된 조건은 현재 보안 레벨 및 과거 보안 레벨이 모두 0임을 나타내는 조건을 포함할 수 있다. 상술한 예시들은 본 발명의 이해를 돕기 위한 예시들로서, 본 발명은 이에 한정되지 않는다.

[78] 도 4는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보를 제공하는 흐름도(400)이다. 이하 설명되는 도 4의 동작들은 도 3의 동작 303의 상세한 동작 중 적어도 일부일 수 있고, 도 3의 동작들이 수행되기 이전에 수행되는 동작들일 수도 있다. 이하 실시예에서 각 동작들은 순차적으로 수행될 수도 있으나, 반드시 순차적으로 수행되는 것은 아니다. 예를 들어, 각 동작들의 순서가 변경될 수도 있으며, 적어도 두 동작들이 병렬적으로 수행될 수도 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다. 이하에서 도 4의 적어도 일부 동작은 도 5를 참조하여 설명할 것이다. 도 5는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보를 저장하는 예시도이다.

[79] 도 4를 참조하면, 다양한 실시예에 따른 전자 장치(예: 도 1의 프로세서(120))는 동작 401에서 전자 장치의 보안 상태를 감지할 수 있다. 프로세서(120)는 실시간, 주기적인 시점, 또는 지정된 이벤트 발생 시점(예: 부팅 시점, 소프트웨어 업데이트 시점, 어플리케이션 설치 시점) 중 적어도 하나에 해당하는 시점에 전자 장치의 보안 상태를 감지할 수 있다. 일 실시예에 따르면, 프로세서(120)는 전자 장치의 루팅 여부, 멀웨어(malware) 감지 여부, warranty bit가 변경(broken) 여부, 보안 엘리먼트(172)에 대한 접근 관리자의 위변조 여부, 전자 장치(101)의 시스템 영역에 대한 불법적 공격 감지 여부, 또는 전자 장치(101)에 설치된 어플리케이션에 대한 불법적 공격 감지 여부 중 적어도 하나를 감지할 수 있다. 프로세서(120)는 warranty bit와 같이, 당업자에게 공지된 기술을 이용하여 전자 장치의 보안 상태를 감지할 수 있다. 예컨대, 프로세서(120)는 전자 장치(101)의 부팅 시, warranty bit를 체크하여 부팅 이미지가 정상적인지 여부를 판단할 수 있다. 프로세서(120)는 warranty bit가 변경된 경우에 부팅 이미지가 비정상적인 것으로 결정하고, 전자 장치의 보안 상태를 루팅(rooting)된 상태로 결정할 수 있다. 이는 예시적인 것으로서, 본 발명은 이에 한정되지 않는다.

[80] 다양한 실시예에 따르면, 전자 장치(예: 프로세서(120))는 동작 403에서 감지된 전자 장치의 보안 상태를 나타내는 보안 상태 정보를 보안 엘리먼트(예: 도 1의 보안 엘리먼트(172))로 전달할 수 있다. 프로세서(120)는 전자 장치의 보안 상태를 나타내는 보안 상태 정보를 생성할 수 있다. 보안 상태 정보는, 상술한 도 3에서 설명한 정보들을 포함할 수 있다. 예를 들어, 프로세서(120)는 도 5에 도시된 바와 같이, 전자 장치(101)가 루팅되었는지 여부를 나타내는 보안 상태 정보(510)를 보안 채널(520)을 통해 보안 엘리먼트(172)로 전달할 수 있다.

[81] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 405에서 보안 상태 정보를 저장할 수 있다. 보안 엘리먼트(172)는 프로세서(120)로부터 보안 상태 정보가 수신되면, 수신된 보안 상태 정보를 보안 엘리먼트(172) 내부의

저장소에 저장할 수 있다. 예를 들어, 보안 엘리먼트(172)는 보안 엘리먼트(172) 내부의 변경 불가능한(immutable) 영역에 전자 장치의 보안 상태 정보를 저장할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 이전 시점에 저장된 보안 상태 정보를 삭제하지 않고, 현재 시점에 프로세서(120)로부터 수신된 보안 상태 정보를 추가 저장할 수 있다. 예를 들어, 보안 엘리먼트(172)는 현재 시점의 보안 상태 정보와 과거 시점의 보안 상태 정보를 변경 불가능한 영역에 함께 저장할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 보안 상태 정보의 변경 이력 정보를 저장할 수 있다. 예를 들어, 보안 엘리먼트(172)는 도 5에 도시된 바와 같이, 전자 장치(101)가 루팅되었는지 여부를 나타내는 보안 상태 정보(530)를 보안 엘리먼트(172) 내부의 저장소에 저장할 수 있다.

[82] 도 6은 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 흐름도(600)이다. 이하 설명되는 도 6의 동작들은 도 3의 동작 301, 303, 및 305의 상세한 동작들 중 적어도 일부일 수 있다. 이하 실시예에서 각 동작들은 순차적으로 수행될 수도 있으나, 반드시 순차적으로 수행되는 것은 아니다. 예를 들어, 각 동작들의 순서가 변경될 수도 있으며, 적어도 두 동작들이 병렬적으로 수행될 수도 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다. 이하에서 도 6의 적어도 일부 동작은 도 7을 참조하여 설명할 것이다. 도 7은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 예시도이다.

[83] 도 6을 참조하면, 다양한 실시예에 따른 전자 장치(예: 도 1의 프로세서(120))는 동작 601에서 제1 어플리케이션의 보안 관련 서비스 요청을 감지할 수 있다. 일실시예에 따르면, 프로세서(120)는 제1 입력에 기초하여 제1 어플리케이션을 실행하고, 실행 중인 제1 어플리케이션에 대한 제2 입력에 기초하여 보안 관련 서비스가 요청됨을 감지할 수 있다. 보안 관련 서비스는, 도 3의 동작 301에서 설명한 바와 같은 서비스를 포함할 수 있다. 예를 들어, 프로세서(120)는 결제 어플리케이션을 통해 결제 요청 이벤트가 감지되는 경우, 결제 어플리케이션을 이용한 보안 관련 서비스 요청이 발생된 것을 감지할 수 있다. 예컨대, 프로세서(120)는 도 7에 도시된 바와 같이, 결제 어플리케이션(710)이 실행된 상태에서 결제 어플리케이션을 통해 결제 요청 이벤트를 감지할 수 있다.

[84] 다양한 실시예에 따르면, 전자 장치(예: 도 1의 프로세서(120))는 동작 603에서 제1 어플리케이션의 보안 상태 정보와 보안 관련 서비스 요청 명령을 생성할 수 있다. 일실시예에 따르면, 프로세서(120)는 제1 어플리케이션의 보안 관련 서비스 요청이 감지되면, 현재 실행 중인 제1 어플리케이션의 보안 상태 정보를 생성하고, 제1 어플리케이션을 이용하여 보안 관련 서비스 요청 명령을 생성할 수 있다. 제1 어플리케이션의 보안 상태 정보는, 제1 어플리케이션의 무결성 및/또는 신뢰성 검증에 필요한 정보로, 예를 들어, 해시 정보를 포함할 수 있다. 일실시예에 따르면, 프로세서(120)는 생성된 제1 어플리케이션의 보안 상태

정보와 보안 관련 서비스 요청 명령을 보안 엘리먼트(172)로 전달할 수 있다. 예를 들어, 프로세서(120)는 도 7에 도시된 바와 같이, 결제 요청 명령(730)과 결제 어플리케이션의 보안 상태 정보(732)를 보안 엘리먼트(172)로 전달할 수 있다.

- [85] 다양한 실시예에 따르면, 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 605에서 기 저장된 제1 어플리케이션의 보안 상태 정보를 획득할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령이 수신되면, 보안 관련 서비스 요청 명령에 기반하여 제1 어플릿을 실행하고, 실행된 제1 어플릿을 이용하여 보안 엘리먼트(172) 내부의 저장소에 기 저장된 제1 어플리케이션의 보안 상태 정보를 획득할 수 있다. 예를 들어, 도 7에 도시된 바와 같이, 보안 엘리먼트(172)는 결제 요청 명령(730)이 수신되면, 결제 요청 명령에 기반하여 결제 어플릿(720)을 실행하고, 결제 어플릿(720)을 이용하여 보안 엘리먼트(172) 내부의 저장소에 저장된 결제 어플리케이션의 보안 상태 정보(740)를 확인 및 획득할 수 있다.
- [86] 다양한 실시예에 따르면, 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 607에서 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보를 비교하여 일치 여부를 결정할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 제1 어플릿을 이용하여 보안 엘리먼트(172) 내부의 저장소에 기 저장된 제1 어플리케이션의 보안 상태 정보와 프로세서(120)로부터 수신된 제1 어플리케이션의 보안 상태 정보를 비교하여 두 보안 상태 정보가 일치하는지 여부를 결정할 수 있다.
- [87] 다양한 실시예에 따르면, 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보가 일치하는 경우, 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 609에서 보안 관련 서비스 요청 명령에 대응되는 기능을 수행할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보가 일치하는 경우, 제1 어플리케이션의 무결성 및/또는 신뢰성이 검증된 것으로 결정하고, 제1 어플릿을 이용하여 보안 관련 서비스 요청 명령을 정상적으로 처리할 수 있다. 예를 들어, 도 7에 도시된 바와 같이, 보안 엘리먼트(172)는 결제 어플릿(720)을 이용하여 결제 요청 명령에 대응하는 결제 기능을 수행할 수 있다.
- [88] 다양한 실시예에 따르면, 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보가 일치하지 않는 경우, 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 611에서 보안 관련 서비스 요청 명령을 무시할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보가 일치하지 않는 경우, 제1 어플리케이션의 무결성 및/또는 신뢰성이 없는 것으로 결정하고, 제1 어플릿을 이용하여 보안 관련 서비스 요청 명령이 처리되지

않도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 프로세서(120)로부터 수신된 결제 요청 명령을 무시 또는 폐기할 수 있다.

- [89] 도 8은 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 신호 흐름도(800)이다. 이하 설명되는 도 8의 동작들은 도 6의 동작들 중 적어도 일부일 수 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다.
- [90] 도 8을 참조하면, 다양한 실시예에 따른 전자 장치(101)의 프로세서(예: 도 1의 프로세서(120))는 동작 810에서 제1 어플리케이션을 이용한 보안 관련 서비스 요청을 감지할 수 있다. 일 실시예에 따르면, 전자 장치(101)의 프로세서(120)는 실행 중인 제1 어플리케이션에 대한 사용자 입력에 기초하여 보안 관련 서비스가 요청됨을 감지할 수 있다. 보안 관련 서비스 요청을 감지하는 동작은 도 6의 동작 601에서 설명한 바와 같은 동작을 포함할 수 있다. 이하에서, 점선으로 표시된 동작은 실시예에 따라 생략될 수 있다.
- [91] 다양한 실시예에 따르면, 전자 장치(101)의 프로세서(120)는 동작 812에서 제1 어플리케이션의 보안 상태 정보와 보안 관련 서비스 요청 명령을 보안 엘리먼트(172)로 전송할 수 있다. 일 실시예에 따르면, 프로세서(120)는 제1 어플리케이션을 이용한 보안 관련 서비스 요청이 감지되면, 제1 어플리케이션을 이용하여 보안 관련 서비스 요청 명령을 생성하고, 제1 어플리케이션의 보안 상태 정보(예: 해시 정보)를 생성할 수 있다. 프로세서(120)는 생성된 보안 관련 서비스 요청 명령 및 제1 어플리케이션의 보안 상태 정보를 보안 엘리먼트(172)로 전송할 수 있다.
- [92] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 814에서 기 저장된 제1 어플리케이션의 보안 상태 정보를 획득할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령 및 제1 어플리케이션의 보안 상태 정보가 수신되면, 수신된 보안 관련 서비스 요청 명령에 기반하여 제1 어플릿을 실행하고, 실행된 제1 어플릿을 이용하여 보안 엘리먼트(172) 내부의 저장소에 기 저장된 제1 어플리케이션의 보안 상태 정보를 획득할 수 있다.
- [93] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 816에서 기 저장된 제1 어플리케이션의 보안 상태 정보와 수신된 제1 어플리케이션의 보안 상태 정보를 비교하여 일치 여부를 결정할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 제1 어플릿을 이용하여 보안 엘리먼트(172) 내부의 저장소에 기 저장된 제1 어플리케이션의 보안 상태 정보와 프로세서(120)로부터 수신된 제1 어플리케이션의 보안 상태 정보를 비교하여 두 보안 상태 정보가 일치하는지 여부를 결정할 수 있다.
- [94] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 818에서 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보의 일치 여부에 기초하여, 보안 관련 서비스 요청 명령에

대응되는 기능을 수행하거나, 보안 관련 서비스 요청 명령을 무시할 수 있다. 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보가 일치하는 경우, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 대응되는 기능을 수행할 수 있다. 기 저장된 제1 어플리케이션의 보안 상태 정보와 생성된 제1 어플리케이션의 보안 상태 정보가 일치하지 않는 경우, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령을 무시할 수 있다.

