(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2022 년 8 월 11 일 (11.08.2022)

WIPO | PCT

(10) 국제공개번호
WO 2022/169233 A1

(51) 국제특허분류:
H04W 4/50 (2018.01) *H04W 12/06* (2009.01)
H04W 48/16 (2009.01) *H04W 84/12* (2009.01)
H04W 48/14 (2009.01)

(21) 국제출원번호: PCT/KR2022/001609

(22) 국제출원일: 2022 년 1 월 28 일 (28.01.2022)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2021-0016214 2021 년 2 월 4 일 (04.02.2021) KR

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

(72) 발명자: **장원준 (JANG, Wonjun)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **정부섭 (JUNG, Buseop)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **김범집 (KIM, Beomjip)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **김학관 (KIM, Hakkwan)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **방혜정 (BANG, Hyejung)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **이두호 (LEE, Dooho)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **이선기 (LEE, Sunkey)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **이순호 (LEE, Soonho)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **조남주 (CHO, Namju)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

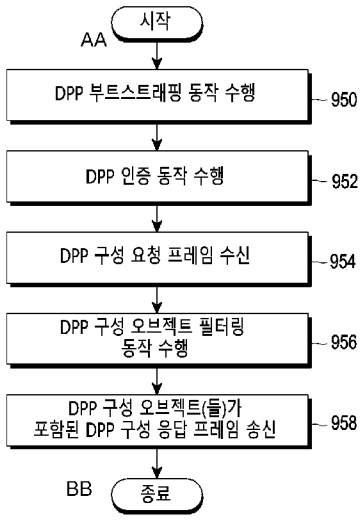
(74) 대리인: **이건주 등 (LEE, Keon-Joo** et al.); 03079 서울시 종로구 대학로9길 16 미화빌딩, Seoul (KR).

(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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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), 유

(54) Title: ELECTRONIC DEVICE FOR TRANSMITTING/RECEIVING NETWORK CONFIGURATION INFORMATION AND OPERATION METHOD THEREOF

(54) 발명의 명칭: 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법



950 ... Carry out DPP bootstrapping operation
952 ... Carry out DPP authentication operation
954 ... Receive DPP configuration request frame
956 ... Carry out DPP configuration object filtering operation
958 ... Transmit DPP configuration response frame including DPP configuration object(s)
AA ... Start
BB ... End

(57) Abstract: An electronic device is provided. The electronic device may comprise a communication circuit and at least one processor. The at least one processor may be configured to: receive, from an external electronic device via the communication circuit, a first message requesting for network configuration information; on the basis of a preset filtering scheme, select at least one network configuration information to be transmitted to the external electronic device, among a plurality of network configuration information stored in the electronic device; and transmit, to the external electronic device via the communication circuit, a second message including the selected at least one network configuration information.

(57) 요약서: 전자 장치가 제공된다. 상기 전자 장치는 통신 회로, 적어도 하나의 프로세서를 포함할 수 있고, 상기 적어도 하나의 프로세서는 상기 통신 회로를 통해, 외부 전자 장치로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하고, 설정되어 있는 필터링 방식을 기반으로 상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치로 송신할 적어도 하나의 네트워크 구성 정보를 선택하고, 상기 통신 회로를 통해, 상기 외부 전자 장치로 상기 선택한 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 송신하도록 설정될 수 있다.

WO 2022/169233 A1

[다음 쪽 계속]

럽 (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: 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법

기술분야

[1] 본 개시는 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법에 관한 것이다.

배경기술

[2] 무선 통신 시스템은 음성 또는 데이터와 같은 다양한 타입들의 통신 서비스들을 제공하기 위해 광범위하게 개발되고 있다. 일반적으로 무선 통신 시스템은 가용한 시스템 자원들(예를 들어, 시간 자원, 주파수 자원, 대역폭 자원, 또는 출력 전력 자원)을 공유하여 다수의 전자 장치들과의 통신을 지원할 수 있는 다중 억세스(Multiple Access: MA) 시스템이다. MA 시스템들은 예를 들어 코드 분할 다중 억세스(Code Division Multiple Access: CDMA) 시스템, 주파수 분할 다중 억세스(Frequency Division Multiple Access: FDMA) 시스템, 시간 분할 다중 억세스(Time Division Multiple Access: TDMA) 시스템, 직교 주파수 분할 다중 억세스(Orthogonal Frequency Division Multiple Access: OFDMA) 시스템, 단일 캐리어-주파수 분할 다중 억세스(Single Carrier Frequency Division Multiple Access: SC-FDMA) 시스템 및 다중 캐리어-주파수 분할 다중 억세스(Multi Carrier Frequency Division Multiple Access: MC-FDMA) 시스템을 포함한다.

[3] 최근 정보 통신 기술의 발전과 더불어 다양한 무선 통신 기술들이 개발되고 있다. 특히 무선 근거리 통신 네트워크(Wireless Local Area Network: WLAN) 기술은 무선 주파수 기술을 바탕으로 스마트 폰, 개인용 디지털 기기(Personal Digital Assistant: PDA), 또는 랩탑 컴퓨터와 같은, 전자 장치를 이용하여 가정이나 기업 또는 특정 서비스 제공 지역에서 무선으로 인터넷에 억세스할 수 있도록 하는 기술이다.

[4] WLAN 시스템에서는 장치들 간의 통신의 유연성을 확보하기 위해, 기지국(Base Station: BS)이나 억세스 포인트(Access Point: AP)와 같은, 관리 엔터티(entity)의 개입 없이 장치들 간 직접 통신을 위한 다양한 프로토콜들이 제안되고 있다. 특히, 와이파이(Wi-Fi) 규격을 기반으로 와이파이 얼라이언스(Wi-Fi Alliance: WFA)에서는 사용자 인터페이스(User Interface: UI)를 구비하고 있지 않거나 또는 제한적인 UI를 구비하고 있는 Wi-Fi 장치를 간단하면서도 효율적으로 Wi-Fi 네트워크에 연결할 수 있는 장치 프로비져닝 프로토콜(Device Provisioning Protocol: DPP)을 개발하였다.

[5] 상기의 정보는 본 개시의 이해를 돕기 위한 배경 정보로서만 제공된다. 상기의 내용 중 어느 것이 본 개시와 관련하여 선행 기술로 적용될 수 있는지 여부에 대한 결정이 내려지지 않았으며, 어떤 주장도 이루어지지 않는다.

발명의 상세한 설명

기술적 과제

[6] 무선 통신 기술 들 중 와이파이 (Wi-Fi) 규격을 기반으로 와이파이 얼라이언스(Wi-Fi Alliance: WFA)에서 규격화하고 있는 장치 프로비져닝 프로토콜(Device Provisioning Protocol: DPP) 기술에서는 다수의 AP들이 존재하고, 다수의 AP들 각각이 고유한 연결 정보를 가지고 있는 경우가 고려되고 있다.

[7] 이 경우, 구성자(configurator)가 등록자(enrollee), 예를 들어 클라이언트 등록자(enrollee client)에게 다수의 AP들에 대한 연결 정보들을 송신해야 할 필요성이 있을 수 있다. 하지만, 현재 DPP 기술에서는 다수의 AP들에 대한 연결 정보들이 존재할 경우 다수의 AP들에 대한 연결 정보들을 어떻게 제공하는지에 대해서는 명시하고 있지 않다.

[8] 또한, DPP 기술에서는 구성자가 클라이언트 등록자에게 AP에 대한 연결 정보를 제공한다고 명시하고 있으나, 클라이언트 등록자에게 제공되는 AP에 대한 연결 정보가 구체적으로 어떤 AP에 대한 연결 정보인지에 대해서는 명시하고 있지 않다.

[9] 본 개시의 측면들은 적어도 상기에서 언급된 문제점들 및/또는 단점들을 다루고, 적어도 하기에서 설명되는 이점들을 제공하는 것에 있다. 따라서. 본 개시의 일 측면은 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법을 제공하는 것이다.

[10] 본 개시의 다른 측면은 DPP 네트워크에서 다수의 네트워크 구성 정보들을 송수신하는 전자 장치 및 그 동작 방법을 제공하는 것이다.

[11] 본 개시의 다른 측면은 DPP 네트워크에서 등록자에 적합한 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법을 제공하는 것이다.

[12] 본 개시의 다른 측면은 DPP 네트워크에서 제공할 네트워크 구성 정보들을 필터링하는 기준을 제공하는 전자 장치 및 그 동작 방법을 제공하는 것이다.

[13] 추가적인 측면들은 다음의 상세한 설명에서 부분적으로 설명될 것이고, 부분적으로는 상세한 설명으로부터 명백해질 것이며, 또는 제시된 실시 예들의 실행에 의해 학습될 수 있다.

과제 해결 수단

[14] 본 개시의 일 측면에 따르면, 전자 장치가 제공된다. 상기 전자 장치는 통신 회로, 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 통신 회로를 통해, 외부 전자 장치로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하고, 설정되어 있는 필터링 방식을 기반으로 상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치로 송신할 적어도 하나의 네트워크 구성 정보를 선택하고, 상기 통신 회로를 통해, 상기 외부 전자 장치로 상기 선택한 적어도 하나의 네트워크 구성 정보를

포함하는 제2 메시지를 송신하도록 설정될 수 있다.

[15] 본 개시의 다른 측면에 따르면, 전자 장치가 제공된다. 상기 전자 장치는 통신 회로, 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 통신 회로를 통해, 외부 전자 장치와 보안 정보를 기반으로 인증 동작을 수행하고, 상기 통신 회로를 통해, 상기 외부 전자 장치로 네트워크 구성 정보를 요청하는 제1 메시지를 송신하고, 상기 통신 회로를 통해, 상기 외부 전자 장치로부터 상기 외부 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 설정되어 있는 필터링 방식을 기반으로 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 수신하도록 설정될 수 있다.

[16] 본 개시의 다른 측면에 따르면, 전자 장치에 의해 수행되는 방법이 제공된다. 상기 방법은 외부 전자 장치로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하는 동작, 설정되어 있는 필터링 방식을 기반으로 상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치로 송신할 적어도 하나의 네트워크 구성 정보를 선택하는 동작, 상기 외부 전자 장치로 상기 선택한 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 송신하는 동작을 포함할 수 있다.

[17] 본 개시의 다른 측면에 따르면, 전자 장치에 의해 수행되는 방법이 제공된다. 상기 방법은 외부 전자 장치와 보안 정보를 기반으로 인증 동작을 수행하는 동작, 상기 외부 전자 장치로 네트워크 구성 정보를 요청하는 제1 메시지를 송신하는 동작, 상기 외부 전자 장치로부터 상기 외부 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 설정되어 있는 필터링 방식을 기반으로 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 수신하는 동작을 포함할 수 있다.

[18] 본 개시의 다른 측면들, 이점들 및 두드러진 특징들은 첨부 도면들과 함께 본 개시의 다양한 실시 예들을 개시하는 하기의 상세한 설명으로부터 해당 기술 분야의 당업자들에게 명백해질 것이다.

도면의 간단한 설명

[19] 본 개시의 특정 실시 예들의 상기와 같은, 그리고 다른 측면들, 특징들, 및 이점들은 첨부 도면과 함께 다음의 상세한 설명으로부터 더욱 명백해질 것이며, 여기서:

[20] 도 1은 본 개시의 일 실시 예에 따른 네트워크 환경 내의 전자 장치를 개략적으로 도시한 블록도이다;

[21] 도 2는 본 개시의 일 실시 예에 따른 전자 장치의 블록도이다;

[22] 도 3은 본 개시의 일 실시 예에 따른 장치 프로비저닝 프로토콜(Device Provisioning Protocol: DPP) 네트워크의 아키텍처를 개략적으로 도시한 도면이다;

[23] 도 4는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 네트워크 구축 동작을 개략적으로 도시한 도면이다;

[24] 도 5는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 등록 동작을 개략적으로 도시한 도면이다;

[25] 도 6은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 네트워크 연결 동작을 개략적으로 도시한 도면이다;

[26] 도 7은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 프로비져닝 프로세스를 개략적으로 도시한 도면이다;

[27] 도 8은 본 개시의 일 실시 예에 따른 커넥터를 사용하는 네트워크 억세스 동작을 개략적으로 도시하고 있는 신호 흐름도이다;

[28] 도 9a는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 순서도이다;

[29] 도 9b는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 순서도이다;

[30] 도 10은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 구성자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 도면이다;

[31] 도 11은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 구성자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 신호 흐름도이다;

[32] 도 12는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 등록자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 도면이다;

[33] 도 13은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 등록자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 신호 흐름도이다;

[34] 도 14는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 도면이다.

[35] 도 15는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 신호 흐름도이다.

[36] 도면들 전반에 걸쳐, 동일한 참조 번호들은 동일하거나 유사한 엘리먼트들, 특징들 및 구조들을 설명하는 데 사용된다는 점에 유의하여야만 한다.

발명의 실시를 위한 형태

[37] 첨부된 도면들을 참조로 하는 하기의 상세한 설명은 청구항들 및 그 균등물들에 의해 정의되는 바와 같은 본 개시의 다양한 실시 예들의 전반적인 이해를 돕기 위해 제공된다. 이는 그 이해를 돕기 위한 다양한 특정 세부 사항들을 포함하고 있지만, 이들은 단지 예시적인 것으로 간주될 것이다.