[95] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 820에서 보안 관련 서비스 요청에 대한 응답 신호를 프로세서(120)로 전달할 수 있다. 응답 신호는, 보안 관련 서비스 요청 명령에 의해 요청된 정보, 보안 관련 서비스 요청 명령에 의해 수행된 기능에 대한 결과를 나타내는 정보, 또는 보안 관련 서비스의 허가(또는 승인) 여부를 나타내는 정보 중 적어도 하나를 포함할 수 있다.

[96] 도 9는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 무선 인터페이스를 통한 서비스를 제공하는 흐름도(900)이다. 이하 설명되는 도 9의 동작들은 도 3의 동작 301, 303, 및 305의 상세한 동작들 중 적어도 일부일 수 있다. 이하 실시예에서 각 동작들은 순차적으로 수행될 수도 있으나, 반드시 순차적으로 수행되는 것은 아니다. 예를 들어, 각 동작들의 순서가 변경될 수도 있으며, 적어도 두 동작들이 병렬적으로 수행될 수도 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다. 이하에서 도 9의 적어도 일부 동작은 도 10을 참조하여 설명할 것이다. 도 10은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 어플리케이션을 이용한 보안 관련 서비스를 제공하는 예시도이다.

[97] 도 9를 참조하면, 다양한 실시예에 따른, 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 901에서 외부 전자 장치로부터의 보안 관련 서비스 요청을 감지할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 프로세서(120), 또는 근거리 무선 통신 모듈(예: 도 2의 (210))을 통해 외부 전자 장치로부터 송신된 보안 관련 서비스 요청 명령(또는 신호)을 수신할 수 있다. 예를 들어, 도 10에 도시된 바와 같이, 보안 엘리먼트(172)는 프로세서(120), 또는 근거리 통신 모듈(210)을 통해 외부 전자 장치로부터 교통 요금 결제를 요청하는 신호를 수신할 수 있다.

[98] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 903에서 기 저장된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 보안 관련 서비스 요청 신호에 관련된 어플릿을 이용하여 기 저장된 보안 상태 정보를 확인하고, 기 저장된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다. 보안 관련 서비스 요청 신호는, 보안 관련 서비스 요청 명령에 관련된 어플릿을 나타내는 정보(예: 식별 정보)를 포함할 수 있다. 보안 엘리먼트(172)는 외부 전자 장치로부터 수신된 보안 관련 서비스 요청 신호에 포함된 정보에 기반하여, 관련된 어플릿을

실행할 수 있다. 예를 들어, 도 10에 도시된 바와 같이, 보안 엘리먼트(172)는 근거리 통신 모듈(210)을 통해 외부 전자 장치로부터 교통 요금 결제를 요청하는 신호가 수신되면, 수신된 교통 요금 결제 요청 신호에 기반하여 교통 카드 어플릿(1020)을 실행할 수 있다. 보안 엘리먼트(172)는 지정된 조건이 "멀웨어가 감지되지 않음"으로 설정된 경우, 교통 카드 어플릿(1020)을 이용하여 보안 엘리먼트(172) 내부의 저장소에 기 저장된 보안 상태 정보에서 멀웨어 감지 여부를 나타내는 정보(1030)를 확인하여 지정된 조건이 만족되는지 여부를 확인할 수 있다. 지정된 조건은, 예시적인 것으로서, 설계자 및/또는 사업자에 의해 설정 및 변경될 수 있다. 예를 들어, 지정된 조건은, 보안 레벨, 루팅 여부, 접근 관리자 위변조 여부 중 적어도 하나에 대한 조건을 포함할 수 있다.

[99] 다양한 실시예에 따르면, 기 저장된 보안 상태 정보가 지정된 조건을 만족하는 경우, 전자 장치(예: 보안 엘리먼트(172))는 동작 905에서 보안 관련 서비스 요청에 대응되는 응답 신호를 외부 전자 장치로 송신할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 기 저장된 보안 상태 정보가 지정된 조건을 만족하는 것으로 확인되는 경우, 보안 상태가 강인한 것으로 판단하고 보안 관련 서비스 제공이 가능한 것으로 결정할 수 있다. 보안 엘리먼트(172)는 제2 어플릿을 이용하여 보안 관련 서비스를 요청하는 명령을 정상적으로 처리하여, 보안 관련 서비스 요청 명령에 대한 응답 신호가 외부 전자 장치로 전송되도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 보안 상태 정보가 멀웨어가 감지되지 않음을 나타내는 경우, 지정된 조건을 만족하는 것으로 결정하고, 교통 카드 어플릿(1020)을 이용하여 근거리 무선 통신망을 통한 교통 요금 결제 응답 신호가 송신되도록 제어할 수 있다.

[100] 다양한 실시예에 따르면, 기 저장된 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 전자 장치(예: 보안 엘리먼트(172))는 동작 907에서 보안 관련 서비스 요청을 무시할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 기 저장된 보안 상태 정보가 지정된 조건을 만족하지 않는 것으로 확인되는 경우, 보안 상태가 취약하여 보안 관련 서비스 제공이 불가능한 것으로 결정하고, 제2 어플릿에서 보안 관련 서비스를 요청하는 명령이 처리되지 않도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 보안 상태 정보가 멀웨어가 감지됨을 나타내는 경우, 지정된 조건을 만족하지 않는 것으로 결정하고, 교통 카드 어플릿(1020)을 이용한 근거리 무선 통신망을 통한 교통 요금 결제 요청이 처리되지 않도록 제어할 수 있다. 예컨대, 보안 엘리먼트(172)는 근거리 무선 통신 모듈(예: 도 2의 근거리 무선 통신 모듈(210))을 통해 송수신되는 패킷을 감시 및 로깅하기 위한 멀웨어가 설치되었으므로, 교통 카드 어플릿(1020)을 이용하여 교통 요금 결제 요청에 대한 응답 신호가 외부 전자 장치로 송신되지 않도록 제어할 수 있다. 다른 예로, 보안 엘리먼트(172)는 근거리 무선 통신 모듈(210)을 통해 송수신되는 패킷을 감시 및 로깅하기 위한 멀웨어가 설치되었으므로, 교통 카드 어플릿(1020)을 이용하여 결제 요청을 거절하는 응답

신호가 근거리 통신망을 통해 외부 전자 장치로 전송되도록 제어할 수 있다. 결제 요청을 거절하는 응답 신호는, 결제 요청에 대한 거절 사유를 나타내는 정보를 포함할 수 있다. 예를 들어, 결제 요청을 거절하는 응답 신호는 보안 문제 감지(예: 멀웨어 감지)를 나타내는 에러 코드를 포함할 수 있다.

[101] 도 11은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 통신 인터페이스를 이용한 보안 엘리먼트에 대한 접근을 제어하는 흐름도(1100)이다. 이하 설명되는 도 11의 동작들은 도 3의 동작 301, 303, 및 305의 상세한 동작들 중 적어도 일부일 수 있다. 이하 실시예에서 각 동작들은 순차적으로 수행될 수도 있으나, 반드시 순차적으로 수행되는 것은 아니다. 예를 들어, 각 동작들의 순서가 변경될 수도 있으며, 적어도 두 동작들이 병렬적으로 수행될 수도 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다. 이하에서 도 11의 적어도 일부 동작은 도 12를 참조하여 설명할 것이다. 도 12는 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 통신 인터페이스를 이용한 보안 엘리먼트에 대한 접근을 제어하는 예시도이다.

[102] 도 11을 참조하면, 다양한 실시예에 따른 전자 장치(예: 도 1의 보안 엘리먼트(172))는 동작 1101에서 접근 관리자의 위변조가 감지됨을 나타내는 보안 상태 정보를 획득할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 내부 저장소에 기 저장된 보안 상태 정보에서 접근 관리자가 위변조되었음을 나타내는 보안 상태 정보를 획득할 수 있다. 예를 들어, 도 12에 도시된 바와 같이, 보안 엘리먼트(172)의 운영 시스템은 기 저장된 보안 상태 정보에서 I2C 및 SWP 인터페이스에 대응되는 접근 관리자가 위변조되었음을 나타내는 정보(1242)를 획득할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 프로세서(120)로부터 보안 엘리먼트(172)에 대한 접근 관리자가 위변조되었음을 나타내는 보안 상태 정보를 수신할 수 있다. 접근 관리자는, 보안 엘리먼트(172)에 대한 접근을 제어하기 위한 접근 권한을 포함할 수 있다.

[103] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 1103에서 위변조된 접근 관리자에 대응되는 인터페이스를 차단 인터페이스로 설정할 수 있다. 보안 엘리먼트(172)는 접근 관리자 위변조에 대응되는 인터페이스를 확인하고, 확인된 인터페이스를 차단 인터페이스로 설정할 수 있다. 예를 들어, 도 12에 도시된 바와 같이, 보안 엘리먼트(172)는 적어도 하나의 다른 구성 요소들과 보안 엘리먼트(172) 사이의 인터페이스인, SWP(1224), SPI(1222), 또는 ISO(1232) 중에서 위변조된 접근 관리자에 대응되는 인터페이스가 SWP(1224)임을 확인하고, SWP(1224)를 통신을 차단할 차단 인터페이스로 설정할 수 있다.

[104] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 1105에서 보안 관련 서비스를 요청하는 명령이 감지되는지 여부를 결정할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)의 운영 시스템은 적어도 하나의 인터페이스를 통해 보안 엘리먼트(172)로 입력되는 보안 관련 서비스 요청

명령을 감지할 수 있다.

- [105] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 1107에서 명령 감지에 이용된 인터페이스가 차단 인터페이스인지 여부를 결정할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)의 운영 시스템은 보안 엘리먼트(172)로 입력되는 보안 관련 서비스 요청 명령이 감지되면, 보안 관련 서비스 요청 명령이 입력된 인터페이스가 차단 인터페이스인지 여부를 결정할 수 있다. 예를 들어, 도 12에 도시된 바와 같이, 보안 엘리먼트(172)는 감지된 보안 관련 서비스 요청 명령이 차단 인터페이스로 설정된 SWP(1224)를 통해 입력되었는지 여부를 결정할 수 있다.
- [106] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 명령 감지에 이용된 인터페이스가 차단 인터페이스가 아닌 경우, 동작 1109에서 감지된 명령을 정상적으로 처리할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)의 운영 시스템은 보안 관련 서비스 요청 명령이 차단 인터페이스가 아닌 다른 인터페이스를 통해 입력된 경우, 보안 엘리먼트(172)는 입력된 보안 관련 서비스 요청 명령을 정상적으로 처리할 수 있다. 예를 들어, 도 12에 도시된 바와 같이, 보안 엘리먼트(172)의 운영 시스템은 보안 관련 서비스 요청 명령이 SPI(1222), 또는 ISO(1232)를 통해 입력된 경우, 입력된 보안 관련 서비스 요청 명령을 정상적으로 처리할 수 있다.
- [107] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 명령 감지에 이용된 인터페이스가 차단 인터페이스인 경우, 동작 1111에서 감지된 명령을 무시할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)의 운영 시스템은 보안 관련 서비스 요청 명령이 차단 인터페이스를 통해 입력된 경우, 보안 엘리먼트(172)는 입력된 보안 관련 서비스 요청 명령을 처리하지 않고 무시할 수 있다. 예를 들어, 도 12에 도시된 바와 같이, 접근 관리자(1210)가 위변조된 경우, 허가되지 않은 어플리케이션이 위변조된 접근 관리자를 이용하여 보안 엘리먼트(172)로 접근을 시도할 수 있으므로, 보안 엘리먼트(172)는 SWP(1224)를 통해 입력되는 보안 관련 서비스 요청 명령을 무시할 수 있다.
- [108] 도 13은 다양한 실시예들에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 정보를 제공하는 흐름도(1300)이다. 이하 설명되는 도 13의 동작들은 도 3의 동작 301, 303, 및 305의 상세한 동작들 중 적어도 일부일 수 있다. 이하 실시예에서 각 동작들은 순차적으로 수행될 수도 있으나, 반드시 순차적으로 수행되는 것은 아니다. 예를 들어, 각 동작들의 순서가 변경될 수도 있으며, 적어도 두 동작들이 병렬적으로 수행될 수도 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다. 이하에서 도 13의 적어도 일부 동작은 도 14를 참조하여 설명할 것이다. 도 14는 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 정보를 제공하는 예시도이다.
- [109] 도 13을 참조하면, 다양한 실시예에 따른 전자 장치(예: 도 1의 프로세서(120))는 동작 1301에서 제3 어플리케이션의 보안 관련 서비스 요청을

감지할 수 있다. 일실시예에 따르면, 프로세서(120)는 제1 입력에 기초하여 제3 어플리케이션을 실행하고, 실행 중인 제3 어플리케이션에 대한 제2 입력에 기초하여 보안 관련 서비스가 요청됨을 감지할 수 있다. 보안 관련 서비스는, 도 3의 동작 301에서 설명한 바와 같은 서비스를 포함할 수 있다. 예를 들어, 프로세서(120)는 금융 관련 어플리케이션을 통해 인증 요청 이벤트가 감지되는 경우, 금융 관련 어플리케이션을 이용한 보안 관련 서비스 요청이 발생된 것을 감지할 수 있다. 예컨대, 프로세서(120)는 도 14에 도시된 바와 같이, 금융 관련 어플리케이션(1410)이 실행된 상태에서 사용자 인증 요청 이벤트를 감지할 수 있다.

[110] 다양한 실시예에 따르면, 전자 장치(예: 프로세서(120))는 동작 1303에서 보안 관련 서비스 요청 명령을 생성할 수 있다. 일실시예에 따르면, 프로세서(120)는 제3 어플리케이션을 이용하여 보안 관련 서비스 요청 명령을 생성할 수 있다. 예를 들어, 프로세서(120)는 금융 관련 어플리케이션을 이용하여 사용자 인증 요청 명령을 생성할 수 있다. 일실시예에 따르면, 보안 관련 서비스 요청 명령은 금융 관련 어플리케이션의 정보(예: 식별 정보)를 포함할 수 있다.

[111] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 1305에서 기 저장된 보안 상태 정보를 획득할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 프로세서(120)로부터 보안 관련 서비스 요청 명령이 수신되면, 보안 엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보를 획득할 수 있다. 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 기반하여, 관련 어플릿이 존재하지 않음을 결정할 수 있다. 예를 들어, 보안 관련 서비스 요청 명령은, 보안 관련 서비스 요청 명령에 포함된 정보에 기초하여, 제3 어플리케이션에 대응되는 어플릿이 존재하지 않음을 결정할 수 있다. 보안 엘리먼트(172)는 운영 시스템을 이용하여 보안 엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보를 획득할 수 있다.

[112] 다양한 실시예에 따르면, 전자 장치(예: 보안 엘리먼트(172))는 동작 1307에서 기 저장된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다. 일 실시예에 따르면, 보안 엘리먼트(172)는 내부 저장소에 저장된 전자 장치(101)의 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 보안 관련 서비스 제공 여부를 결정할 수 있다. 예컨대, 도 14에 도시된 바와 같이, 보안 엘리먼트(172)는 내부 저장소에서 현재 보안상태 정보(1422)와 보안 이력 정보(1420)를 획득하고, 획득된 정보들이 지정된 조건을 만족하는지 여부를 결정할 수 있다. 지정된 조건은, 예를 들어, 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 모두 보안 레벨 0인 조건을 나타낼 수 있다. 이는 예시적인 것으로서, 본 발명의 다양한 실시예들은 이에 한정되지 않는다. 예를 들어, 지정된 조건은, 루팅 여부 및 멀웨어 감지 여부에 대한 조건일 수 있다. 보안 엘리먼트(172)는 지정된 조건에 기초하여, 보안 엘리먼트(172) 내부의

저장소에서 보안 상태 정보를 획득하고, 획득된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다.

- [113] 다양한 실시예에 따르면, 기 저장된 보안 상태 정보가 지정된 조건을 만족하는 경우, 전자 장치(예: 보안 엘리먼트(172))는 동작 1309에서 보안 관련 서비스 요청에 대한 응답 신호를 제공할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 현재 보안 상태 정보와 보안 이력 정보가 지정된 조건을 만족하는 경우, 보안 관련 서비스 요청 명령을 처리함으로써, 요청된 보안 관련 서비스가 제공되도록 제어할 수 있다. 예를 들어, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령에 의해 요청된 보안 관련 정보(예: 인증서 정보)를 포함하는 응답 신호를 프로세서(120)로 제공할 수 있다.
- [114] 다양한 실시예에 따르면, 기 저장된 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 전자 장치(예: 보안 엘리먼트(172))는 동작 1311에서 보안 관련 서비스 요청 명령을 무시할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 현재 보안 상태 정보와 보안 이력 정보가 지정된 조건을 만족하지 않는 경우, 보안 관련 서비스 요청 명령을 무시함으로써, 요청된 보안 관련 서비스가 제공되지 않도록 제어할 수 있다. 보안 엘리먼트(172)는 과거 보안 상태 정보를 나타내는 보안 이력 정보와 현재 보안 상태 정보가 지정된 조건을 만족하지 못하는 경우, 보안 상태로 인해 서비스가 불가능함을 나타내는 응답 신호를 프로세서(120)로 제공할 수 있다.
- [115] 도 15는 다양한 실시예에 따른 전자 장치에서 전자 장치의 보안 상태 정보에 기초하여 보안 관련 정보를 제공하는 신호 흐름도(1500)이다. 이하 설명되는 도 15의 동작들은 도 13의 동작들 중 적어도 일부일 수 있다. 여기에서, 전자 장치는 도 1의 전자 장치(101)일 수 있다. 이하에서, 점선으로 표시된 동작은 실시예에 따라 생략될 수 있다.
- [116] 도 15를 참조하면, 다양한 실시예에 따른 전자 장치(101)의 프로세서(예: 도 1의 프로세서(120))는 동작 1510에서 제3 어플리케이션을 이용한 보안 관련 서비스 요청을 감지할 수 있다. 일실시예에 따르면, 전자 장치(101)의 프로세서(120)는 실행 중인 제3 어플리케이션에 대한 사용자 입력에 기초하여 보안 관련 서비스가 요청됨을 감지할 수 있다. 보안 관련 서비스 요청을 감지하는 동작은 도 13의 동작 1301에서 설명한 바와 같은 동작을 포함할 수 있다.
- [117] 다양한 실시예에 따르면, 전자 장치(101)의 프로세서(120)는 동작 1512에서 보안 관련 서비스 요청 명령을 보안 엘리먼트(예: 도 1의 보안 엘리먼트(172))로 전송할 수 있다. 일실시예에 따르면, 프로세서(120)는 제3 어플리케이션을 이용한 보안 관련 서비스 요청이 감지되면, 제3 어플리케이션을 이용하여 보안 관련 서비스 요청 명령을 생성하고, 생성된 보안 관련 서비스 요청 명령을 보안 엘리먼트(172)로 전송할 수 있다.
- [118] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 1514에서 기 저장된 보안 상태 정보를 획득할 수 있다. 일실시예에 따르면, 보안

엘리먼트(172)는 프로세서(120)로부터 보안 관련 서비스 요청 명령이 수신되면, 수신된 보안 관련 서비스 요청 명령에 기반하여, 관련 어플릿이 존재하지 않음을 결정할 수 있다. 예를 들어, 보안 관련 서비스 요청 명령은, 보안 관련 서비스 요청 명령에 포함된 정보에 기초하여, 제3 어플리케이션에 대응되는 어플릿이 존재하지 않음을 결정할 수 있다. 보안 엘리먼트(172)는 운영 시스템을 이용하여 보안 엘리먼트(172) 내부의 저장소에 저장된 보안 상태 정보를 획득할 수 있다. 예를 들어, 보안 엘리먼트(172)는 내부 저장소에서 현재 보안 상태 정보와 보안 이력 정보를 포함하는 보안 상태 정보를 획득할 수 있다.

[119] 다양한 실시예에 따르면, 전자 장치(101)의 보안엘리먼트(172)는 동작 1516에서 기 저장된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다. 일실시예에 따르면, 보안 엘리먼트(172)는 현재 보안 상태 정보와 보안 이력 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다. 지정된 조건은, 예를 들어, 현재 보안 상태 정보와 보안 이력 정보가 모두 보안 레벨 0인 조건을 나타낼 수 있다. 이는 예시적인 것으로서, 본 발명의 다양한 실시예들은 이에 한정되지 않는다. 예를 들어, 지정된 조건은, 루팅 여부 및 멀웨어 감지 여부에 대한 조건일 수 있다. 보안 엘리먼트(172)는 보안 엘리먼트(172) 내부의 저장소에서 지정된 조건에 관련된 보안 상태 정보를 획득하고, 획득된 보안 상태 정보가 지정된 조건을 만족하는지 여부를 결정할 수 있다.

[120] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 1518에서 기 저장된 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 보안 관련 서비스를 제공하거나, 보안 관련 서비스 요청 명령을 무시하도록 결정할 수 있다. 기 저장된 보안 상태 정보가 지정된 조건을 만족하는 경우, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령을 정상적으로 처리하여 요청된 보안 관련 서비스가 제공되도록 할 수 있다. 기 저장된 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 보안 엘리먼트(172)는 보안 관련 서비스 요청 명령을 무시하여 요청된 보안 관련 서비스가 제공되지 않도록 할 수 있다.

[121] 다양한 실시예에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 동작 1520에서 서비스 요청에 대한 응답 신호를 프로세서(120)로 전달할 수 있다. 응답 신호는, 보안 관련 서비스 요청 명령에 의해 요청된 정보, 보안 관련 서비스 요청 명령에 의해 수행된 기능에 대한 결과를 나타내는 정보, 또는 보안 관련 서비스의 허가(또는 승인) 여부를 나타내는 정보 중 적어도 하나를 포함할 수 있다.

[122] 상술한 다양한 실시예들에서는, 전자 장치(101)의 보안 엘리먼트(172)에 전자 장치(101)의 보안 상태를 나타내는 보안 상태 정보를 저장하고, 이를 이용하여 보안 관련 서비스 제공 여부를 결정하는 것에 대해 설명하였다. 그러나, 다양한 실시예들에 따르면, 전자 장치(101)의 보안 엘리먼트(172)는 적어도 하나의 외부 전자 장치(예: 도 1의 전자 장치(102))의 보안 상태 정보를 저장할 수 있다. 예를

들어, 보안 엘리먼트(172)는 적어도 하나의 외부 전자 장치(102)의 루팅 여부, 적어도 하나의 외부 전자 장치(102)의 멀웨어 감지 여부, 적어도 하나의 외부 전자 장치(102)의 warranty bit의 변경 여부, 적어도 하나의 외부 전자 장치(102)의 보안 엘리먼트(172)에 대한 접근 관리자의 위변조 여부, 적어도 하나의 외부 전자 장치(102)의 시스템 영역에 대한 보안 상태 정보, 또는 적어도 하나의 외부 전자 장치(102)에 설치된 어플리케이션에 대한 보안 상태 정보 중 적어도 하나를 저장할 수 있다. 전자 장치(101)는 프로세서(120) 및/또는 통신 모듈(190)을 통해 적어도 하나의 외부 전자 장치로부터 보안 관련 서비스 요청 명령(또는 신호)을 수신하고, 보안 엘리먼트(172)를 통해 보안 엘리먼트(172) 내부의 저장소에 기 저장된 적어도 하나의 외부 전자 장치의 보안 상태 정보에 기초하여, 적어도 하나의 외부 전자 장치로부터 요청된 보안 관련 서비스를 제공할지 여부를 결정할 수 있다. 예를 들어, 전자 장치(101)의 보안 엘리먼트(172)는 내부의 저장소에 기 저장된 적어도 하나의 외부 전자 장치의 보안 상태 정보에 기초하여, 보안 관련 서비스 요청 명령을 정상적으로 처리하거나, 무시할 수 있다.