따라서, 해당 기술 분야의 당업자들은 본 개시의 범위 및 사상을 벗어나지 않고 여기에서 설명되고 있는 다양한 실시 예들의 다양한 변경들 및 수정들이 이루어질 수 있음을 인식할 것이다. 게다가, 명확성과 간결성을 위해 공지의 기능들 및 구성들에 대한 설명은 생략될 수 있다.

[38] 하기의 상세한 설명 및 청구항들에서 사용되는 용어들 및 단어들은 서지적 의미들에 한정되지 않고, 발명자에 의한 본 개시의 명확하고 일관된 이해를 가능하게 하기 위해 사용된 것에 불과하다. 따라서, 본 개시의 다양한 실시 예들에 대한 하기의 상세한 설명은 첨부된 청구항들 및 그 균등물들에 의해 정의되는 바와 같은 본 개시를 제한하기 위한 것이 아니라, 단지 예시의 목적으로 제공된다는 것이 해당 기술 분야의 당업자들에게 명백해야만 할 것이다.

[39] 단수 형태들 "한(a)", "한(an)", 및 "상기(the)"는 문맥이 명백하게 달리 지시하지 않는 한, 복수 지시 대상들을 포함하는 것으로 이해될 것이다. 따라서, 예를 들어 "컴포넌트 표면(component surface)"에 대한 참조는 그와 같은 표면들 중 하나 또는 그 이상에 대한 참조를 포함한다.

[40] 본 명세서에서 사용되는 기술적 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 개시의 다양한 실시 예들을 한정하려는 의도가 아님을 유의해야 한다. 또는, 본 명세서에서 사용되는 기술적 용어는 본 명세서에서 특별히 다른 의미로 정의되지 않는 한, 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 의미로 해석되어야 하며, 과도하게 포괄적인 의미로 해석되거나, 과도하게 축소된 의미로 해석되지 않아야 한다. 또는, 본 명세서에서 사용되는 기술적인 용어가 본 개시의 사상을 정확하게 표현하지 못하는 잘못된 기술적 용어일 때에는, 당업자가 올바르게 이해할 수 있는 기술적 용어로 대체되어 이해되어야 할 것이다. 또는, 본 개시의 다양한 실시 예들에서 사용되는 일반적인 용어는 사전에 정의되어 있는 바에 따라, 또는 전후 문맥상에 따라 해석되어야 하며, 과도하게 축소된 의미로 해석되지 않아야 한다.

[41] 본 출원에서, "구성된다" 또는 "포함한다" 등의 용어는 명세서 상에 기재된 여러 구성 요소들, 또는 여러 동작들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 동작들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 동작들을 더 포함할 수 있는 것으로 해석되어야 한다.

[42] 또는, 본 명세서에서 사용되는 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 개시의 권리 범위를 벗어나지 않으면서 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.

[43] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[44] 이하, 첨부된 도면을 참조하여 본 개시에 따른 다양한 실시 예들을 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 또는, 본 개시의 다양한 실시 예들을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 개시의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또는, 첨부된 도면은 본 개시의 사상을 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 개시의 사상이 제한되는 것으로 해석되어서는 아니 됨에 유의하여야만 한다. 본 개시의 사상은 첨부된 도면들 외에 모든 변경들, 균등물들 내지 대체물들에 까지도 확장되는 것으로 해석되어야 한다.

[45] 이하, 본 개시의 다양한 실시 예들에서는 단말(terminal)을 설명할 것이나, 단말은 전자 장치(electronic device), 이동국(mobile station), 이동 장비(mobile equipment: ME), 사용자 장비(user equipment: UE), 사용자 단말(user terminal: UT), 가입자국(subscriber station: SS), 무선 장치(wireless device), 휴대 장치(handheld device), 억세스 단말(access terminal: AT)로 칭해질 수 있다. 또는, 본 개시의 다양한 실시 예들에서 단말은 예를 들어 휴대폰, 개인용 디지털 기기(personal digital assistant: PDA), 스마트 폰(smart phone), 무선 모뎀(wireless MODEM), 노트북과 같이 통신 기능을 갖춘 장치가 될 수 있다.

[46] 또는, 본 개시의 다양한 실시 예들을 구체적으로 설명함에 있어서, 무선 억세스 표준화 단체인 IEEE(institute of electrical and electronics engineers)와 와이파이 얼라이언스(Wi-Fi alliance: WFA)에서 제공하는 규격들을 참조로 할 것이지만, 본 개시의 주요한 요지는 유사한 기술적 배경을 가지는 여타의 통신 시스템들에도 본 개시의 범위를 크게 벗어 나지 아니 하는 범위에서 약간의 변형으로 적용 가능하며, 이는 본 개시의 기술 분야에서 숙련된 기술적 지식을 가진 자의 판단으로 가능할 것이다.

[47] 도 1은 본 개시의 일 실시 예에 따른 네트워크 환경(100) 내의 전자 장치(101)를 개략적으로 도시한 블록도이다.

[48] 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. 본 개시의 일 실시 예에 따르면, 전자 장치(101)는 서버(108)를 통하여 전자 장치(104)와 통신할 수 있다. 본 개시의 일 실시 예에 따르면, 전자 장치(101)는 프로세서(120), 메모리(130), 입력

모듈(150), 음향 출력 모듈(155), 디스플레이 모듈(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 연결 단자(178), 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. 본 개시의 어떤 실시 예들에서는, 전자 장치(101)에는, 이 구성요소들 중 적어도 하나(예: 연결 단자(178))가 생략되거나, 하나 이상의 다른 구성요소가 추가될 수 있다. 본 개시의 어떤 실시 예들에서는, 이 구성요소들 중 일부들(예: 센서 모듈(176), 카메라 모듈(180), 또는 안테나 모듈(197))은 하나의 구성요소(예: 디스플레이 모듈(160))로 통합될 수 있다.

[49] 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. 본 개시의 일 실시 예에 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 저장하고, 휘발성 메모리(132)에 저장된 명령 또는 데이터를 처리하고, 결과 데이터를 비 휘발성 메모리(134)에 저장할 수 있다. 본 개시의 일 실시 예에 따르면, 프로세서(120)는 메인 프로세서(121)(예: 중앙 처리 장치 또는 어플리케이션 프로세서) 또는 이와는 독립적으로 또는 함께 운영 가능한 보조 프로세서(123)(예: 그래픽 처리 장치, 신경망 처리 장치(NPU: neural processing unit), 이미지 시그널 프로세서, 센서 허브 프로세서, 또는 커뮤니케이션 프로세서)를 포함할 수 있다. 예를 들어, 전자 장치(101)가 메인 프로세서(121) 및 보조 프로세서(123)를 포함하는 경우, 보조 프로세서(123)는 메인 프로세서(121)보다 저전력을 사용하거나, 지정된 기능에 특화되도록 설정될 수 있다. 보조 프로세서(123)는 메인 프로세서(121)와 별개로, 또는 그 일부로서 구현될 수 있다.

[50] 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: 디스플레이 모듈(160), 센서 모듈(176), 또는 통신 모듈(190))와 관련된 기능 또는 상태들의 적어도 일부를 제어할 수 있다. 본 개시의 일 실시 예에 따르면, 보조 프로세서(123)(예: 이미지 시그널 프로세서 또는 커뮤니케이션 프로세서)는 기능적으로 관련 있는 다른 구성요소(예: 카메라 모듈(180) 또는 통신 모듈(190))의 일부로서 구현될 수 있다. 본 개시의 일 실시 예에 따르면, 보조 프로세서(123)(예: 신경망 처리 장치)는 인공지능 모델의 처리에 특화된 하드웨어 구조를 포함할 수 있다. 인공지능 모델은 기계 학습을 통해 생성될 수 있다. 이러한 학습은, 예를 들어, 인공지능이 수행되는 전자 장치(101) 자체에서 수행될 수 있고, 별도의 서버(예: 서버(108))를 통해 수행될 수도 있다. 학습

알고리즘은, 예를 들어, 지도형 학습(supervised learning), 비지도형 학습(unsupervised learning), 준지도형 학습(semi-supervised learning) 또는 강화 학습(reinforcement learning)을 포함할 수 있으나, 전술한 예에 한정되지 않는다. 인공지능 모델은, 복수의 인공 신경망 레이어들을 포함할 수 있다. 인공 신경망은 심층 신경망(DNN: deep neural network), CNN(convolutional neural network), RNN(recurrent neural network), RBM(restricted boltzmann machine), DBN(deep belief network), BRDNN(bidirectional recurrent deep neural network), 심층 Q-네트워크(deep Q-networks) 또는 상기 중 둘 이상의 조합 중 하나일 수 있으나, 전술한 예에 한정되지 않는다. 인공지능 모델은 하드웨어 구조 이외에, 추가적으로 또는 대체적으로, 소프트웨어 구조를 포함할 수 있다.

[51] 메모리(130)는, 전자 장치(101)의 적어도 하나의 구성요소(예: 프로세서(120) 또는 센서 모듈(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 비 휘발성 메모리(134)를 포함할 수 있다.

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

[53] 입력 모듈(150)은, 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 모듈(150)은, 예를 들면, 마이크, 마우스, 키보드, 키(예: 버튼), 또는 디지털 펜(예: 스타일러스 펜)을 포함할 수 있다.

[54] 음향 출력 모듈(155)은 음향 신호를 전자 장치(101)의 외부로 출력할 수 있다. 음향 출력 모듈(155)은, 예를 들면, 스피커 또는 리시버를 포함할 수 있다. 스피커는 멀티미디어 재생 또는 녹음 재생과 같이 일반적인 용도로 사용될 수 있다. 리시버는 착신 전화를 수신하기 위해 사용될 수 있다. 본 개시의 일 실시 예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

[55] 디스플레이 모듈(160)은 전자 장치(101)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 디스플레이 모듈(160)은, 예를 들면, 디스플레이, 홀로그램 장치, 또는 프로젝터 및 해당 장치를 제어하기 위한 제어 회로를 포함할 수 있다. 본 개시의 일 실시 예에 따르면, 디스플레이 모듈(160)은 터치를 감지하도록 설정된 터치 센서, 또는 상기 터치에 의해 발생되는 힘의 세기를 측정하도록 설정된 압력 센서를 포함할 수 있다.

[56] 오디오 모듈(170)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 본 개시의 일 실시 예에 따르면, 오디오 모듈(170)은, 입력 모듈(150)을 통해 소리를 획득하거나, 음향 출력 모듈(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.

[57] 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. 본 개시의 일 실시 예에 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.

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

[59] 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. 본 개시의 일 실시 예에 따르면, 연결 단자(178)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.

[60] 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. 본 개시의 일 실시 예에 따르면, 햅틱 모듈(179)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.

[61] 카메라 모듈(180)은 정지 영상 및 동영상을 촬영할 수 있다. 본 개시의 일 실시 예에 따르면, 카메라 모듈(180)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.

[62] 전력 관리 모듈(188)은 전자 장치(101)에 공급되는 전력을 관리할 수 있다. 본 개시의 일 실시 예에 따르면, 전력 관리 모듈(188)은, 예를 들면, PMIC(power management integrated circuit)의 적어도 일부로서 구현될 수 있다.

[63] 배터리(189)는 전자 장치(101)의 적어도 하나의 구성요소에 전력을 공급할 수 있다. 본 개시의 일 실시 예에 따르면, 배터리(189)는, 예를 들면, 재충전 불가능한 1차 전지, 재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.

[64] 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. 본 개시의 일 실시 예에 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, 와이파이(Wi-Fi:

wireless fidelity) direct 또는 IrDA(infrared data association)와 같은 근거리 통신 네트워크) 또는 제 2 네트워크(199)(예: 레거시 셀룰러 네트워크, 5세대 (5th generation: 5G) 네트워크, 차세대 통신 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부의 전자 장치(104)와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성요소(예: 단일 칩)로 통합되거나, 또는 서로 별도의 복수의 구성요소들(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 또는 인증할 수 있다.

[65] 무선 통신 모듈(192)은 4세대 (4th generation: 4G) 네트워크 이후의 5G 네트워크 및 차세대 통신 기술, 예를 들어, NR 접속 기술(new radio access technology)을 지원할 수 있다. NR 접속 기술은 고용량 데이터의 고속 전송(eMBB(enhanced mobile broadband)), 단말 전력 최소화와 다수 단말의 접속(mMTC(massive machine type communications)), 또는 고신뢰도와 저지연(URLLC(ultra-reliable and low-latency communications))을 지원할 수 있다. 무선 통신 모듈(192)은, 예를 들어, 높은 데이터 전송률 달성을 위해, 고주파 대역(예: mmWave 대역)을 지원할 수 있다. 무선 통신 모듈(192)은 고주파 대역에서의 성능 확보를 위한 다양한 기술들, 예를 들어, 빔포밍(beamforming), 거대 배열 다중 입출력(massive MIMO(multiple-input and multiple-output)), 전차원 다중입출력(FD-MIMO: full dimensional MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 또는 대규모 안테나(large scale antenna)와 같은 기술들을 지원할 수 있다. 무선 통신 모듈(192)은 전자 장치(101), 외부 전자 장치(예: 전자 장치(104)) 또는 네트워크 시스템(예: 제 2 네트워크(199))에 규정되는 다양한 요구사항을 지원할 수 있다. 본 개시의 일 실시 예에 따르면, 무선 통신 모듈(192)은 eMBB 실현을 위한 Peak data rate(예: 20Gbps 이상), mMTC 실현을 위한 손실 Coverage(예: 164dB 이하), 또는 URLLC 실현을 위한 U-plane latency(예: 다운링크(DL) 및 업링크(UL) 각각 0.5ms 이하, 또는 라운드 트립 1ms 이하)를 지원할 수 있다.

[66] 안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부의 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 본 개시의 일 실시 예에 따르면, 안테나 모듈(197)은 서브스트레이트(예: PCB) 위에 형성된 도전체 또는 도전성 패턴으로 이루어진 방사체를 포함하는 안테나를 포함할 수 있다. 본 개시의 일 실시 예에 따르면, 안테나 모듈(197)은 복수의 안테나들(예: 어레이 안테나)을 포함할 수 있다. 이런 경우, 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 상기 복수의 안테나들로부터 선택될 수 있다. 신호 또는 전력은 상기 선택된 적어도 하나의 안테나를 통하여 통신 모듈(190)과

외부의 전자 장치 간에 송신되거나 수신될 수 있다. 본 개시의 일 실시 예에 따르면, 방사체 이외에 다른 부품(예: RFIC(radio frequency integrated circuit))이 추가로 안테나 모듈(197)의 일부로 형성될 수 있다.

[67] 본 개시의 다양한 실시 예들에 따르면, 안테나 모듈(197)은 mmWave 안테나 모듈을 형성할 수 있다. 본 개시의 일 실시 예에 따르면, mmWave 안테나 모듈은 인쇄 회로 기판, 상기 인쇄 회로 기판의 제 1 면(예: 아래 면)에 또는 그에 인접하여 배치되고 지정된 고주파 대역(예: mmWave 대역)을 지원할 수 있는 RFIC, 및 상기 인쇄 회로 기판의 제 2 면(예: 윗면 또는 측 면)에 또는 그에 인접하여 배치되고 상기 지정된 고주파 대역의 신호를 송신 또는 수신할 수 있는 복수의 안테나들(예: 어레이 안테나)을 포함할 수 있다.

[68] 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))을 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.

[69] 본 개시의 일 실시 예에 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. 외부의 전자 장치(102, 또는 104) 각각은 전자 장치(101)와 동일한 또는 다른 종류의 장치일 수 있다. 본 개시의 일 실시 예에 따르면, 전자 장치(101)에서 실행되는 동작들의 전부 또는 일부는 외부의 전자 장치들(102, 104, 또는 108) 중 하나 이상의 외부의 전자 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 외부의 전자 장치들에게 그 기능 또는 그 서비스의 적어도 일부를 수행하라고 요청할 수 있다. 상기 요청을 수신한 하나 이상의 외부의 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, 모바일 에지 컴퓨팅(MEC: mobile edge computing), 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다. 전자 장치(101)는, 예를 들어, 분산 컴퓨팅 또는 모바일 에지 컴퓨팅을 이용하여 초저지연 서비스를 제공할 수 있다. 본 개시의 다른 실시 예에 있어서, 외부의 전자 장치(104)는 IoT(internet of things) 기기를 포함할 수 있다. 서버(108)는 기계 학습 및/또는 신경망을 이용한 지능형 서버일 수 있다. 본 개시의 일 실시 예에 따르면, 외부의 전자 장치(104) 또는 서버(108)는 제 2 네트워크(199) 내에 포함될 수 있다. 전자 장치(101)는 5G 통신 기술 및 IoT 관련 기술을 기반으로 지능형 서비스(예: 스마트 홈, 스마트 시티, 스마트 카, 또는 헬스 케어)에 적용될 수 있다.

[70] 본 문서에 개시된 다양한 실시 예들에 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 실시 예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

[71] 본 문서의 다양한 실시 예들 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시 예들로 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.

[72] 본 문서의 다양한 실시 예들에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구현된 유닛을 포함할 수 있으며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로와 같은 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, 본 개시의 일 실시 예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

[73] 본 문서의 다양한 실시 예들은 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 저장 매체는, 비일시적(non-transitory) 저장 매체의 형태로 제공될 수 있다.

여기서, '비일시적'은 저장 매체가 실재(tangible)하는 장치이고, 신호(signal)(예: 전자기파)를 포함하지 않는다는 것을 의미할 뿐이며, 이 용어는 데이터가 저장 매체에 반영구적으로 저장되는 경우와 임시적으로 저장되는 경우를 구분하지 않는다.

[74] 본 개시의 일 실시 예에 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: 스마트 폰들) 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.

[75] 본 개시의 다양한 실시 예들에 따르면, 상기 기술한 구성요소들의 각각의 구성요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있으며, 복수의 개체 중 일부는 다른 구성요소에 분리 배치될 수도 있다. 본 개시의 다양한 실시 예들에 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. 본 개시의 다양한 실시 예들에 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.

[76] 한편, WFA에서는 Wi-Fi 기술을 기반으로 하는 장치 프로비져닝 프로토콜(device provisioning protocol: DPP)를 제안한 바 있으며, DPP는 사용자 인터페이스(user interface: UI)를 구비하고 있지 않거나 또는 제한적인 UI를 구비하고 있는 Wi-Fi 장치를 간단하면서도 효율적으로 Wi-Fi 네트워크에 연결할 수 있는 프로토콜이다.

[77] 도 2는 본 개시의 일 실시 예에 따른 전자 장치(101)의 블록도이다.

[78] 도 2를 참조하면, 전자 장치(예: 도 1의 전자 장치(101))는 DPP를 구현하는 장치일 수 있다. 이하, 설명의 편의상 DPP를 구현하는 장치를 DPP 장치라 칭하기로 한다.

[79] 전자 장치(101)는 외부 전자 장치(예: 도 1의 전자 장치(102 또는 104)), 예를

들어 피어 장치(peer device)와 하나 또는 그 이상의 안테나들(201)을 사용하여 신호들을 송수신하는 통신 회로(202)(예: 도 1의 통신 모듈(190))를 포함할 수 있다.

[80] 전자 장치(101)는 하나 또는 그 이상의 단일 코어 프로세서들 또는 하나 또는 그 이상의 다중 코어 프로세서들로 구현될 수 있는 적어도 하나의 프로세서(204)(예: 도 1의 프로세서(120))와, 전자 장치(101)의 동작을 위한 인스트럭션(instruction)들을 저장하는 메모리(206)(예: 도 1의 메모리(130))를 포함할 수 있다.

[81] 전자 장치(101)는 네트워크 외부의 구성 요소(component)들과 통신하기 위한 유선 및/또는 무선 인터페이스를 제공하는 인터페이스 모듈(208)(예: 도 1의 인터페이스(177))를 포함할 수 있다. 하나 또는 그 이상의 안테나들(201), 통신 회로(202), 또는 인터페이스 모듈(208) 중 적어도 일부는, 예를 들어 도 1의 통신 모듈(190) 및 안테나 모듈(198)의 적어도 일부로 구현될 수 있다.

[82] 본 개시의 다양한 실시 예들에 따르면, 전자 장치(예: 도 1의 전자 장치(101))는 통신 회로(예: 도 2의 통신 회로(202)), 적어도 하나의 프로세서(예: 도 2의 프로세서(204))를 포함할 수 있다. 상기 적어도 하나의 프로세서는 상기 통신 회로를 통해, 외부 전자 장치(예: 도 1의 전자 장치(102) 또는 전자 장치(104))로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하고, 설정되어 있는 필터링 방식을 기반으로 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치(102 또는 104)로 송신할 적어도 하나의 네트워크 구성 정보를 선택하고, 상기 통신 회로(202)를 통해, 상기 외부 전자 장치(102 또는 104)로 상기 선택한 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 송신하도록 설정될 수 있다. 일 실시 예에서, 네트워크 구성 정보는 DPP 구성 오브젝트(DPP configuration object)가 될 수 있다. 일 실시 예에서, 네트워크 구성 정보를 요청하는 제1 메시지는 DPP 구성 요청 프레임(DPP configuration request frame)이 될 수 있다. 일 실시 예에서, 전자 장치(101)에 의해 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지는 DPP 구성 응답 프레임(DPP configuration response frame)이 될 수 있다.

[83] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식은 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식 또는 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식 중 적어도 하나를 포함할 수 있다. 일 실시 예에서, 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있으며, 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식은 등록자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있다.

[84] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식은 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식, 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식, 또는 적어도 하나의 필터링

조건을 포함하는 세컨더리(secondary) 필터링 방식 중 적어도 하나를 포함할 수 있다.

[85] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 적어도 하나의 프로세서(204)는 상기 통신 회로(202)를 통해, 스캔 동작을 수행하여 다른 외부 전자 장치들(예: 도 1의 전자 장치(102) 또는 전자 장치(104))을 검출하고, 상기 검출된 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)를 선택하고, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하도록 설정될 수 있다.

[86] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 적어도 하나의 프로세서(204)는 상기 통신 회로(202)를 통해, 상기 외부 전자 장치(102 또는 104)로부터 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 수신하고, 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 다른 외부 전자 장치들(102 또는 104)을 확인하고, 상기 확인된 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)를 선택하고, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하도록 설정될 수 있다.

[87] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 적어도 하나의 필터링 조건을 포함하는 세컨더리(secondary) 필터링 방식일 경우, 상기 적어도 하나의 프로세서(204)는 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 적어도 하나의 필터링 조건을 만족하는 적어도 하나의 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하도록 설정될 수 있다.

[88] 본 개시의 다양한 실시 예들에 따르면, 상기 적어도 하나의 필터링 조건은, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 세컨더리 필터링 방식이 적용되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제1 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)가 설정되어 있는 기간 내에 억세스한 기록을 가지는 적어도 하나의

다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제2 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)와 설정되어 있는 거리 내에 존재하는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제3 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상위 계층을 통해 선택되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제4 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 채널 품질이 임계 채널 품질 이상인 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제5 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 네트워크 품질을 기반으로 선택되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제6 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)와 설정되어 있는 거리 내에 존재하고, 상기 전자 장치(101)가 설정되어 있는 기간 내에 억세스한 기록을 가지는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제7 조건, 또는 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)와 설정되어 있는 거리 내에 존재하고, 상위 계층을 통해 선택되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제8 조건 중 적어도 하나를 포함할 수 있다.

[89] 본 개시의 다양한 실시 예들에 따르면, 상기 적어도 하나의 프로세서(204)는 상기 통신 회로(202)를 통해, 상기 외부 전자 장치(102 또는 104)와 보안 정보를 기반으로 인증 동작을 수행하도록 더 설정될 수 있다. 본 개시의 일 실시 예에서, 인증 동작은 상기 전자 장치(101)와 외부 전자 장치(102 또는 104)간에 DPP 인증 요청 프레임 및 DPP 인증 응답 프레임이 송수신되는 동작을 포함할 수 있다. 본 개시의 일 실시 예에서, 상기 DPP 인증 요청 프레임에 포함되는 응답자(responder)의 공중 부트스트래핑 키(public bootstrapping key)에 대한

해쉬(hash), 개시자(initiator)의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 프로토콜 키, 또는 제1 중개키로 인크립트된 개시자 넌스 어트리뷰트(initiator nonce attribute)와 개시자 능력들 어트리뷰트(initiator capabilities attribute) 중 적어도 하나는 인증 동작, 예를 들어 DPP 인증 동작에서 사용되는 보안 정보일 수 있다. 본 개시의 일 실시 예에서, 상기 DPP 인증 응답 프레임에 포함되는 응답자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 부트스트래핑 키에 대한 해쉬, 응답자의 공중 프로토콜 키, 또는 제2 중개키로 인크립트된 응답자 넌스 어트리뷰트(responder nonce attribute), 응답자 능력들 어트리뷰트(responder capabilities attribute), 및 개시자 능력들 어트리뷰트 중 적어도 하나는 인증 동작, 예를 들어 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[90] 본 개시의 다양한 실시 예들에 따르면, 전자 장치(예: 도 1의 전자 장치(101))는 통신 회로(예: 도 2의 통신 회로(202)), 적어도 하나의 프로세서(예: 도 2의 프로세서(204))를 포함할 수 있다. 상기 적어도 하나의 프로세서(204)는 상기 통신 회로(202)를 통해, 상기 통신 회로(202)를 통해, 외부 전자 장치(예: 도 1의 전자 장치(102) 또는 전자 장치(104))와 보안 정보를 기반으로 인증 동작을 수행하고, 상기 통신 회로(202)를 통해, 상기 외부 전자 장치(102 또는 104)로 네트워크 구성 정보를 요청하는 제1 메시지를 송신하고, 상기 통신 회로(202)를 통해, 상기 외부 전자 장치(102 또는 104)로부터 상기 외부 전자 장치(102 또는 104)에 저장되어 있는 다수의 네트워크 구성 정보들 중 설정되어 있는 필터링 방식을 기반으로 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 수신하도록 설정될 수 있다. 본 개시의 일 실시 예에서, 네트워크 구성 정보는 DPP 구성 오브젝트가 될 수 있다. 본 개시의 일 실시 예에서, 네트워크 구성 정보를 요청하는 제1 메시지는 DPP 구성 요청 프레임이 될 수 있다. 본 개시의 일 실시 예에서, 외부 전자 장치(102 또는 104)에 의해 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지는 DPP 구성 응답 프레임이 될 수 있다.