- [123] 다양한 실시예에 따르면, 전자 장치(예: 도 1의 전자 장치(101))의 동작 방법은, 프로세서(예: 도 1의 프로세서(120))에서, 상기 전자 장치의 보안 상태 정보를 획득하는 동작, 상기 프로세서(120)의 제어에 의해 동작하는 보안 엘리먼트에서, 상기 전자 장치의 보안 상태 정보를 상기 보안 엘리먼트(예: 도 1의 보안 엘리먼트(172)) 내부의 저장소에 저장하는 동작, 상기 보안 엘리먼트(172)에서, 보안 관련 서비스 요청 명령을 감지하는 동작, 상기 보안 엘리먼트(172)에서 상기 내부의 저장소에 저장된 상기 전자 장치의 보안 상태 정보를 획득하는 동작, 및 상기 보안 엘리먼트(172)에서, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작을 포함할 수 있다.
- [124] 다양한 실시예에 따르면, 상기 전자 장치의 보안 상태 정보는, 상기 전자 장치의 루팅 여부에 대한 정보, 멀웨어(malware) 감지 여부에 대한 정보, 위런티 비트(warranty bit) 변경 여부에 대한 정보, 접근 관리자의 위변조 여부에 대한 정보, 상기 전자 장치의 시스템 영역에 대한 보안 상태 정보, 또는 상기 전자 장치에 설치된 어플리케이션에 대한 보안 상태 정보 중 적어도 하나를 포함할 수 있다.
- [125] 다양한 실시예에 따르면, 상기 보안 상태 정보는, 보안 레벨, 또는 보안 문제의 종류 중 적어도 하나를 나타낼 수 있다.
- [126] 다양한 실시예에 따르면, 상기 지정된 조건은, 상기 보안 관련 서비스 요청 명령의 종류에 기초하여 결정될 수 있다.
- [127] 다양한 실시예에 따르면, 상기 보안 관련 서비스를 요청하는 명령은, 상기 프로세서(120), 또는 외부 전자 장치(예: 도 1의 전자 장치(102))로부터 수신될 수 있다.

- [128] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작은, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는 경우, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령을 정상적으로 처리하여 상기 명령에 대응되는 기능을 수행하는 동작, 및 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령을 무시하는 동작을 포함할 수 있다.
- [129] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)에서, 상기 프로세서(120)로부터 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 수신하는 동작을 더 포함하며, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작은, 상기 보안 엘리먼트(172)에서, 획득된 보안 상태 정보에서 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 확인하는 동작, 상기 보안 엘리먼트(172)에서, 상기 수신된 어플리케이션의 보안 상태 정보와 상기 확인된 어플리케이션의 보안 상태 정보가 일치하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작을 포함할 수 있다.
- [130] 다양한 실시예에 따르면, 상기 프로세서(120)에서, 상기 전자 장치에 상기 어플리케이션이 설치되는 시점에 상기 어플리케이션의 보안 상태 정보를 결정하는 동작, 및 상기 프로세서(120)에서, 상기 결정된 어플리케이션의 보안 상태 정보를 상기 보안 엘리먼트(172)로 전송하여 상기 보안 엘리먼트(172)의 저장소에 저장되도록 제어하는 동작을 더 포함할 수 있다.
- [131] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작은, 상기 보안 엘리먼트(172)에서, 상기 전자 장치의 보안 상태 정보가 접근 관리자의 위변조에 관련된 조건을 만족하는지 여부를 결정하는 동작, 상기 전자 장치의 보안 상태 정보가 접근 관리자의 위변조에 관련된 조건을 만족하지 않는 경우, 상기 보안 엘리먼트(172)에서 상기 감지된 보안 관련 서비스 요청 명령에 대응되는 인터페이스를 확인하는 동작, 상기 확인된 인터페이스가 상기 위변조된 접근 관리자에 대응되는 인터페이스인 경우, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령을 무시하는 동작, 및 상기 확인된 인터페이스가 상기 위변조된 접근 관리자에 대응되는 인터페이스가 아닌 경우, 상기 보안 엘리먼트(172)에서, 상기 감지된 보안 관련 서비스 요청 명령에 대응되는 기능을 수행하는 동작을 포함할 수 있다.
- [132] 다양한 실시예에 따르면, 상기 보안 엘리먼트(172)에서, 상기 보안 관련 서비스 요청 명령에 대한 응답 신호를 상기 프로세서(120), 또는 외부 전자 장치(102)로 제공하는 동작을 더 포함하며, 상기 응답 신호는, 상기 보안 관련 서비스 요청 명령에 의해 요청된 정보, 보안 관련 서비스 요청 명령에 의해 수행된 기능에

대한 결과를 나타내는 정보, 또는 보안 관련 서비스에 대한 승인 여부를 나타내는 정보 중 적어도 하나를 포함할 수 있다.

- [133] 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.
- [134] 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 항목들 중 어느 하나, 또는 그들의 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.
- [135] 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, 일 실시예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.
- [136] 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 저장매체는, 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 일시적으로 저장되는 경우를 구분하지 않는다.

- [137] 일실시에 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 스토어™)를 통해 또는 두 개의 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, 일시적으로 생성될 수 있다.
- [138] 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,
상기 전자 장치의 보안 상태 정보를 획득하는 프로세서; 및
상기 프로세서의 제어에 의해 동작하고, 상기 프로세서로부터 상기 전자 장치의 보안 상태 정보를 수신하고, 수신된 전자 장치의 보안 상태 정보를 저장하는 저장소를 포함하는 보안 엘리먼트를 포함하고,
상기 보안 엘리먼트는,
보안 관련 서비스 요청 명령을 감지하고,
상기 저장소에서 상기 전자 장치의 보안 상태 정보를 획득하고,
상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 전자 장치.
- [청구항 2] 제1항에 있어서,
상기 전자 장치의 보안 상태 정보는, 상기 전자 장치의 루팅 여부에 대한 정보, 멀웨어(malware) 감지 여부에 대한 정보, 워런티 비트(warranty bit) 변경 여부에 대한 정보, 접근 관리자의 위변조 여부에 대한 정보, 상기 전자 장치의 시스템 영역에 대한 보안 상태 정보, 또는 상기 전자 장치에 설치된 어플리케이션에 대한 보안 상태 정보 중 적어도 하나를 포함하는 전자 장치.
- [청구항 3] 제1항에 있어서,
상기 보안 상태 정보는, 보안 레벨, 또는 보안 문제의 종류 중 적어도 하나를 나타내는 전자 장치.
- [청구항 4] 제1항에 있어서,
상기 지정된 조건은, 상기 보안 관련 서비스 요청 명령의 종류에 기초하여 결정되는 전자 장치.
- [청구항 5] 제1항에 있어서,
상기 보안 관련 서비스를 요청하는 명령은, 상기 프로세서, 또는 외부 전자 장치로부터 수신되는 전자 장치.
- [청구항 6] 제1항에 있어서,
상기 보안 엘리먼트는, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는 경우, 상기 감지된 보안 관련 서비스 요청 명령을 정상적으로 처리하여 상기 명령에 대응되는 기능을 수행하고,
상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 상기 감지된 보안 관련 서비스 요청 명령을 무시하는 전자 장치.
- [청구항 7] 제1항에 있어서,
상기 보안 엘리먼트는, 상기 프로세서로부터 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 수신하고,

상기 저장소에 저장된 상기 전자 장치의 보안 상태 정보에서 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 획득하고,

상기 수신된 어플리케이션의 보안 상태 정보와 상기 획득된 어플리케이션의 보안 상태 정보가 일치하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 전자 장치.

[청구항 8]

제7항에 있어서,

상기 프로세서는, 상기 전자 장치에 상기 어플리케이션이 설치된 시점에 상기 어플리케이션의 보안 상태 정보를 결정하고,

상기 결정된 어플리케이션의 보안 상태 정보를 상기 보안 엘리먼트로 전송하여 상기 보안 엘리먼트의 저장소에 저장되도록 제어하는 전자 장치.

[청구항 9]

제1항에 있어서,

상기 보안 엘리먼트는, 상기 전자 장치의 보안 상태 정보가 접근 관리자의 위변조에 관련된 조건을 만족하는지 여부를 결정하고,

상기 전자 장치의 보안 상태 정보가 접근 관리자의 위변조에 관련된 조건을 만족하지 않는 경우, 상기 감지된 보안 관련 서비스 요청 명령에 대응되는 인터페이스를 확인하고,

상기 확인된 인터페이스가 상기 위변조된 접근 관리자에 대응되는

인터페이스인 경우, 상기 감지된 보안 관련 서비스 요청 명령을 무시하고,

상기 확인된 인터페이스가 상기 위변조된 접근 관리자에 대응되는

인터페이스가 아닌 경우, 상기 감지된 보안 관련 서비스 요청 명령에 대응되는 기능을 수행하는 전자 장치.

[청구항 10]

제9항에 있어서,

상기 보안 엘리먼트는, 상기 보안 관련 서비스 요청 명령에 대한 응답 신호를 상기 프로세서, 또는 외부 전자 장치로 제공하고,

상기 응답 신호는, 상기 보안 관련 서비스 요청 명령에 의해 요청된 정보, 보안 관련 서비스 요청 명령에 의해 수행된 기능에 대한 결과를 나타내는 정보, 또는 보안 관련 서비스에 대한 승인 여부를 나타내는 정보 중 적어도 하나를 포함하는 전자 장치.

[청구항 11]

전자 장치의 동작 방법에 있어서,

프로세서에서, 상기 전자 장치의 보안 상태 정보를 획득하는 동작;

상기 프로세서의 제어에 의해 동작하는 보안 엘리먼트에서, 상기 전자 장치의 보안 상태 정보를 상기 보안 엘리먼트 내부의 저장소에 저장하는 동작;

상기 보안 엘리먼트에서, 보안 관련 서비스 요청 명령을 감지하는 동작;

상기 보안 엘리먼트에서 상기 내부의 저장소에 저장된 상기 전자 장치의 보안 상태 정보를 획득하는 동작; 및

상기 보안 엘리먼트에서, 상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작을 포함하는 방법.

- [청구항 12] 제11항에 있어서,
상기 전자 장치의 보안 상태 정보는, 상기 전자 장치의 루팅 여부에 대한 정보, 멀웨어(malware) 감지 여부에 대한 정보, 워런티 비트(warranty bit) 변경 여부에 대한 정보, 접근 관리자의 위변조 여부에 대한 정보, 상기 전자 장치의 시스템 영역에 대한 보안 상태 정보, 또는 상기 전자 장치에 설치된 어플리케이션에 대한 보안 상태 정보 중 적어도 하나를 포함하며,
상기 보안 상태 정보는, 보안 레벨, 또는 보안 문제의 종류 중 적어도 하나를 나타내며,
상기 지정된 조건은, 상기 보안 관련 서비스 요청 명령의 종류에 기초하여 결정되고,
상기 보안 관련 서비스를 요청하는 명령은, 상기 프로세서, 또는 외부 전자 장치로부터 수신되는 방법.

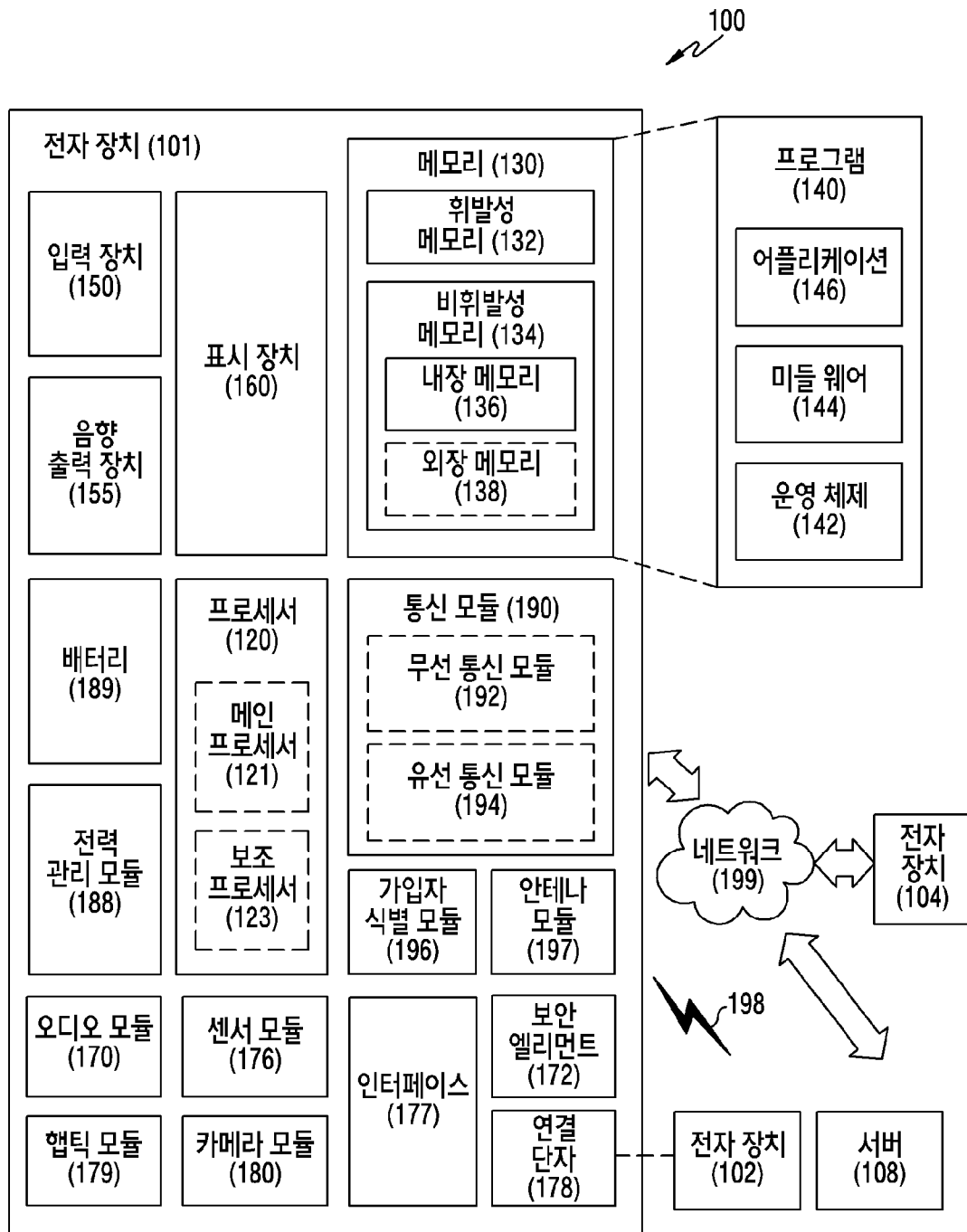
- [청구항 13] 제11항에 있어서,
상기 보안 엘리먼트에서, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작은,
상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하는 경우, 상기 보안 엘리먼트에서, 상기 감지된 보안 관련 서비스 요청 명령을 정상적으로 처리하여 상기 명령에 대응되는 기능을 수행하는 동작; 및
상기 획득된 전자 장치의 보안 상태 정보가 지정된 조건을 만족하지 않는 경우, 상기 보안 엘리먼트에서, 상기 감지된 보안 관련 서비스 요청 명령을 무시하는 동작을 포함하는 방법.

- [청구항 14] 제11항에 있어서,
상기 보안 엘리먼트에서, 상기 프로세서로부터 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 수신하는 동작을 더 포함하며,
상기 보안 엘리먼트에서, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작은,
상기 보안 엘리먼트에서, 획득된 보안 상태 정보에서 상기 보안 관련 서비스 요청 명령에 관련된 어플리케이션의 보안 상태 정보를 확인하는 동작; 및
상기 보안 엘리먼트에서, 상기 수신된 어플리케이션의 보안 상태 정보와 상기 확인된 어플리케이션의 보안 상태 정보가 일치하는지 여부에 기초하여, 상기 감지된 보안 관련 서비스 요청 명령을 처리 또는 무시하는 동작을 포함하는 방법.

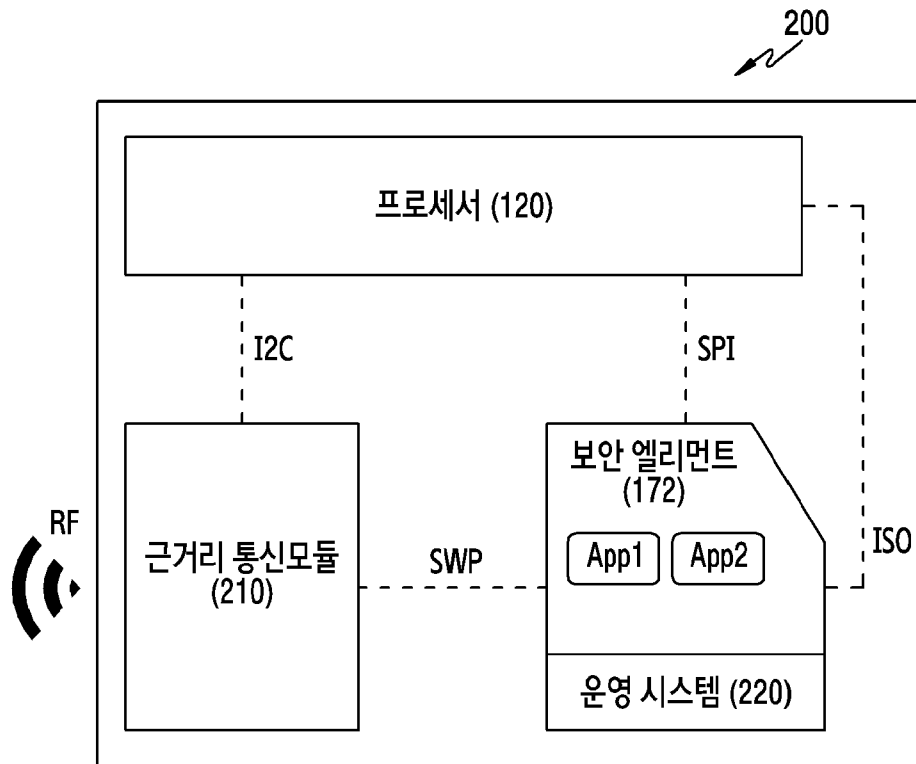
- [청구항 15] 제14항에 있어서,

상기 프로세서에서, 상기 전자 장치에 상기 어플리케이션이 설치되는 시점에 상기 어플리케이션의 보안 상태 정보를 결정하는 동작; 및
상기 프로세서에서, 상기 결정된 어플리케이션의 보안 상태 정보를 상기 보안 엘리먼트로 전송하여 상기 보안 엘리먼트의 저장소에 저장되도록 제어하는 동작을 더 포함하는 방법.

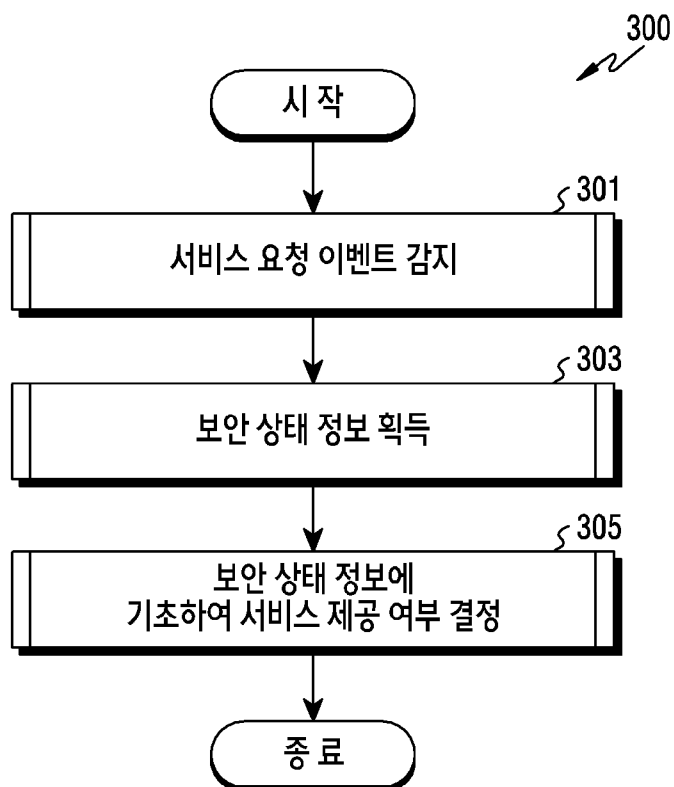
[도 1]



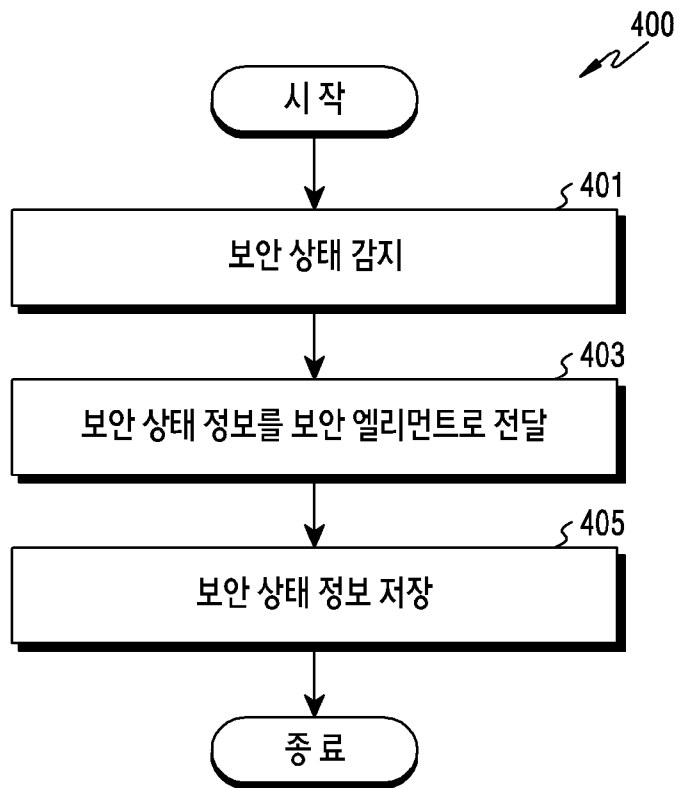
[도2]



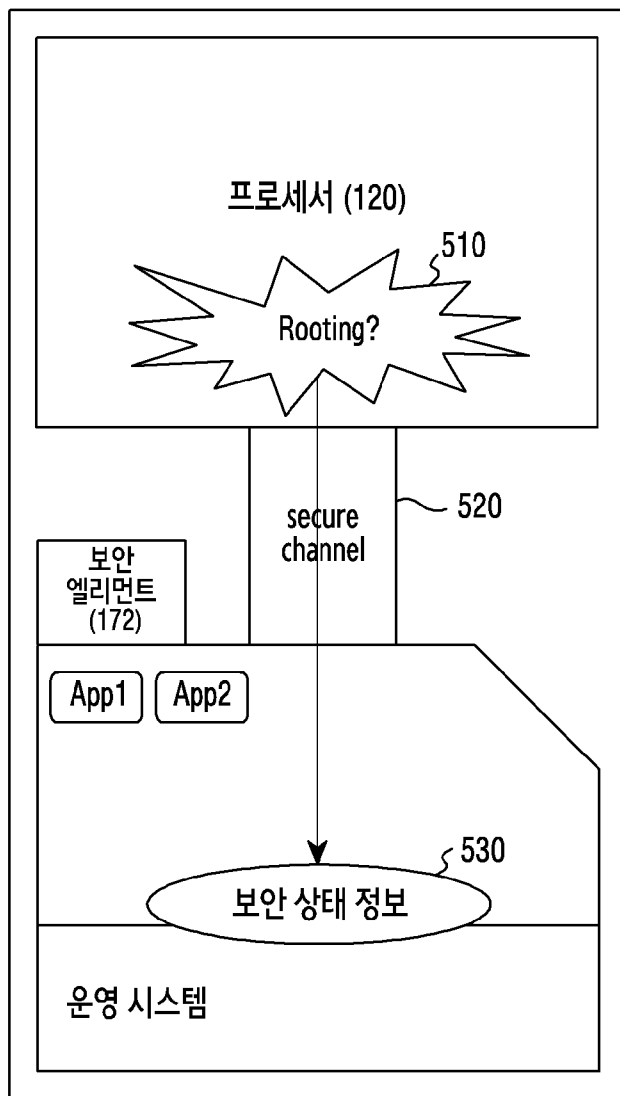
[도3]