[91] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식은 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식, 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식, 또는 적어도 하나의 필터링 조건을 포함하는 세컨더리 필터링 방식 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있으며, 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식은 등록자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있다.

[92] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 적어도 하나의 프로세서(204)는 상기 통신 회로(202)를 통해, 상기 외부 전자 장치(102 또는 104)로 상기 전자 장치(101)의 스캔 결과를 송신하도록 더 설정될 수 있고, 상기

제2 메시지에 포함되어 있는 적어도 하나의 네트워크 구성 정보는 상기 외부 전자 장치(102 또는 104)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 스캔 결과에 상응하는 다른 외부 전자 장치들(예: 도 1의 전자 장치(102) 또는 전자 장치(104)) 중 상기 외부 전자 장치(102 또는 104)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보일 수 있다.

[93] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 제2 메시지에 포함되어 있는 적어도 하나의 네트워크 구성 정보는, 상기 외부 전자 장치(102 또는 104)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 검출된 다른 외부 전자 장치들(102 또는 104) 중 상기 외부 전자 장치(102 또는 104)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보일 수 있다.

[94] WFA에서 제안하고 있는 DPP에 대해서 구체적으로 설명하면 다음과 같다.

[95] 본 개시의 일 실시 예에서, Wi-Fi 장치를 간편하고 안전하게 네트워크에 연결할 수 있는 프로세스를 제공하는 것은 Wi-Fi 기술의 지속적인 성장과 확대를 위해 필수적일 수 있다. 특히, UI를 구비하고 있지 않거나, 또는 UI를 구비하고 있을지라도 그 UI에 제한이 있는 Wi-Fi 장치들이 많은 스마트 홈 또는 IoT와 같은 마켓에서는 Wi-Fi 장치를 간편하고 안전하게 네트워크에 연결할 수 있는 프로세스를 제공하는 것이 보다 필수적일 수 있다.

[96] Wi-Fi 장치의 네트워크 연결을 구성하기 위해서는 Wi-Fi 장치로 네트워크 정보와 보안 크리덴셜(secure credential)이 제공되어야만 할 수 있다. 본 개시의 일 실시 예에서, 보안 크리덴셜은 Wi-Fi 심플 구성 규격(Wi-Fi simple configuration specification)에서 정의된 바와 같은 피어-대-피어(peer-to-peer: P2P) 그룹에 조인(join)하기 위해 필요로 되는 정보일 수 있다. UI를 구비하고 있지 않거나, 또는 그 UI에 제한이 있는 Wi-Fi 장치를 네트워크에 추가하는 동작은 번거로울 뿐만 아니라, Wi-Fi 장치의 제조사마다 다른 방식으로 이루어질 수 있다.

[97] Wi-Fi 장치를 간단하면서도 효율적으로 Wi-Fi 네트워크에 연결시킬 수 있는 Wi-Fi 장치 구성 방식에 대한 필요성이 대두되고 있고, 이를 위해, WFA 에서는 UI를 구비하고 있지 않거나 또는 제한적인 UI를 구비하고 있는 Wi-Fi 장치를 간단하면서도 효율적으로 Wi-Fi 네트워크에 연결할 수 있는 DPP를 개발한 바 있다.

[98] DPP에서는, 표준화된 메커니즘(mechanism)을 기반으로, Wi-Fi 장치의 구성을 간략화시킬 수 있고, 예를 들어 스마트 폰으로 제품 QR (quick response) 코드를 스캔하는 것과 같은 비교적 쉬운 방식으로 Wi-Fi 장치를 Wi-Fi 네트워크에 바로 연결시킬 수 있다. 본 개시의 일 실시 예에서, DPP 는 예를 들어, 네트워크 셋업과 클라이언트 장치(client device) 프로비저닝을 간략화시키는 동시에 향상된

사용자 경험, 강화된 보안, 및/또는 IoT 장치 프로비져닝 지원을 제공할 수 있다.

[99] 본 개시의 다양한 실시 예들에 따르면, DPP 에서는, 예를 들어 가정이나 사무실과 같은, 네트워크에서 네트워크 관리자가 신뢰성 있는 장치, 예를 들어 스마트 폰과 같은 신뢰성 있는 장치를 사용하여 억세스 포인트(access point: AP)를 셋업하고, 다른 클라이언트 장치, 예를 들어 다른 클라이언트 Wi-Fi 장치들의 네트워크 억세스들을 관리할 수 있다. 예를 들어, DPP는 스무스한(smooth) 사용자 경험을 지원하는 동시에 강력한 암호 원칙을 사용하여 보안 네트워크 연결을 유지할 수 있도록 하는 프로토콜이다.

[100] 도 3은 본 개시의 일 실시 예에 따른 DPP 네트워크의 아키텍쳐를 개략적으로 도시한 도면이다.

[101] 본 개시의 일 실시 예에서, 도 3에 도시되어 있는 DPP 네트워크의 아키텍쳐는 Wi-Fi 프로비져닝 역할(Wi-Fi provisioning role)에 따른 아키텍쳐임에 유의하여야만 할 것이다.

[102] 도 3을 참조하면, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자 장치(예: 제1 전자 장치(310))와, 외부 전자 장치들(예: 제2 전자 장치(320), 제3 전자 장치(330))을 포함할 수 있다. 본 개시의 일 실시 예에서, 제1 전자 장치(310), 제2 전자 장치(320), 제3 전자 장치(330) 각각은 DPP 장치일 수 있다.

[103] DPP 아키텍처는 DPP 부트스트래핑(bootstrapping) 동작, DPP 인증(authentication) 동작, DPP 프로비져닝(provisioning)(또는 구성(configuration)) 동작, 및 DPP 연결성(connectivity)(또는 소개(introduction)) 동작 동안 장치 역할(device role)들을 정의하며, 장치 역할들은 2개의 타입들, 예를 들어 구성자(configurator) 및 등록자(enrollee), 또는 개시자(initiator) 및 응답자(responder)를 포함할 수 있다. 도 3에서, 제1 전자 장치(310)는 구성자로서 동작하고, 제2 전자 장치(320)와 제3 전자 장치(330)는 각각 등록자로서 동작할 수 있다.

[104] DPP 네트워크에서, 구성자는 장치 대 장치 (device-to-device: D2D) 통신 또는 인프라스트럭쳐 (infrastructure) 통신을 위해 장치들을 등록하고 프로비젼하는 능력들을 가지는 논리 엔터티(logical entity)일 수 있다.

[105] DPP 네트워크에서, 개시자는 DPP 인증 프로토콜을 개시하는 DPP 장치를 나타내며, 구성자 또는 등록자 중 어느 하나가 개시자가 될 수 있다. 본 개시의 일 실시 예에서, 응답자는 개시자에 의한 DPP 인증 프로토콜의 개시에 응답하는 DPP 장치를 나타내며, 구성자 또는 등록자 중 어느 하나가 응답자가 될 수 있다.

[106] 구성자는 등록자의 셋업을 지원하고, 구성자와 등록자는 DPP 부트스트래핑 동작, DPP 인증 동작 및 DPP 구성 동작에 관여될 수 있다. 구성자 또는 등록자는 DPP 부트스트래핑 동작 및 DPP 인증 동작에서 개시자로 동작할 수 있다. 이와는 달리, DPP 구성 동작 및 DPP 소개 동작은 등록자만 개시할 수 있다.

[107] 구성자 및 등록자는 DPP 인증 동작을 시작하기 전에 동일한 타원 곡선(elliptic curve)으로부터의 부트스트래핑 키들을 소유할 수 있다. 본 개시의 일 실시

예에서, 타원 곡선은 암호키들을 생성하는데 사용되는 알고리즘일 수 있다. 본 개시의 일 실시 예에서, 필요할 경우 (그리고 부트스트래핑 방법에 따라), 부트스트래핑 키들이 요청시 생성될 수 있다. DPP 인증 동작은 개시자가 이전 부트스트래핑 메커니즘의 일부로서 응답자의 부트스트래핑 키를 획득하는 것을 요구할 수 있다. 선택적으로, DPP 인증 동작에서 구성자 및 등록자는 상호 인증을 제공하기 위해 구성자 및 등록자 서로의 부트스트래핑 키들을 획득할 수 있다.

[108] 인증이 완료된 후, 구성자는 D2D 통신 또는 인프라스트럭처 통신을 위해 등록자를 프로비젼할 수 있다. 이런 프로비져닝의 일부로서, 구성자는 등록자가 DPP 네트워크에서 다른 피어(peer)들, 예를 들어 다른 외부 전자 장치들과 보안 연관(secure association)들을 설정하는 것을 가능하게 할 수 있다.

[109] 본 개시의 일 실시 예에서, 구성자 및 등록자에 대해서 구체적으로 설명하면 다음과 같다.

[110] 첫 번째로, 구성자에 대해서 설명하기로 한다.

[111] DPP 네트워크에서 특정한 DPP 장치, 예를 들어 메인 DPP 장치가 구성자로 지정될 수 있다. 구성자는 중앙 구성 포인트로서, AP를 포함하는 DPP 네트워크에 포함되는 모든 DPP 장치들을 프로비젼할 수 있다. DPP 네트워크에 포함되어 있는 다양한 DPP 장치들 중 어느 하나가 구성자가 될 수 있다.

[112] 두 번째로, 등록자에 대해서 설명하기로 한다.

[113] 본 개시의 일 실시 예에서, 등록자는 DPP 네트워크의 네트워크 관리자가 DPP 네트워크에 연결하고자 하는 DPP 장치이다. DPP 네트워크에 추가되는 DPP 장치, 예를 들어 AP, 스마트 가전, 컴퓨터, 프린터, 또는 TV 가 등록자가 될 수 있으며, 구성자를 제외한, Wi-Fi 기능을 구현할 수 있는 모든 DPP 장치들이 등록자가 될 수 있다.

[114] 도 4는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 네트워크 구축 동작을 개략적으로 도시한 도면이다.

[115] 도 4를 참조하면, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자 장치(예: 제1 전자 장치(410))와 외부 전자 장치(예: 제2 전자 장치(420))를 포함할 수 있다. 도 4에서, 제1 전자 장치(410)와 제2 전자 장치(420) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(410)는 구성자로서 동작하고, 제2 전자 장치(420)는 AP 등록자로서 동작한다고 가정하기로 한다.

[116] 본 개시의 일 실시 예에서, 제1 전자 장치(410)는 DPP를 기반으로 등록자인 제2 전자 장치(420), 일 예로 초기 AP(420)를 프로비젼할 수 있다. 제1 전자 장치(410)는 다른 등록자들인 클라이언트 등록자(enrollee client)들(도 4에 별도로 도시되어 있지 않음)을 프로비젼하고, 따라서 등록자들이 DPP 네트워크를 검색하고, 선택하고, 연결할 수 있도록 할 수 있다.

[117] 도 4에 나타낸 바와 같이, 초기 등록 절차에서 DPP 네트워크의 네트워크 관리자는 이동 장치인 제1 전자 장치(410)를 구성자로 설정한 후, 제1 전자

장치(410)를 통해 등록자로 간주되는 AP(enrollee AP), 예를 들어 제2 전자 장치(420)를 구성할 수 있다. 이와 같은 AP 구성 동작은 네트워크 연결 전에 수행될 수 있으며, 이런 AP 구성 동작을 통해 DPP 네트워크가 구축될 수 있다.

[118] 도 5는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 등록 동작을 개략적으로 도시한 도면이다.

[119] 도 5를 참조하면, DPP 네트워크가 구축된 후 DPP 네트워크의 관리자는 DPP 장치들을 등록하는 등록 절차를 개시할 수 있다. 본 개시의 일 실시 예에서, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자 장치(예: 제1 전자 장치(510))와 외부 전자 장치들(예: 제2 전자 장치(520), 제3 전자 장치(530), 제4전자 장치(540), 또는 제5 전자 장치(550))을 포함할 수 있다. 도 5에서는, 제1 전자 장치(510)는 구성자로 동작하고, 제2 전자 장치(520), 제3 전자 장치(530), 제4전자 장치(540), 및 제5 전자 장치(550) 각각은 클라이언트 등록자로 동작한다고 가정하기로 한다.