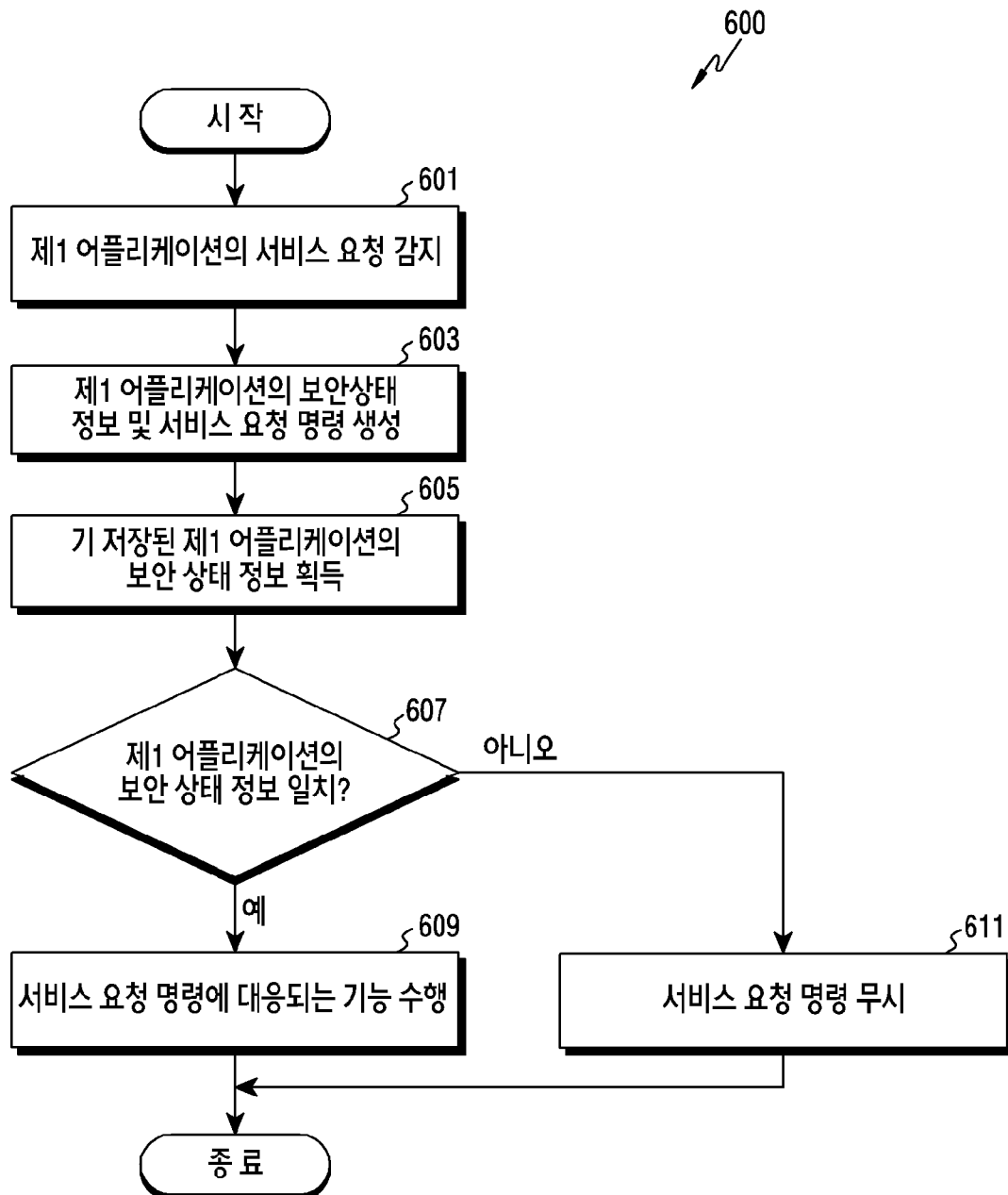
[도4]



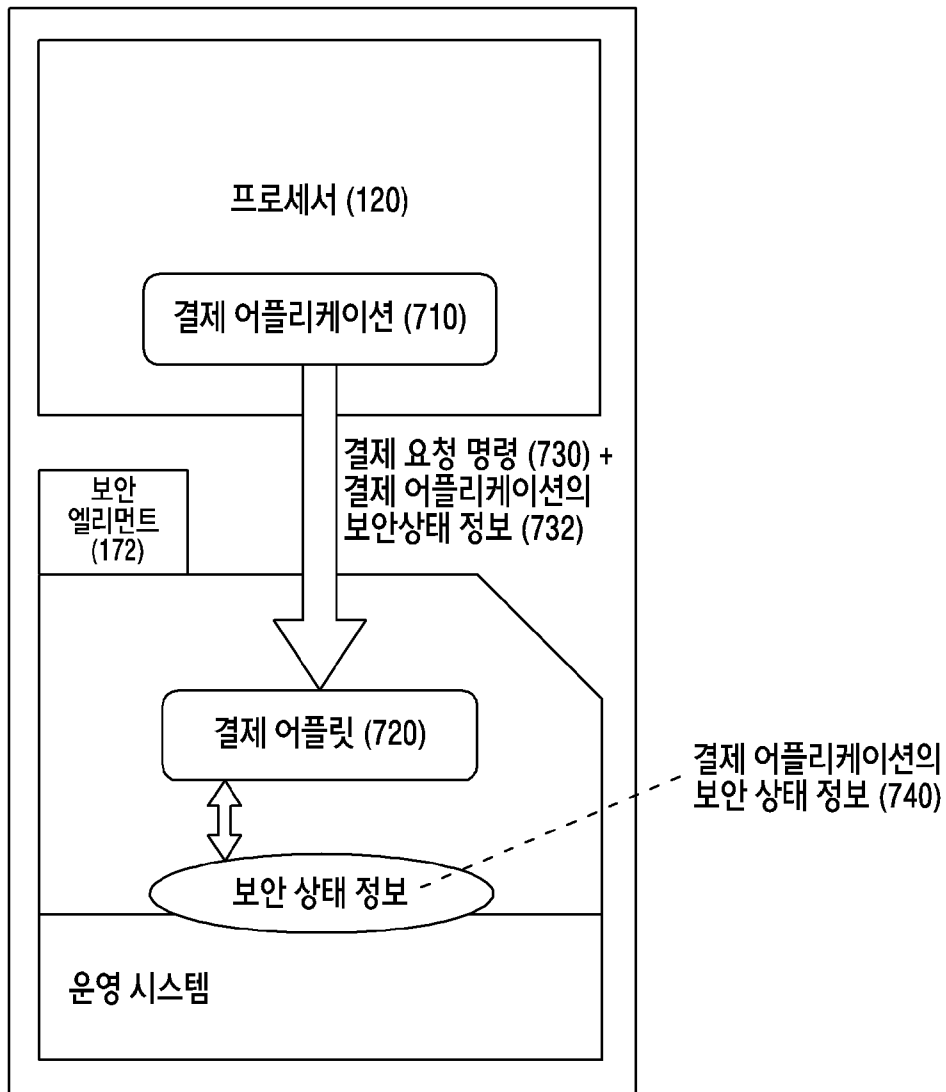
[도5]



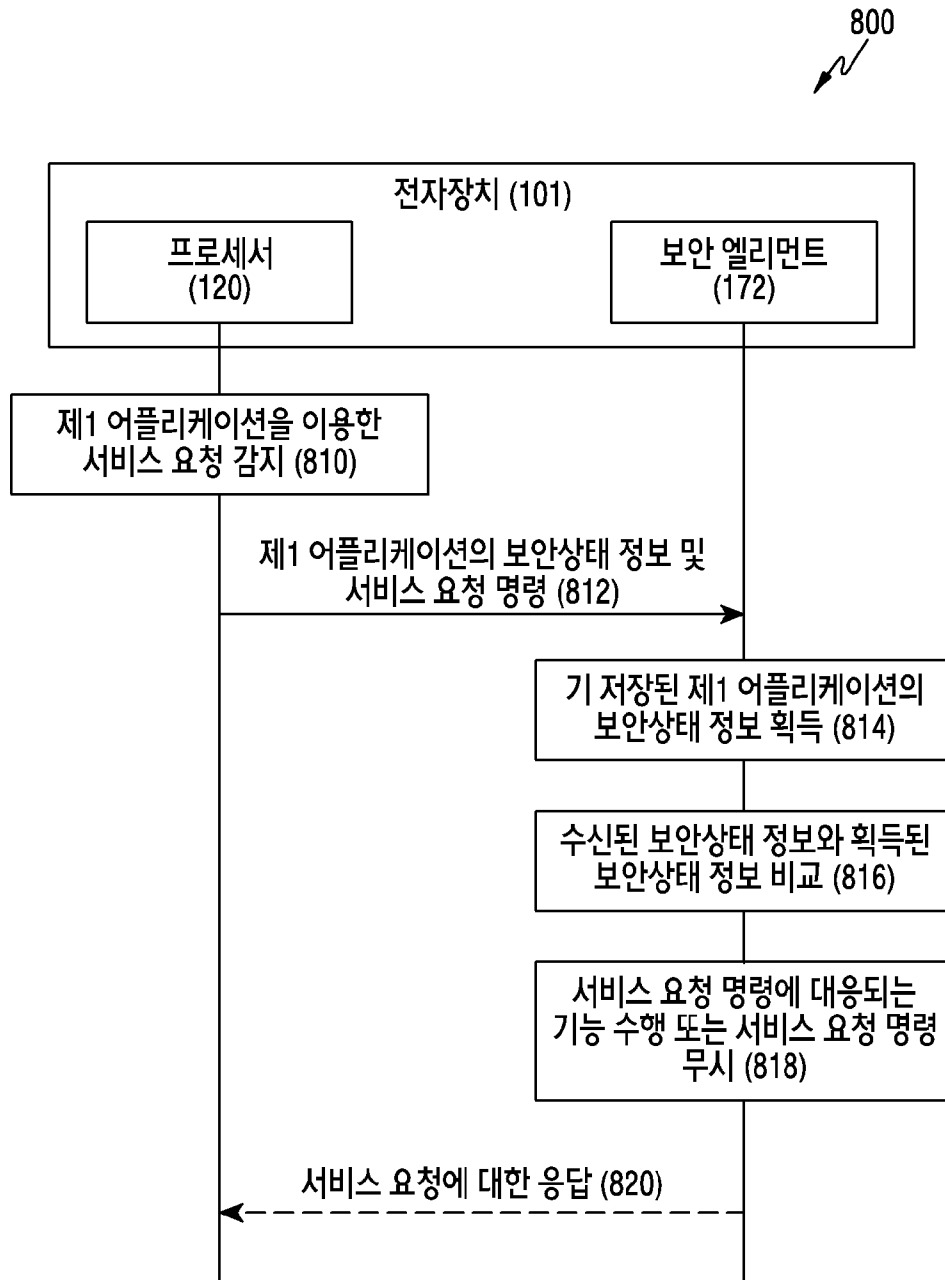
[도6]



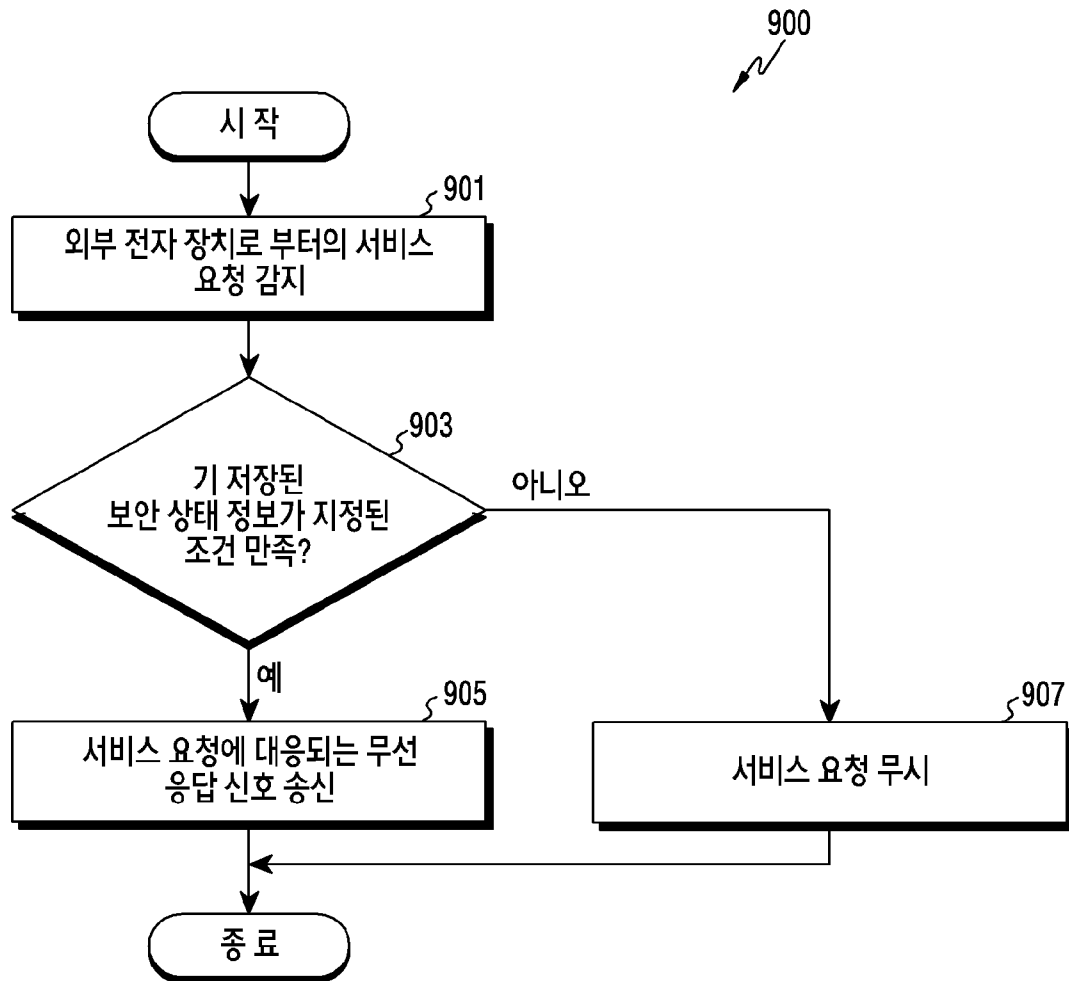
[도7]