[120] 제2 전자 장치(520), 제3 전자 장치(530), 제4전자 장치(540), 또는 제5 전자 장치(550) 중 적어도 하나는 제1 전자 장치(510)에서 프로비젼하는 정보를 기반으로 DPP 네트워크에 대한 연결을 위한 구성을 획득할 수 있다. 그리고 나서, 제1 전자 장치(510)는 해당 외부 전자 장치와 개별적인 보안 크리덴셜(secure credential)을 생성하고, 이에 따라 해당 외부 전자 장치는 DPP 네트워크에 대한 연결을 설정할 수 있다. 본 개시의 일 실시 예에서, 보안 크리덴셜은 피어-대-피어(peer to peer: P2P) 그룹에 조인하기 위해 필요로 되는 정보일 수 있다.

[121] 도 6은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 네트워크 연결 동작을 개략적으로 도시한 도면이다.

[122] 도 6을 참조하면, DPP 네트워크에 DPP 장치들이 등록된 후, 해당 클라이언트 등록자는 등록 절차에서 획득된 DPP 네트워크에 대한 연결을 위한 구성을 기반으로 AP(620)를 통해 DPP 네트워크를 탐색하고, 탐색된 DPP 네트워크에 연결할 수 있다. 본 개시의 일 실시 예에서, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자 장치(예: 제1 전자 장치(610))와 외부 전자 장치들(예: 제2 전자 장치(620), 제3 전자 장치(630), 제4전자 장치(640), 제5 전자 장치(650), 및 제6 전자 장치(660))를 포함할 수 있다. 도 6에서는, 제1 전자 장치(610)는 구성자로 동작하고, 제2 전자 장치(620)는 AP로서 동작하고, 제3 전자 장치(630), 제4전자 장치(640), 제5 전자 장치(650), 및 제6 전자 장치(660) 각각은 등록자로 동작한다고 가정하기로 한다.

[123] 본 개시의 일 실시 예에서, AP인 제2 전자 장치(620)는 구성자인 제1 전자 장치(610)와 연결되어 있고, 등록자들인 제3 전자 장치(630), 제4 전자 장치(640), 제5 전자 장치(650), 또는 제6 전자 장치(660) 중 적어도 하나는 제2 전자 장치(620)를 통해 DPP 네트워크를 탐색하고, 탐색된 DPP 네트워크에 연결할 수 있다.

[124] 한편, WFA는 Wi-Fi 네트워크에 Wi-Fi 장치를 추가하는 동작을 훨씬 간단하고 효율적으로 할 수 있도록 Wi-Fi Easy Connect를 개발한 바 있다. Wi-Fi Easy Connect는 부트스트래핑 메커니즘을 지원하며, 부트스트래핑 메커니즘은 Wi-Fi 장치 별 사용자의 작업을 최소화하면서 Wi-Fi 네트워크에 구성자와 등록자를 안전하게 추가할 수 있도록 하는 메커니즘이다. Wi-Fi Easy Connect는 부트스트래핑 메커니즘을 지원하기 위해 등록자 QR 코드를 사용할 수 있다.

[125] 본 개시의 일 실시 예에서, QR 코드는 예를 들어 보안 키, Wi-Fi 장치의 고유 식별자 같은, 다양한 정보들을 포함할 수 있다. QR 코드는 QR 코드 스캔 기능을 구비하는 Wi-Fi 장치에 의해 인식될 수 있으며, Wi-Fi 장치 인증을 위해 사용자가 직접 정보를 입력해야 하는 번거로움을 방지할 수 있다. 또는, QR 코드는 데이터 입력 에러로 발생할 수 있는 이슈 역시 방지할 수 있다.

[126] Wi-Fi Easy Connect 네트워크에서 QR 코드와 구성자를 사용한 프로비져닝 동작의 일 예에 대해서 설명하기로 한다.

[127] (1) 구성자가 구비하고 있는 카메라를 사용하여 등록자의 QR 코드가 스캔될 수 있다. QR 코드는 스티커 또는 카드의 형태로 제공될 수 있다.

[128] (2) 구성자는 QR 코드를 리드(read)하고, 해독하여 자동으로 등록자와 안전한 Wi-Fi 통신 링크를 검색하고, 검색 결과를 기반으로 등록자와 안전한 Wi-Fi 통신 링크를 설정할 수 있다.

[129] (3) 구성자는 보안 채널을 사용하여 등록자에 Wi-Fi 네트워크 정보를 구성할 수 있다.

[130] (4) 등록자에 대한 Wi-Fi 네트워크 정보 구성이 완료되면, 등록자는 구성자가 제공한 Wi-Fi 네트워크 정보를 사용하여 사용자의 개입 없이 Wi-Fi 네트워크를 탐색하고, 탐색 결과를 기반으로 특정 Wi-Fi 네트워크를 선택하고, 선택한 Wi-Fi 네트워크에 대한 연결 동작을 수행할 수 있다.

[131] 한편, Wi-Fi Easy Connect 네트워크에서 구성자가 QR 코드를 인식할 수 있는 기능을 구비하고 있지 않거나, 또는 등록자가 QR 코드를 디스플레이하는 기능을 구비하고 있지 않을 경우에는 사용자가 직접 스트링(string)을 입력함으로써 구성자와 등록자 간의 Wi-Fi 통신 링크 설정이 가능할 수 있다.

[132] 한편, Wi-Fi Easy Connect 기술은 다양한 방식들로 Wi-Fi 장치들을 프로비젼할 수 있도록 유연하게 설계되었으며, 구성자 또는 등록자가 프로비져닝 동작을 개시하도록 지원할 수 있다. 상기에서 설명한 바와 같은 프로비져닝 동작의 일 예에서도 알 수 있는 바와 같이, 구성자로 동작하는 Wi-Fi 장치, 예를 들어 스마트 폰은 등록자로 동작하는 Wi-Fi 장치, 예를 들어 IoT 장치의 QR 코드를 스캔하고, IoT 장치의 QR 코드를 프로비젼될 Wi-Fi 네트워크 정보에 포함시킬 수 있다.

[133] 이와는 달리, 구성자가 Wi-Fi 구성 프로비져닝을 위해 등록자의 QR 코드를 제공할 수 있다. 예를 들어, 호텔의 Wi-Fi 네트워크에서 구성자가 등록자, 예를 들어 호텔 객실 TV에 QR 코드를 제공할 수 있다. 그러면, 고객은 프로비져닝 동작을 수행할 스마트 폰을 사용하여 호텔 객실 TV를 통해 제공되는 QR 코드를

스캔하고, 이에 따라 상기에서 설명한 바와 같이 프로비져닝 동작이 수행될 수 있다. 예를 들어, 고객의 스마트 폰이 호텔의 Wi-Fi 네트워크에 온 보딩될 수 있다(on boarding).

[134] 본 개시의 일 실시 예에서, DPP에서 제안된 프로비져닝 프로세스는 총 4개의 동작들, 즉 DPP 부트스트래핑 동작과, DPP 인증 동작과, DPP 구성 동작 및 DPP 억세스 동작을 포함할 수 있다. 본 개시의 일 실시 예에서, DPP 억세스 동작은 피어 발견(peer discovery) 동작으로도 칭해질 수 있다. 본 개시의 일 실시 예에서, DPP 부트스트래핑 동작, DPP 인증 동작, 및 DPP 구성 동작까지의 세 개의 동작들에서는 1개의 전자 장치가 구성자로서 동작하고, 외부 전자 장치가 등록자로서 동작할 수 있다. 본 개시의 일 실시 예에서, 구성자는 상기에서 설명한 바와 같이 DPP 네트워크에 연결되는 전자 장치들을 구성하는 동작을 수행할 수 있다.

[135] 본 개시의 일 실시 예에서, 등록자인 AP는 상기에서 설명한 바와 같이 네트워크에 대한 억세스를 제공하는 동작을 수행할 수 있다. 본 개시의 일 실시 예에서, 등록자는 클라이언트 등록자 또는 AP가 될 수 있으며, 네트워크 구성이 완료될 경우, 등록자는 AP에 연결되어 네트워크에 억세스할 수 있거나 또는 AP로 동작하여 네트워크에 대한 억세스를 제공할 수 있다.

[136] DPP 부트스트래핑 동작, DPP 인증 동작, DPP 구성 동작 및 DPP 억세스 동작에 대해서 설명하면 다음과 같다.

[137] 첫 번째로, DPP 부트스트래핑 동작에 대해서 설명하기로 한다.

[138] 본 개시의 일 실시 예에 따르면, DPP 부트스트래핑 동작에서 DPP 장치들은 보안 프로비져닝 연결(secure provisioning connection)을 설정하기 위해 공중 부트스트래핑 키(public bootstrapping key)들을 교환할 수 있다. 본 개시의 일 실시 예에서, 공중 부트스트래핑 키들은 DPP 부트스트래핑 동작에서 사용되는 보안 정보일 수 있다.

[139] 이에 대해서 설명하면, DPP 장치에는 식별자(identifier: ID)가 할당되며, DPP 장치에 할당되는 ID에는 QR 코드나 사용자가 리드할 수 있는 스트링 (인쇄물 또는 디지털)이 공중 키(public key) 및 사설 키(private key) 형태로 포함될 수 있다. DPP 부트스트래핑 동작에서 구성자와 등록자는 신뢰성 있는 관계를 설정하여 상호 인증을 수행하고, 상호 인증 결과를 기반으로 보안 연결을 설정할 수 있다.

[140] 본 개시의 일 실시 예에서, 상기에서 설명한 바와 같이 DPP 부트스트래핑 동작에서는 공중 부트스트래핑 키들이 교환되며, 공중 부트스트래핑 키들은 구성자와 등록자 간의 상호 인증이 필요한지 여부에 따라 어느 한 방향으로만 송신되거나 또는 양방향으로 교환될 수 있다. DPP 부트스트래핑 동작에서는 예를 들어 QR 코드 방식과, Bluetooth 방식과, 블루투스 저 에너지(Bluetooth low energy: BLE) 방식과, 근거리 통신(near field communication: NFC) 방식과, 공중 키 교환(public key exchange: PKEX) 방식과, 클라우드(cloud) 방식과 같은 다양한

방식들을 기반으로 공중 부트스트래핑 키들이 교환될 수 있다.

[141] 이렇게 공중 부트스트래핑 키들이 교환된 후, 구성자와 등록자간에 연결이 설정될 수 있다. 본 개시의 일 실시 예에서, 공중 부트스트래핑 키들은 DPP 부트스트래핑 동작 이후의 DPP 구성 동작에서 등록자가 수신하는 보안 크리덴셜과는 다를 수 있다. 본 개시의 일 실시 예에서, 부트스트래핑 정보는 DPP 부트스트래핑 동작 이후의 DPP 인증 동작 및 DPP 구성 동작에서 사용되며, 전세계 동작 클래스/채널 페어(global operating class/channel pair)들의 스몰 리스트(small list) 및 매체 접속 제어(medium access control: MAC) 어드레스를 포함할 수 있다. 본 개시의 일 실시 예에서, 전세계 동작 클래스/채널 페어들의 스몰 리스트는 이상적으로 1개의 채널만을 포함할 수 있다.

[142] 두 번째로, DPP 인증 동작 및 DPP 구성 동작에 대해서 설명하기로 한다.

[143] 본 개시의 일 실시 예에 따르면, DPP 인증 동작에서 DPP 장치들은 DPP 인증 프로토콜에서의 부트스트래핑 키들을 사용하여 신뢰성 있고 안전한 채널을 설정하고, DPP 구성 동작에서 구성자는 DPP 구성 프로토콜을 실행하여 DPP 인증 동작 동안 설정된 보안 채널을 통해 등록자를 프로비젼할 수 있다. 이에 대해서 설명하면 다음과 같다.

[144] 본 개시의 일 실시 예에 따르면, DPP 부트스트래핑 동작이 완료되면 구성자와 등록자가 DPP 인증 프로토콜을 사용하여 보안 Wi-Fi 연결을 설정할 수 있다. DPP 인증 동작 및 DPP 구성 동작에서 개시자인 구성자는 DPP 부트스트래핑 동작을 통해 획득한 채널 정보를 기반으로 응답자인 등록자로 인증을 요청할 수 있다. 일 예로, 구성자는 DPP 인증 요청 프레임을 응답자로 송신함으로써 인증을 요청할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임은 응답자의 공중 부트스트래핑 키에 대한 해쉬(hash), 개시자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 프로토콜 키, 또는 제1 중개키(intermediate key)로 인크립트(encrypt)된 개시자 넌스(nonce) 어트리뷰트(initiator nonce attribute)와 개시자 능력들 어트리뷰트(initiator capabilities attribute) 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임에 포함되는 응답자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 프로토콜 키, 또는 제1 중개키로 인크립트된 개시자 넌스 어트리뷰트와 개시자 능력들 어트리뷰트 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[145] 본 개시의 일 실시 예에서, 등록자는 DPP 부트스트래핑 동작을 통해 획득한 채널 정보를 기반으로 해당 채널에서 대기하면서 구성자의 인증 요청에 응답할 수 있다. 일 예로, 등록자는 DPP 인증 응답 프레임을 구성자로 송신함으로써 인증 요청에 응답할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임은 응답자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 부트스트래핑 키에 대한 해쉬, 응답자의 공중 프로토콜 키, 또는 제2 중개키로 인크립트된 응답자 넌스(nonce) 어트리뷰트(responder nonce attribute), 응답자 능력들

어트리뷰트(responder capabilities attribute), 및 개시자 능력들 어트리뷰트 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임에 포함되는 응답자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 부트스트래핑 키에 대한 해쉬, 응답자의 공중 프로토콜 키, 또는 제2 중개키로 인크립트된 응답자 넌스 어트리뷰트, 응답자 능력들 어트리뷰트, 및 개시자 능력들 어트리뷰트 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[146] 이렇게, DPP 인증 동작이 완료됨에 따라 구성자와 등록자 간에는 보안 연결이 설정되고, 보안 연결이 설정된 후 등록자는 구성자로부터 네트워크 구성 정보를 획득하기 위한 트랜잭션(transaction)을 시작할 수 있다. 일 예로, 응답자는 구성자로 DPP 구성 요청(configuration request) 프레임을 송신하고, 구성자는 DDP 구성 요청 프레임에 대한 응답 프레임인 DDP 구성 응답 프레임을 응답자로 송신할 수 있다. 응답자는 DPP 구성 프로토콜을 통해 획득한 보안 크리덴셜과 네트워크 정보를 검증하고, 그 결과를 구성자로 송신할 수 있다. 이와 같은 DPP 구성 동작이 완료됨에 따라 등록자는 AP로 동작하거나 또는 타겟(target) AP를 탐색하고, 탐색된 타겟 AP와 안전하게 연결될 수 있다.