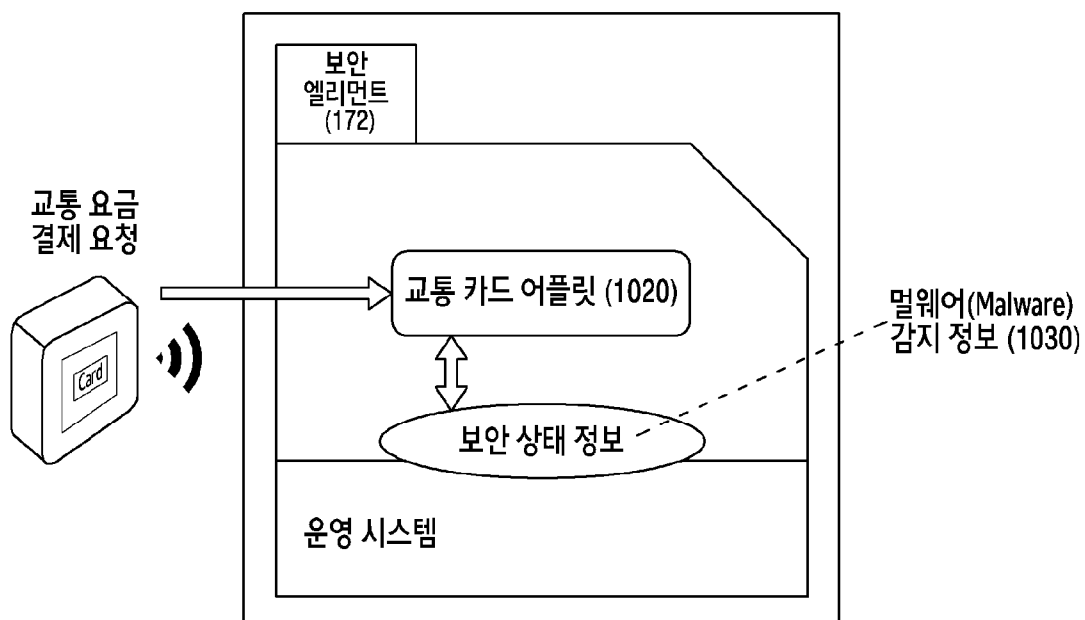
[도8]



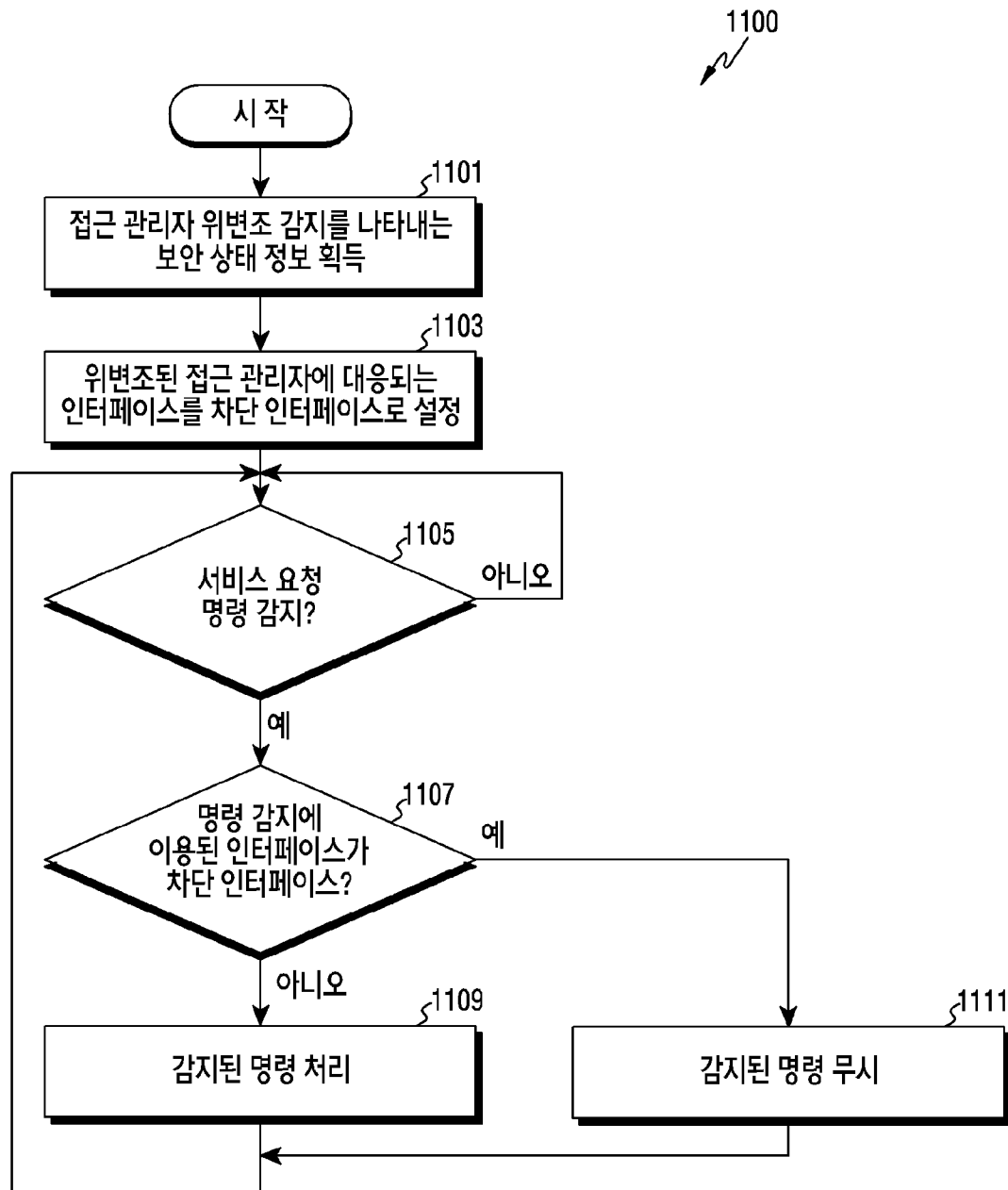
[도9]



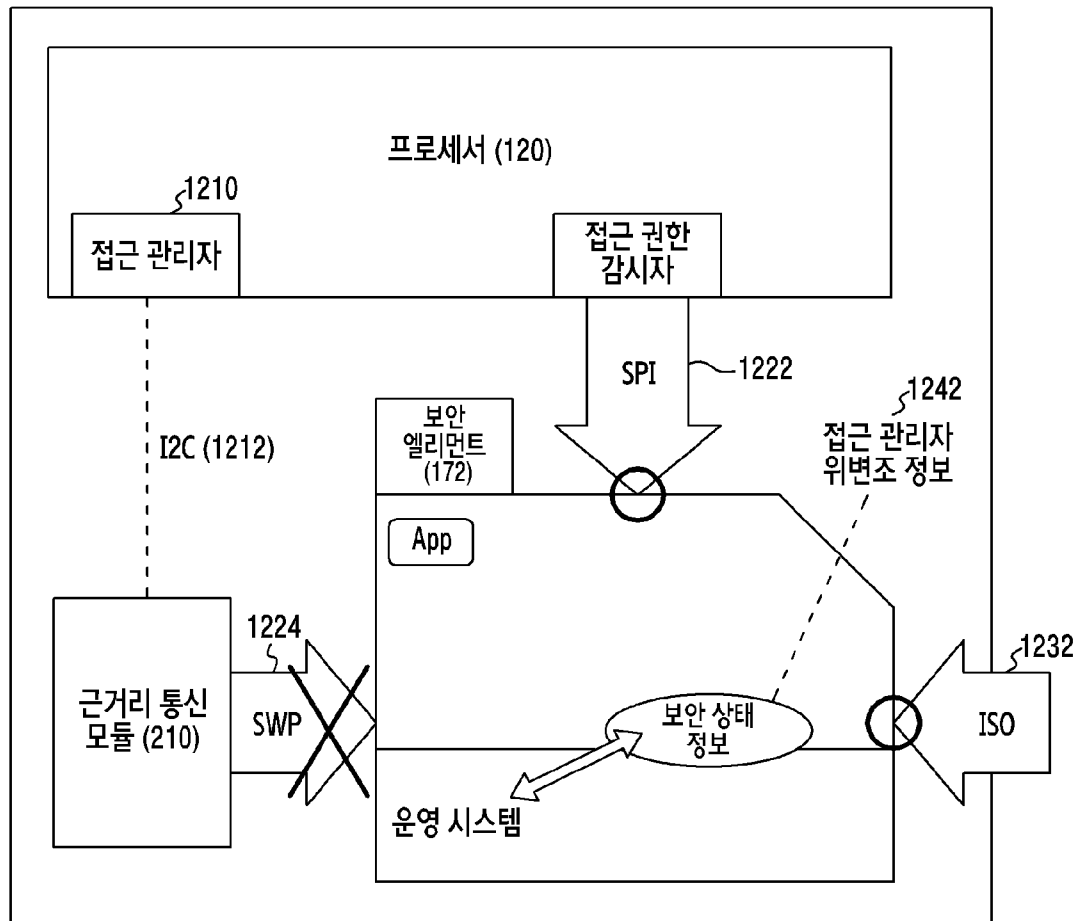
[도10]



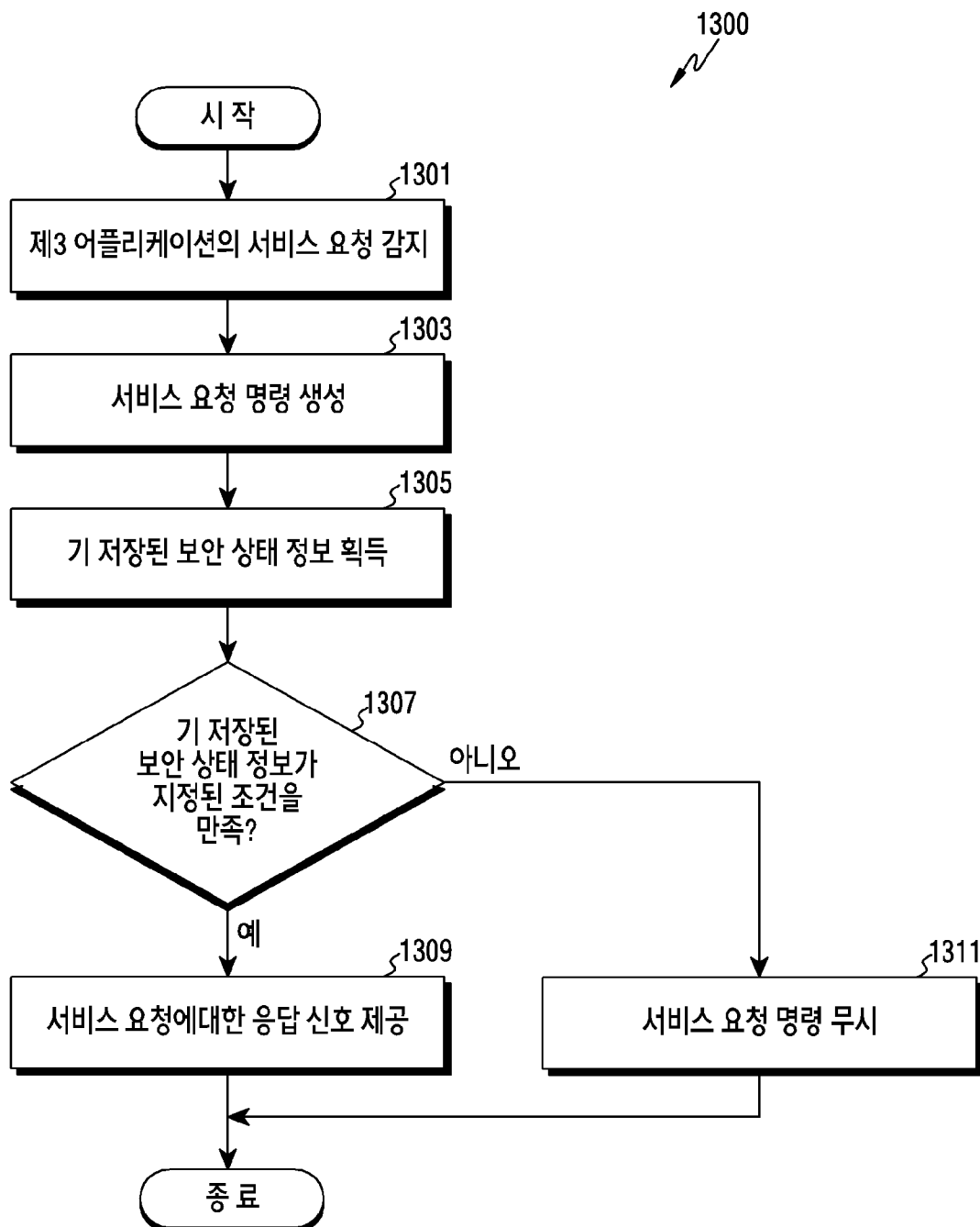
[도11]