[147] 본 개시의 일 실시 예에서, DPP 구성 동작에서 송수신되는 인코딩된 구성 정보는 DPP 구성 오브젝트(configuration object)를 포함할 수 있으며, DPP 구성 오브젝트는 다음과 같은 DPP 구성 오브젝트 파라미터들을 포함할 수 있으며, DPP 구성 오브젝트는 JSON (javascript object notation) 인코딩된 데이터 구조(data structure)일 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트는 네트워크 구성 정보라 칭해질 수 있다.

[148] (1) Wi-Fi 기술 오브젝트(Wi-Fi technology object)

[149] Wi-Fi 기술 오브젝트는 프로비젼될 정책(policy)의 Wi-Fi 기술을 식별하며, Wi-Fi 기술 오브젝트는 AP 인프라 연결과 같은 연결 타입을 지시할 수 있다. 본 개시의 일 실시 예에서, 등록자는 DDP 구성 요청 프레임에 포함되는 Wi-Fi 기술 오브젝트의 값을 프로비젼될 Wi-Fi 기술을 지시하는 값으로 설정할 수 있고, 구성자는 DPP 구성 응답 프레임에 포함되는 Wi-Fi 기술 오브젝트의 값을 등록자와 구성자 간의 동작에서 사용되는 Wi-Fi 기술을 지시하는 값으로 설정할 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 기술 오브젝트는 DPP 인증 동작 및 DPP 구성 동작 등에서 사용될 Wi-Fi 기술을 지시할 수 있다.

[150] (2) DPP 발견 오브젝트

[151] DPP 발견 오브젝트는 예를 들어 서비스 집합 식별자(service set identifier: SSID), 동작 채널(operating channel), 또는 동작 밴드(operating band) 등과 같은, 동작 또는 발견 정보를 포함할 수 있다.

[152] (3) 크리덴셜 오브젝트

[153] 크리덴셜 오브젝트는 보안 네트워크 억세스를 획득하기 위해 등록자에서 프로비젼되는 크리덴셜 정보를 포함할 수 있다. 크리덴셜 정보는 DPP 구성

오브젝트에 포함되어 있는 인증 및 키 관리(authentication and key management: AKM) 타입 파라미터의 값에 의존적일 수 있다.

[154] 한편, DPP 구성 동작에서 보안 크리덴셜 정보 및 SSID와 같은 네트워크 정보를 포함하는 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트가 구성자로부터 등록자로 송신될 수 있다. 본 개시의 일 실시 예에서, 보안 크리덴셜 정보는 커넥터(connector)를 포함할 수 있으며, 커넥터는 등록자에서 프로비전되는 크리덴셜 정보이며, 커넥터는 등록자들의 페어에 의해 사용되어 DPP 네트워크 소개 프로토콜을 사용하여 보안성 연관(security association)을 설정하는데 사용될 수 있다.

[155] 본 개시의 일 실시 예에서, 커넥터는 구성자가 사인한(sign) 크리덴셜로서, 클라이언트 등록자가 AP 등록자에 연결하는데 사용될 수 있다. 본 개시의 일 실시 예에서, 구성자는 예를 들어 사인 키 페어(signing key pair)인 c-sign-key 및 C-sign-key를 소유하며, c-sign-key는 구성자가 커넥터들을 사인하기 위해 사용되고, C-sign-key는 프로비전되는 DPP 장치들이 동일한 구성자에 의해 사인된 다른 DPP 장치들의 커넥터들을 검증하기 위해 사용될 수 있다.

[156] 각 등록자의 커넥터는 공중 키, 네트워크 역할(network role), 그룹 어트리뷰트 정보를 포함하며, 구성자에 의해 사인될 수 있다. 공중 키는 해당 등록자의 ID를 제공할 수 있다. 네트워크 역할은 해당 등록자가 클라이언트 등록자(enrollee client 또는 enrollee STA)인지 또는 AP 등록자(enrollee AP)로 등록할 것인지를 지시할 수 있다. 그룹 어트리뷰트 정보는 등록자가 네트워크 연결을 설정할 수 있는지 여부를 검출하는 데 사용될 수 있다. 커넥터 시그니쳐(connector signature)는 해당 커넥터 콘텐트들이 구성자에 의해 생성되었음을 증명할 수 있다. 커넥터는 암호가 아닌 공중 키를 포함하기 때문에 보안 크리덴셜 정보는 Wi-Fi 장치, 즉 등록자마다 다를 수 있다. 예를 들어, 다른 등록자는 해당 커넥터를 사용하여 네트워크에 억세스할 수 없으며, 해당 커넥터에 상응하는 등록자가 특정 AP에 속할 경우에는 다른 AP가 특정 AP로 가장할 수 없음을 의미할 수 있다.

[157] 본 개시의 일 실시 예에서, 클라이언트 등록자는 네트워크 정보를 기반으로 AP 등록자를 탐색할 수 있다. 클라이언트 등록자는 커넥터를 기반으로 인증 동작을 수행하고, 네트워크 소개(network introduction: NI) 프로토콜을 기반으로 네트워크 연결을 설정할 수 있다. 커넥터를 사용할 경우의 이점은 AP에 연결된 각 등록자가 고유한 보안 크리덴셜 정보를 갖는다는 점일 수 있다.

[158] 도 7은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 프로비져닝 프로세스를 개략적으로 도시한 도면이다.

[159] 도 7을 참조하면, 전자 장치, 예를 들어 제1 전자 장치(710)와 외부 전자 장치, 예를 들어, 제2 전자 장치(700) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(710)는 구성자이면서 개시자로서 동작하고, 제2 전자 장치(700)는 등록자이면서 응답자로서 동작한다고 가정하기로 한다.

[160] 동작 711에서, 등록자이면서 응답자로서 동작하는 제2 전자 장치(700)는 DPP 존재 안내(DPP presence announcement) 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 존재 안내 프레임은 구성자인 개시자에게 응답자가 DPP 교환에 참여할 준비가 되어 있다는 것을 시그널하기 위해 사용되며, 송신자, 일 예로 응답자의 공중 부트스트래핑 키를 포함하는 해쉬를 포함할 수 있다. 본 개시의 일 실시 예에서, 응답자의 공중 부트스트래핑 키를 포함하는 해쉬는 DPP 부트스트래핑 동작에서 사용되는 보안 정보일 수 있다. 본 개시의 일 실시 예에서, 프로비젼되지 않는 장치의 공중 키의 해쉬의 유출(leakage)을 방지하기 위한 DPP 존재 안내 프레임에 대한 해쉬는 SHA256("chirp" | B_R)일 수 있다. 본 개시의 일 실시 예에서, B_R은 응답자, 예를 들어 제2 전자 장치(700)의 공중 부트스트래핑 키를 나타낼 수 있다.

[161] 동작 713에서, 제2 전자 장치(700)는 DPP 부트스트래핑 동작 동안 명시된 채널에서 청취 동작을 수행할 수 있다. 구성자이면서 개시자로 동작하는 제1 전자 장치(710)는 아웃 오브 밴드(out-of-band: OOB) 메카니즘, 예를 들어, QR 코드 스캔, NFC 탭, 또는 BLE 교환을 사용하여 제2 전자 장치(700)로부터 부트스트래핑 정보를 획득할 수 있다. 본 개시의 일 실시 예에서, 부트스트래핑 정보는 DPP 인증을 위한 제2 전자 장치(700)의 공중 부트스트래핑 키(B_R), 전세계 동작 클래스 채널, 및/또는 채널 리스트를 포함할 수 있다. DPP 부트스트래핑 동작 동안, 동작 715에서, 제2 전자 장치(700)는 제1 전자 장치(710)가 제2 전자 장치(700)를 발견하는 것을 도와주도록 그 존재를 선택적으로 안내할 수 있다. 동작 717에서, 제2 전자 장치(700)는 DPP 존재 안내 프레임을 송신할 수 있다.

[162] 동작 719에서, 제1 전자 장치(710)는 DPP 인증 요청 프레임들을 브로드캐스트함으로써 부트스트래핑 동안 수신되는 채널 정보를 기반으로 하는 채널에서 동작을 시작할 수 있다. 예를 들어, 제1 전자 장치(710)는 동작 721, 동작 723 및 동작 725에서 지속적으로 DPP 인증 요청 프레임들을 브로드캐스트할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임은 SHA256(B_R), SHA256(B_I), P_I 및 {I-nonce, I-capabilities}$_{k1}$을 포함할 수 있다. 예를 들어, SHA256(B_R)는 B_R에 대한 SHA256 해쉬를 나타내고, B_I는 제1 전자 장치(710)의 공중 부트스트래핑 키를 나타내고, SHA256(B_I)는 B_I에 대한 SHA256 해쉬를 나타내고, P_I는 제1 전자 장치(710)의 공중 프로토콜 키를 나타내고, I-nonce는 개시자 넌스(nonce) 어트리뷰트(initiator nonce attribute)를 나타내고, I-capabilities는 개시자 능력들 어트리뷰트(initiator capabilities attribute)를 나타내고, k1은 제1 중개키(intermediate key)를 나타낼 수 있다. 본 개시의 일 실시 예에서, {I-nonce, I-capabilities}$_{k1}$는 k1로 인크립트된 I-nonce 및 I-capabilities를 나타낼 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임에 포함되는 SHA256(B_R), SHA256(B_I), P_I, 또는 {I-nonce, I-capabilities}$_{k1}$ 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[163] 동작 727에서, 제1 전자 장치(710)가 DPP 인증 요청 프레임들을 브로드캐스트하고, 제2 전자 장치(700)가 이 DPP 인증 요청 프레임을 성공적으로 수신하게 되면, B_R 에 대한 해쉬 함수 값인 $H(B_R)$과 매치할 수 있다. 동작 729에서, 제2 전자 장치(700)는 DPP 인증 요청 프레임에 대한 응답 프레임인 DPP 인증 응답 프레임을 제1 전자 장치(710)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임은 DPP 상태(DPP status) 필드, $SHA256(B_R)$, $[SHA256(B_I)]$, P_R 및 $\{R\text{-nonce, I-nonce, R-capabilities, }\{R\text{-auth}\}_{ke}\}_{k2}$을 포함할 수 있다. 예를 들어, P_R은 제2 전자 장치(700)의 공중 프로토콜 키를 나타내고, R-nonce는 응답자 넌스(nonce) 어트리뷰트(responder nonce attribute)를 나타내고, R-capabilities는 응답자 능력들 어트리뷰트(responder capabilities attribute)를 나타내고, R-auth는 응답자, 예를 들어 제2 전자 장치(700)의 인증 태그(authentication tag)를 나타내고, ke는 인크립션 키를 나타내고, k2는 제2 중개키를 나타내고, [ ]는 선택적으로 존재하는 값을 나타낸다. 예를 들어, $[SHA256(B_I)]$는 특정 조건이 만족되거나, 또는 선택적으로 DPP 인증 응답 프레임에 포함될 수 있다. 본 개시의 일 실시 예에서, $\{R\text{-auth}\}_{ke}$ 는 ke로 인크립트된 R-auth를 나타낼 수 있다. 본 개시의 일 실시 예에서, $\{R\text{-nonce, I-nonce, R-capabilities, }\{R\text{-auth}\}_{ke}\}_{k2}$는 k2로 인크립트된 R-nonce, I-nonce, R-capabilities, 및 $\{R\text{-auth}\}_{ke}$를 나타낼 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임에 포함되는 $SHA256(B_R)$, $[SHA256(B_I)]$, P_R, 또는 $\{R\text{-nonce, I-nonce, R-capabilities, }\{R\text{-auth}\}_{ke}\}_{k2}$ 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[164] DPP status 필드는 하기 표 1에 나타낸 바와 같은 상태를 나타낼 수 있다.

[165] [표 1]

[166]

Status or Error	Value	Meaning
STATUS_OK	0	No errors or abnormal behavior
STATUS_NOT_COMPATIBLE	1	The DPP Initiator and Responder have incompatible capabilities
STATUS_AUTH_FAILURE	2	Authentication failed
STATUS_BAD_CODE	3	The code used in PKEX is bad
STATUS_BAD_GROUP	4	An unsupported group was offered
STATUS_CONFIGURE_FAILURE	5	Configurator refused to configure Enrollee
STATUS_RESPONSE_PENDING	6	Responder will reply later
STATUS_INVALID_CONNECTOR	7	Received Connector is invalid for some reason. The sending device needs to be reconfigured.
STATUS_NO_MATCH	8	Received Connector is verified and valid but no matching Connector could be found. The receiving device needs to be reconfigured.
STATUS_CONFIG_REJECTED	9	Enrollee rejected the configuration.
STATUS_NO_AP	10	Enrollee failed to discover an access point.
STATUS_CONFIGURE_PENDING	11	Configuration response is not ready yet. The enrollee needs to request again.
STATUS_CSR_NEEDED	12	Configuration requires a Certificate Signing Request. The enrollee needs to request again.
STATUS_CSR_BAD	13	The Certificate Signing Request was invalid.
STATUS_NEW_KEY_NEEDED	14	The Enrollee needs to generate a new Protocol key.

[167] 동작 731에서, 제2 전자 장치(700)로부터 DPP 인증 응답 프레임을 수신한 제1 전자 장치(710)는 제2 전자 장치(700)로 DPP 인증 확인 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 확인 프레임은 DPP status 필드, SHA256(B_R), [SHA256(B_I)] 및 $\{\text{I-auth}\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, I-auth는 개시자, 예를 들어 제1 전자 장치(710)의 인증 태그(authenticating tag)를 나타내며, ke는 인크립션 키를 나타낼 수 있다. 본 개시의 일 실시 예에서, $\{\text{I-auth}\}_{ke}$ 는 ke로 인크립트된 I-auth를 나타낼 수 있다.

[168] 동작 733에서, 제1 전자 장치(710)로부터 DPP 인증 확인 프레임을 수신한 제2 전자 장치(700)는 제1 전자 장치(710)로 DPP 구성 요청 프레임을 송신할 수 있다. 일 실시 예에서, DPP 구성 요청 프레임은 $\{\text{E-nonce, configuration attributes}\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, E-nonce는 E-nonce 어트리뷰트를 나타내며, configuration attributes는 구성 어트리뷰트 오브젝트들을 나타낼 수 있다. 구성 어트리뷰트 오브젝트는 디바이스 이름(device name) 어트리뷰트, Wi-Fi 기술(Wi-Fi technology) 어트리뷰트, 또는 네트워크 역할 어트리뷰트 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, $\{\text{E-nonce, configuration attributes}\}_{ke}$ 는 ke로 인크립트된 E-nonce 및 configuration attributes를 나타낼 수

있다.

[169] 동작 735에서 DPP 구성 요청 프레임을 수신한 제1 전자 장치(710)는 제2 전자 장치(700)로 DPP 구성 요청 프레임에 대한 응답인 DPP 구성 응답 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임은 DPP status 필드와, $\{\text{E-nonce, configuration object}\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, configuration object는 DPP 구성 오브젝트를 나타낼 수 있다. 본 개시의 일 실시 예에서, $\{\text{E-nonce, configuration object}\}_{ke}$ 는 ke로 인크립트된 E-nonce 및 configuration object를 나타낼 수 있다.

[170] 동작 737에서, DPP 구성 응답 프레임을 수신한 제2 전자 장치(700)는 DPP 구성 결과 프레임을 제1 전자 장치(710)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 결과 프레임은 $\{\text{DPP Status, E-nonce}\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, $\{\text{DPP Status, E-nonce}\}_{ke}$ 는 ke로 인크립트된 DPP Status 및 E-nonce를 나타낼 수 있다.

[171] 세 번째로, 프로비져닝 프로세스에서의 DPP 억세스 동작에 대해서 설명하기로 한다.

[172] 본 개시의 일 실시 예에서, 네트워크 소개 프로토콜은 구성자가 제공하는 커넥터를 사용하여 클라이언트 등록자가 AP 등록자에 안전하게 연결할 수 있도록 사용되며, 네트워크 소개 프로토콜을 기반으로 하는 DPP 억세스 동작은 다음과 같다.

[173] (1) 클라이언트 등록자들과 AP 등록자 각각은 자신의 커넥터가 구성자에 의해 사인되었는지 여부를 확인할 수 있다.

[174] (2) 클라이언트 등록자들 각각은 자신의 역할이 호환 가능함을(compatible) 확인하고, AP 등록자와 통신을 설정할 수 있다.

[175] (3) 클라이언트 등록자들은 그룹 어트리뷰트가 일치하는지 확인할 수 있다.

[176] (4) AP 등록자와 클라이언트 등록자들 각각은 공중 커넥터 키를 기반으로 페어와이즈 마스터 키(pairwise master key: PMK)를 도출할 수 있다.

[177] (5) 도출된 PMK를 기반으로 AP 등록자와 클라이언트 등록자들 간에 연결이 설정될 수 있다.

[178] 도 8은 본 개시의 일 실시 예에 따른 커넥터를 사용하는 네트워크 억세스 동작을 개략적으로 도시하고 있는 신호 흐름도이다.

[179] 도 8을 참조하면, 전자 장치, 예를 들어 제1 전자 장치(800)와 외부 전자 장치, 예를 들어, 제2 전자 장치(810) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(800)는 AP 등록자로서 동작하고, 제2 전자 장치(810)는 클라이언트 등록자로서 동작한다고 가정하기로 한다.

[180] 동작 811에서, 클라이언트 등록자인 제2 전자 장치(810)는 IEEE 802.11 규격을 기반으로 하는 IEEE 802.11 스캐닝(scanning) 동작을 수행할 수 있다. 동작 813에서 제2 전자 장치(810)는 IEEE 802.11 스캐닝 동작 수행에 따라 AP 등록자인 제1 전자 장치(800)를 발견할 수 있다. 동작 815에서, 제2 전자

장치(810)는 발견된 제1 전자 장치(800)로 커넥터 어트리뷰트를 포함하는 피어 발견 요청(peer discovery request) 프레임을 송신할 수 있다. 동작 817에서 제1 전자 장치(800)는 제2 전자 장치(810)로부터 피어 발견 요청 프레임을 수신하고, 피어 발견 요청 프레임에 대한 응답으로 피어 발견 응답 프레임을 제2 전자 장치(810)로 송신할 수 있다. 본 개시의 일 실시 예에서, 피어 발견 응답 프레임은 커넥터 어트리뷰트와 상태 어트리뷰트를 포함하며, 상태 어트리뷰트는 DPP 상태 어트리뷰트를 나타낼 수 있다.

[181] 동작 819에서 제2 전자 장치(810)는 제1 전자 장치(800)로부터 피어 발견 응답 프레임을 수신하면, 제1 전자 장치(800)와 IEEE 802.11 규격을 기반으로 하는 IEEE 802.11 인증 동작을 수행할 수 있다. 동작 821에서 제2 전자 장치(810)는 제1 전자 장치(800)와 IEEE 802.11 규격을 기반으로 하는 IEEE 802.11 연관(association) 동작을 수행할 수 있다. 동작 823에서 제2 전자 장치(810)는 네트워크 키인 인증 및 키 관리(authentication and key management: AKM)를 사용하여 제1 전자 장치(800)에 연관될 수 있다.

[182] 본 개시의 다양한 실시 예들에 따른 DPP 구성 오브젝트에 대해서 설명하면 다음과 같다.

[183] 일 실시 예에서, 구성자는 DPP 네트워크에 대한 보안 억세스를 설정하기 위한, 크리덴셜들 뿐만 아니라 네트워크를 발견하기 위한 정보를 등록자에게 프로비젼할 수 있다. 등록자는 DPP 구성 요청 프레임에 DPP 구성 요청 오브젝트를 포함시키고, DPP 구성 요청 오브젝트가 포함된 DPP 구성 요청 프레임을 구성자로 송신할 수 있다.

[184] 구성자는 DPP 구성 요청 프레임을 수신할 경우, 수신된 DPP 구성 요청 프레임을 프로세싱하여 하나 또는 그 이상의 DPP 구성 오브젝트들을 생성할 수 있다. 구성자는 생성된 하나 또는 그 이상의 DPP 구성 오브젝트들을 DPP 구성 요청 프레임에 대한 응답 프레임인 DPP 구성 응답 프레임에 포함시키고, 하나 또는 그 이상의 DPP 구성 오브젝트들이 포함된 DPP 구성 응답 프레임을 등록자로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임에는 하나 또는 그 이상의 DPP 구성 오브젝트들 뿐만 아니라 DPP status 필드가 포함될 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임에 포함되는 하나 또는 그 이상의 DPP 구성 오브젝트들은 DPP status 및 설정된 적어도 하나의 조건들을 기반으로 달라질 수 있다. 이에 대해서 설명하면 다음과 같다.

[185] 본 개시의 일 실시 예에서, 구성이 정상적으로 진행되었고, 등록자에 네트워크 연결 권한을 부여하고자 할 경우 구성자는 DPP 구성 응답 프레임에 DPP status 및 하나 또는 그 이상의 DPP 구성 오브젝트들을 포함시키고, DPP status 및 하나 또는 그 이상의 DPP 구성 오브젝트들이 포함된 DPP 구성 응답 프레임을 등록자로 송신할 수 있다. 이 경우, DPP 구성 응답 프레임에 포함되는 어트리뷰트(attribute)들은 하기 표 2와 같이 나타낼 수 있다.

[186] [표 2]

[187]

Attribute	Required (R) / Conditional (C)	Notes
DPP Status	R	If configuration is succeeded, it is marked as STATUS_OK.
Wrapped Data	R	The following sub-attribites are wrapped with AES-SIV ciphertext.
Enrollee Nonce	R	This attribite is a component of Wrapped Data.
DPP Configuration Object (one or more)	C	One or more JSON encoded DPP Configuration Object attribute. These are components of Wrapped Data.

[188] 표 2에서, DPP Status 어트리뷰트는 에러나 비정상적인 동작이 존재하지 않음을 나타내는 "STATUS_OK"로 마킹되며, "STATUS_OK"는 구성이 성공적임을 지시할 수 있다.

[189] 표 2에서, Wrapped Data는 다음 서브-어트리뷰트(sub-attribute)들이 AES-SIV (advanced encryption standard - synthetic initialization vector) 암호문(ciphertext)으로 랩되는(wrapped) 것을 지시할 수 있다. 표 2에서, Enrollee Nonce는 Wrapped Data 어트리뷰트의 컴포넌트(component)일 수 있다. 표 2에서, DPP Configuration Object 어트리뷰트는 하나 또는 그 이상의 JSON 인코딩된 DPP 구성 오브젝트 어트리뷰트이며, DPP Configuration Object 어트리뷰트 역시 Wrapped Data의 컴포넌트일 수 있다.

[190] 본 개시의 일 실시 예에서, DPP 구성 오브젝트는 AP의 네트워크에 억세스하기 위한 Wi-Fi 연결 유형, SSID, 크리덴셜 정보를 포함할 수 있다. DPP 구성 오브젝트는 상기에서 설명한 바와 같이 Wi-Fi 기술 오브젝트, 발견 오브젝트, 또는 크리덴셜 오브젝트 등을 포함할 수 있다. Wi-Fi 기술 오브젝트는 사용될 Wi-Fi 연결 타입을 나타내고, 발견 오브젝트는 SSID를 포함하며, 크리덴셜 오브젝트는 AKM 타입에 따라 키, 암호, 및/또는 커넥터를 포함할 수 있다.

[191] 본 개시의 일 실시 예에서, AKM 파라미터의 값이 DPP를 나타내는 값일 경우 커넥터를 이용해 구성자와 AP 등록자간의 인증이 진행될 수 있다. 본 개시의 일 실시 예에서, AKM파라미터의 값이 DPP를 나타내는 값이 아닌 사전 공유된 키(preshared Key: PSK) 또는 SAE (simultaneous authentication of equals) 등을 나타내는 다른 값일 경우, Passphrase 또는 Password 등을 사용하여 구성자와 레가시(legacy) AP간의 인증이 진행될 수 있다.

[192] 본 개시의 일 실시 예에서, 구성자는 DPP 구성 응답 프레임에 JSON 인코딩된 DPP 구성 오브젝트를 하나 또는 그 이상 포함시킬 수 있기 때문에, 다수의 AP들에 대한 네트워크 억세스 권한을 하나의 DPP 구성 응답 프레임을 통해 송신할 수 있다.

[193] 본 개시의 일 실시 예에서, JSON 인코딩된 DPP 구성 오브젝트의 일 예는 하기 표 3과 같이 나타낼 수 있다.