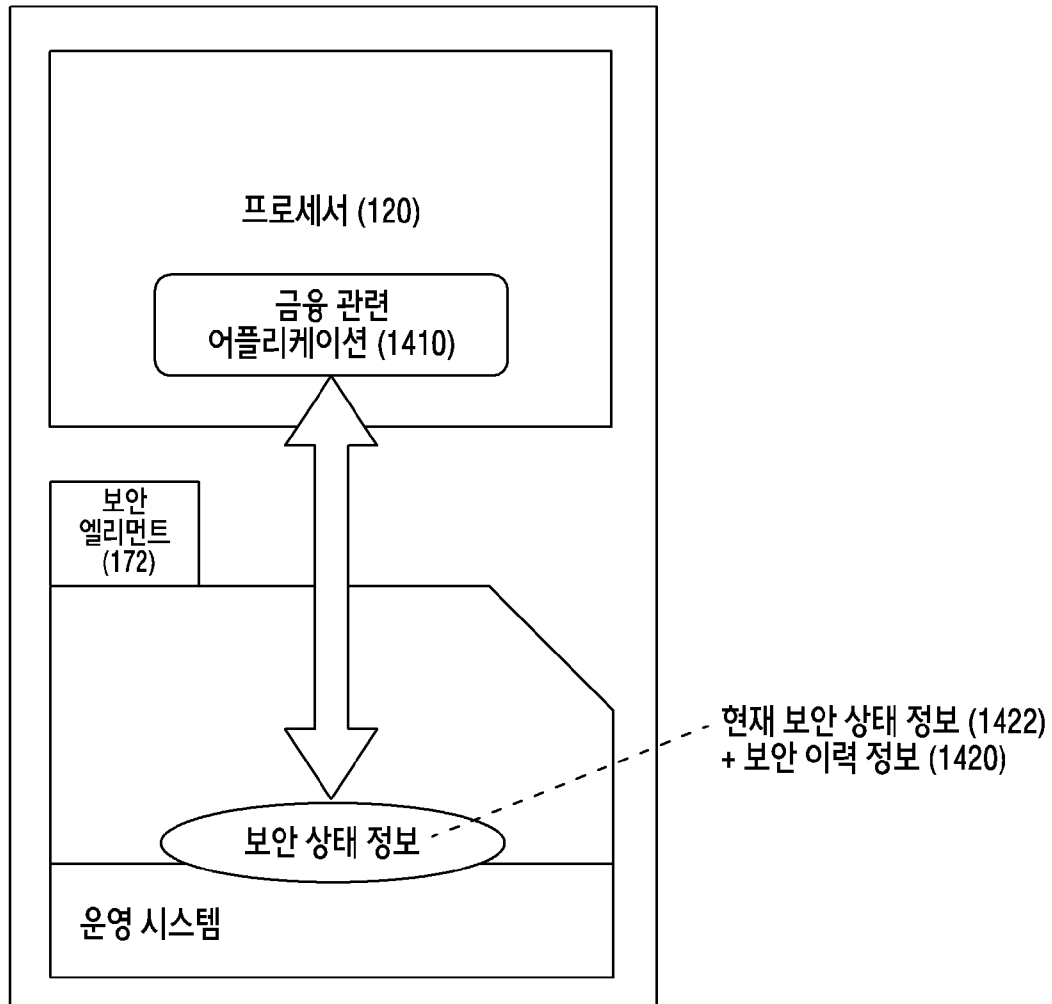
[도12]



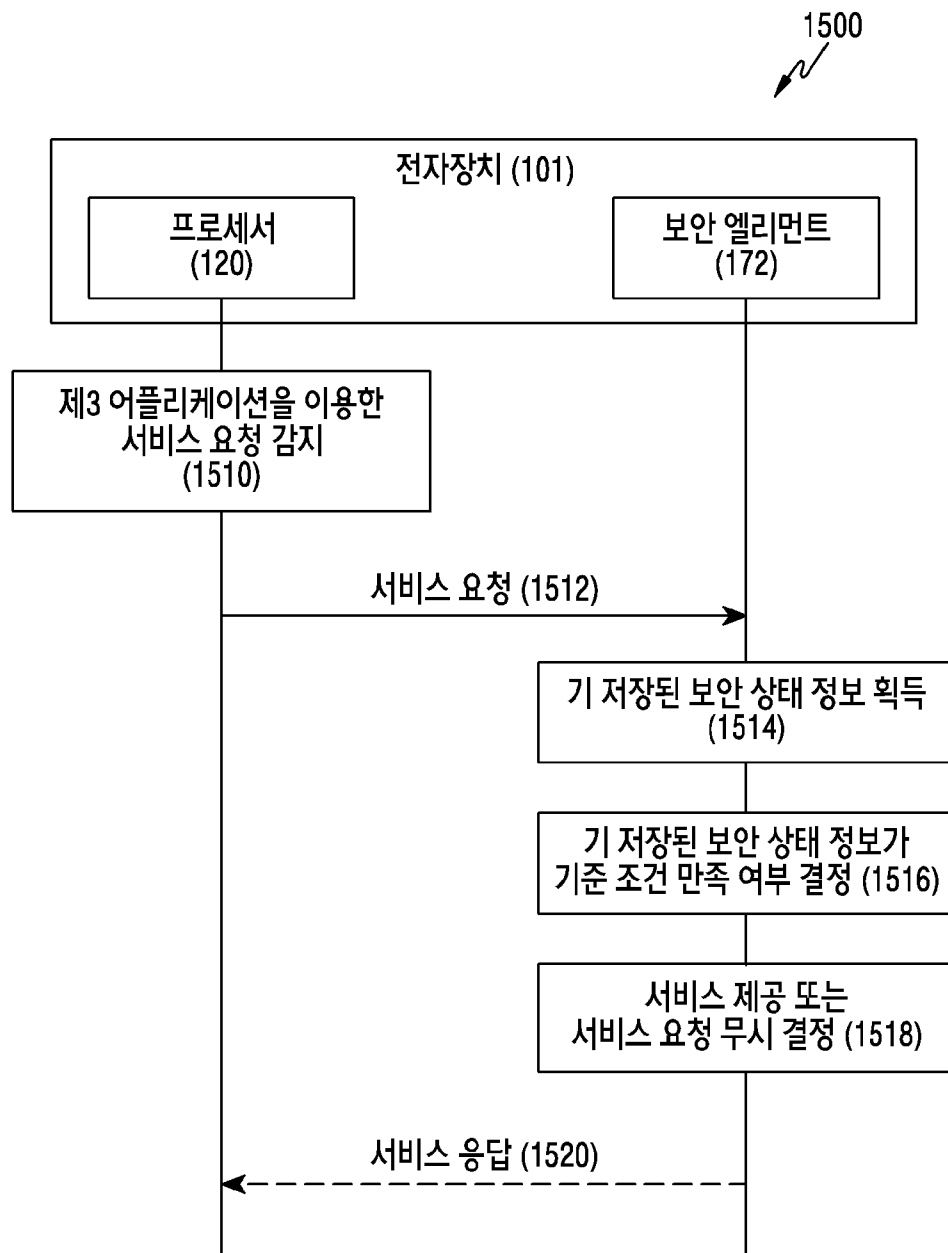
[도13]



[도 14]



[도 15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2019/011774

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56(2013.01)i, G06F 21/60(2013.01)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 21/56; G06F 11/30; G06F 15/16; G06F 21/00; G06F 21/55; G06F 21/57; G06Q 20/12; G06Q 20/16; H04W 12/06; G06F 21/60

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: status, rooting, secure, service, application, deactivation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2013-0015236 A (KT CORPORATION) 13 February 2013 See paragraphs [0025], [0055], [0057], [0063], [0067]-[0068]; claim 1; and figure 6.	1-15
A	KR 10-2012-0057871 A (INFOSEC CO., LTD.) 07 June 2012 See paragraphs [0040]-[0067]; claim 1; and figures 3-4.	1-15
A	KR 10-2014-0139752 A (INFRAWARE TECHNOLOGY, INC. et al.) 08 December 2014 See paragraphs [0043]-[0082]; and figures 1-3.	1-15
A	KR 10-2012-0136126 A (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY) 18 December 2012 See paragraphs [0016]-[0045]; and figures 1-3.	1-15
A	KR 10-2017-0077425 A (SAMSUNG ELECTRONICS CO., LTD.) 06 July 2017 See claims 1-3; and figure 4.	1-15
A	US 2012-0178420 A1 (OULD, Christopher James) 12 July 2012 See claims 1-11; and figure 5.	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

07 JANUARY 2020 (07.01.2020)

Date of mailing of the international search report

08 JANUARY 2020 (08.01.2020)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsu-ro, Seo-gu,
Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2019/011774

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2013-0015236 A	13/02/2013	KR 10-1839607 B1	22/03/2018
KR 10-2012-0057871 A	07/06/2012	KR 10-1206737 B1	30/11/2012
		KR 10-1206740 B1	30/11/2012
		KR 10-2012-0057870 A	07/06/2012
		US 2012-0137369 A1	31/05/2012
KR 10-2014-0139752 A	08/12/2014	None	
KR 10-2012-0136126 A	18/12/2012	KR 10-1266037 B1	21/05/2013
KR 10-2017-0077425 A	06/07/2017	CN 107085790 A	22/08/2017
		EP 3190557 A1	12/07/2017
		US 2017-0186015 A1	29/06/2017
		WO 2017-116144 A1	06/07/2017
US 2012-0178420 A1	12/07/2012	US 2009-0273435 A1	05/11/2009
		US 8149085 B2	03/04/2012
		US 9167432 B2	20/10/2015

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/56(2013.01)i, G06F 21/60(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/56; G06F 11/30; G06F 15/16; G06F 21/00; G06F 21/55; G06F 21/57; G06Q 20/12; G06Q 20/16; H04W 12/06; G06F 21/60

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: 상태(status), 루팅(rooting), 보안(secure), 서비스(service), 애플리케이션(application), 비활성화(disable)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2013-0015236 A (주식회사 케이티) 2013.02.13 단락 [0025], [0055], [0057], [0063], [0067]-[0068]; 청구항 1; 및 도면 6 참조.	1-15
A	KR 10-2012-0057871 A (인포섹(주)) 2012.06.07 단락 [0040]-[0067]; 청구항 1; 및 도면 3-4 참조.	1-15
A	KR 10-2014-0139752 A (주식회사 인프라웨어테크놀로지 등) 2014.12.08 단락 [0043]-[0082]; 및 도면 1-3 참조.	1-15
A	KR 10-2012-0136126 A (충남대학교산학협력단) 2012.12.18 단락 [0016]-[0045]; 및 도면 1-3 참조.	1-15
A	KR 10-2017-0077425 A (삼성전자주식회사) 2017.07.06 청구항 1-3; 및 도면 4 참조.	1-15
A	US 2012-0178420 A1 (CHRISTOPHER JAMES OULD) 2012.07.12 청구항 1-11; 및 도면 5 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

“D” 본 국제출원에서 출원인이 인용한 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후 “X”에 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

2020년 01월 07일 (07.01.2020)

국제조사보고서 발송일

2020년 01월 08일 (08.01.2020)

ISA/KR의 명칭 및 우편주소



대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

김성희

전화번호 +82-42-481-3516



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2013-0015236 A	2013/02/13	KR 10-1839607 B1	2018/03/22
KR 10-2012-0057871 A	2012/06/07	KR 10-1206737 B1	2012/11/30
		KR 10-1206740 B1	2012/11/30
		KR 10-2012-0057870 A	2012/06/07
		US 2012-0137369 A1	2012/05/31
KR 10-2014-0139752 A	2014/12/08	없음	
KR 10-2012-0136126 A	2012/12/18	KR 10-1266037 B1	2013/05/21
KR 10-2017-0077425 A	2017/07/06	CN 107085790 A	2017/08/22
		EP 3190557 A1	2017/07/12
		US 2017-0186015 A1	2017/06/29
		WO 2017-116144 A1	2017/07/06
US 2012-0178420 A1	2012/07/12	US 2009-0273435 A1	2009/11/05
		US 8149085 B2	2012/04/03
		US 9167432 B2	2015/10/20