[194] [표 3]

[195]


```
{
  "wi-fi_tech":"infra",
  "discovery":
  {
    "ssid":"mywifi"
  },
  "cred":
  {
    "akm":"dpp",
    "signedConnector":
"eyJ0eXAiOiJkcHBDb24iLCJraWQiOiJrTWNlZ0RCUG1OWlZha0FzQlpPek9vQ3N2UWprcl9uRUFwOXV
GLUVEbVZFIiwiYWxnIjoiRVMyNTYifQ.eyJncm91cHMiOlt7Imdyb3VwSWQiOiJob21lIiwibmV0Um9sZSI
6InN0YSJ9LHsiZ3JvdXBJZCI6ImNvdHRhZ2UiLCJuZXRSb2xlIjoic3RhIn1dLCJuZXRBY2Nlc3NLZXkiOnsia
3R5IjoiRUMiLCJjcnYiOiJQLTI1NiIsIngiOiJYai16VjJpRWIlOFh3eUE5aWpwc0w2eHlMdkRpSUJ0aHJITzha
Vnh3bXBBIiwieSI6IkxVc0RCbW43bnYtTENubjZmQm9YS3NLcExHSmlWcFlfa25UY2tHZ3NnZVUifSwiZ
XhwaXJ5IjoiMjAxOS0wMS0zMVQyMjowMDowMCswMjowMCJ9.8fJSNCpDjv5BEFfmlqEbBNTaHx2L6c
_22Uvr9KYjtAw88VfvEUWiruECUSJCUVFqv1yDEE4RJVdTIw3aUDhlMw",
    "csign":
```


[196]


```
{
      "kty":"EC",
      "crv":"P-256",
      "x":"MKBCTNIcKUSDii11ySs3526iDZ8AiTo7Tu6KPAqv7D4",
      "y":"4EtI6SRW2YiLUrN5vfvVHuhp7x8PxltmWWlbbM4IFyM",
      "kid":"kMcegDBPmNZVakAsBZOzOoCsvQjkr_nEAp9uF-EDmVE"
    },
    "ppKey":
    {
      "kty":"EC",
      "crv":"P-256",
      "x":"XX_ZuJR9nMDSb54C_okhGiJ7OjCZOlWOU9m8zAxgUrU",
      "y":"Fekm5hyGii80amM_REV5sTOG3-sl1H6MDpZ8TSKnb7c"
    }
  }
}
```


[197] 상기에서 설명한 바와 같이, 구성자는 DPP 구성 응답 프레임에 JSON 인코딩된 DPP 구성 오브젝트를 하나 또는 그 이상 포함시킬 수 있기 때문에, 다수의 AP들에 대한 네트워크 억세스 권한을 하나의 DPP 구성 응답 프레임을 통해 송신할 수 있다.

[198] 본 개시의 일 실시 예에서, DPP 구성 응답 프레임에 1개의 DPP 구성 오브젝트가 포함될 경우가 도 7의 동작 735에 해당될 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임에 예를 들어 3개의 DPP 구성 오브젝트가 포함될 경우 도 7의 동작 735의 DPP 구성 응답 프레임은 DPP status 필드와, {E-nonce, configuration object, configuration object, configuration object}$_{ke}$를 포함할 수 있다. 그리고, 3개의 DPP 구성 오브젝트들은 하기 표 4와 같이 각각 JSON 인코딩될 수

있다.

[199] [표 4]

[200]

```
{
    "wi-fi_tech": ... ,
    "discovery": ...
    "cred": ...
} {
    "wi-fi_tech": ... ,
    "discovery": ... ,
    "cred": ...
} {
    "wi-fi_tech": ... ,
    "discovery": ... ,
    "cred": ...
}
```

[201] 표 4에 나타낸 바와 같은 3개의 DPP 구성 오브젝트들은 설명의 편의를 위해 일 예로 표 3에 나타낸 바와 같은 JSON 인코딩된 DPP 구성 오브젝트를 간략하게 나타낸 것임에 유의하여야만 할 것이다.

[202] 한편, 사용자 환경에서는 가정, 사무실, 또는 사업장과 같은 특정 장소에 다수의 AP들이 존재할 수 있고, 일반적으로는 AP들이 동일한 SSID 및 암호를 가지고, 따라서 다중 AP 로밍 네트워크가 구성될 수 있다.

[203] 하지만 예를 들어 보안, 특수한 목적, 또는 다중 AP 로밍 네트워크 구성에 관련된 정보를 인지하지 못하는 상황과 같은 다양한 이유들로 인해 다중 AP 로밍 네트워크가 구성되지 않고, 대신에 각 AP가 고유한 SSID와 고유한 암호를 가지는 경우가 발생될 수 있다. 이 경우, 새로운 등록자들에 대해 다수의 AP들 각각을 연결시켜야 하는 번거로움이 발생될 수 있다. 또는, 구성자가 송신하는 AP의 크리덴셜 정보는 등록자의 관점에서 최적 AP에 대한 보안 연결을 보장하지 못할 수 있다.

[204] 다양한 실시 예들은 DPP 네트워크에서 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[205] 다양한 실시 예들은 DPP 네트워크에서 다수의 네트워크 구성 정보들을 송수신하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[206] 다양한 실시 예들은 DPP 네트워크에서 등록자에 적합한 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[207] 다양한 실시 예들은 DPP 네트워크에서 제공할 네트워크 구성 정보들을 필터링하는 기준을 제공하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[208] 다양한 실시 예들은 DPP 네트워크에서 설정되어 있는 조건들을 기반으로 다수의 DPP 구성 오브젝트들을 제공하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[209] 본 개시의 다양한 실시 예들에서, 네트워크 구성 정보의 일 예는 DPP 구성 오브젝트가 될 수 있다.

[210] 도 9a는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 순서도이다.

[211] 도 9a를 참조하면, 동작 900에서, 전자 장치(예: 도 1의 전자 장치(101))는 외부 전자 장치(예: 도 1의 전자 장치(102) 또는 전자 장치(104))와 DPP 부트스트래핑 동작을 수행할 수 있다. 도 9a에서는 전자 장치는 구성자로서 동작하고, 외부 전자 장치는 등록자로서 동작한다고 가정하기로 한다. 구성자와 등록자간에 수행되는 DPP 부트스트래핑 동작에 대해서는 도 7에서 설명한 바 있으므로, 전자 장치와 외부 전자 장치간에 수행되는 DPP 부트스트래핑 동작에 대한 설명은 생략하기로 한다.

[212] 동작 902에서 전자 장치는 외부 전자 장치와 DPP 인증 동작을 수행할 수 있다. 구성자와 등록자간에 수행되는 DPP 인증 동작에 대해서는 도 7에서 설명한 바 있으므로, 전자 장치와 외부 전자 장치간에 수행되는 DPP 인증 동작에 대한 설명은 생략하기로 한다.

[213] 동작 904에서 전자 장치는 DPP 인증 동작이 완료됨에 따라 외부 전자 장치로부터 DPP 구성 요청 프레임을 수신할 수 있다. 일 실시 예에서, DPP 구성 요청 프레임은 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 요청하는 메시지가 될 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 도 7에서 설명한 바와 같이 $\{\text{E-nonce, configRequest}\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, E-nonce는 E-nonce 어트리뷰트를 나타내고, configRequest 는 DPP 구성 요청 오브젝트 어트리뷰트를 나타내고, ke는 인크립션 키를 나타낼 수 있다. 본 개시의 일 실시 예에서, $\{\text{E-nonce, configRequest}\}_{ke}$는 ke로 인크립트된 E-nonce 및 configRequest를 나타낼 수 있다.

[214] 동작 906에서 DPP 구성 요청 프레임을 수신한 전자 장치는 Wi-Fi 스캔 필터링 방식을 적용할 것인지 여부를 결정할 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 필터링 방식은 Wi-Fi 스캔 결과를 기반으로 DPP 구성 오브젝트가 제공될 적어도 하나의 AP를 선택하고, 선택한 적어도 하나의 AP에 상응하는 DPP 오브젝트를 제공하도록 하는 방식일 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 필터링 방식에서 사용되는 Wi-Fi 스캔 결과는 구성자, 예를 들어, 전자 장치에 의해 수행된 Wi-Fi 스캔 동작에 대한 Wi-Fi 스캔 결과 또는 등록자, 예를 들어, 외부 전자 장치에 의해 수행된 Wi-Fi 스캔 동작에 대한 Wi-Fi 스캔 결과일 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 결과는 스캔된 AP들 각각에 대한 정보, 예를 들어 AP ID 또는 AP 주소(address)를 포함할 수 있다.

[215] 본 개시의 일 실시 예에 따르면, 동작 906에서, 전자 장치는 DPP 네트워크의 네트워크 상황에 따라 Wi-Fi 스캔 필터링 방식을 적용할 것인지 여부를 결정할 수 있다. 본 개시의 일 실시 예에서, 동작 906에서, 전자 장치는 상위 계층, 예를 들어 어플리케이션 계층(application layer)을 통해 제공되는 입력을 기반으로 Wi-Fi 스캔 필터링 방식을 적용할 것인지 여부를 결정할 수 있다. 일 예로, UI를 통해 Wi-Fi 스캔 필터링 방식을 적용할지 여부가 선택될 수 있다.

[216] 동작 906에서 Wi-Fi 스캔 필터링 방식을 적용하기로 결정할 경우, 전자 장치는 동작 908에서 Wi-Fi 스캔 결과를 기반으로 스캔된 AP 들 중 전자 장치 자신이 DPP 구성 오브젝트를 저장하고 있는 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트는 크리덴셜 오브젝트를 포함하므로, 크리덴셜 오브젝트를 저장하고 있을 경우 DPP 구성 오브젝트를 저장하고 있다고 가정할 수 있음에 유의하여야만 할 것이다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 결과가 전자 장치의 Wi-Fi 스캔 결과일 경우 스캔된 AP들은 전자 장치의 Wi-Fi 스캔 동작에 의해 스캔된 AP들일 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 결과가 외부 전자 장치의 Wi-Fi 스캔 결과일 경우 스캔된 AP들은 외부 전자 장치의 Wi-Fi 스캔 동작에 의해 스캔된 AP들일 수 있다. 본 개시의 일 실시 예에서, 전자 장치는 크리덴셜 리스트를 저장하고 있으며, 크리덴셜 리스트는 다수의 AP들 각각에 대한 AP ID와 크리덴셜 오브젝트를 포함할 수 있다. 본 개시의 일 실시 예에서, 전자 장치는 Wi-Fi 스캔 결과에 포함되어 있는 AP ID들 중 전자 장치의 크리덴셜 리스트에 포함되어 있는 적어도 하나의 AP ID를 검출하고, 검출된 적어도 하나의 AP ID에 상응하는 적어도 하나의 AP를 선택할 수 있다.

[217] 이와는 달리, 동작 906에서 Wi-Fi 스캔 필터링 방식을 적용하기로 결정하지 않은 경우, 전자 장치는 동작 910에서 전자 장치 자신이 DPP 구성 오브젝트를 저장하고 있는 다수의 AP들 중 적어도 하나의 AP를 선택할 수 있다.

[218] 동작 912에서 전자 장치는 선택된 적어도 하나의 AP에 대해 세컨더리(secondary) 필터링 방식을 적용하여 DPP 구성 오브젝트를 제공할 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식은 적어도 하나의 조건을 기반으로 DPP 구성 오브젝트가 제공될 적어도 하나의 AP를 선택하고, 선택한 적어도 하나의 AP에 상응하는 DPP 구성 오브젝트를 제공하도록 하는 방식일 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식은 필요에 따라 적용될 수도 있고, 적용되지 않을 수도 있으며, 세컨더리 필터링 방식에 대해서는 하기에서 설명할 것이므로 여기서는 그 상세한 설명을 생략하기로 한다.

[219] 동작 914에서 전자 장치는 선택된 적어도 하나의 AP에 대한 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 외부 전자 장치로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임은 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 포함하는 메시지가 될 수 있다.

[220] 본 개시의 일 실시 예에 따르면, 도 9a에서는 전자 장치가 Wi-Fi 스캔 필터링 방식을 적용할지 여부를 결정하는 동작에 대해서 설명하고 있으나, Wi-Fi 스캔 필터링 방식을 적용할지 여부를 결정하는 동작을 수행하지 않고 Wi-Fi 스캔 필터링 방식을 적용하는 형태로, 또는 Wi-Fi 스캔 필터링 방식을 적용하지 않는 형태로 적어도 하나의 DPP 구성 오브젝트를 제공할 수도 있음은 물론이다. 본

개시의 일 실시 예에 따르면, Wi-Fi 스캔 필터링 방식을 적용할지 여부 또는 세컨더리 필터링 방식을 적용할 지 여부는 DPP 장치, 예를 들어 전자 장치 또는 외부 전자 장치에 미리 설정되어 있을 수도 있고, 또는 필요에 따라 상위 계층, 예를 들어 어플리케이션 계층을 통해 설정될 수도 있다. 일 예로, UI를 통해 Wi-Fi 스캔 필터링 방식을 적용할지 여부 또는 세컨더리 필터링 방식을 적용할 지 여부가 선택될 수 있다.

[221] 본 개시의 일 실시 예에서, Wi-Fi 스캔 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식 또는 등록자 기반 Wi-Fi 스캔 필터링 방식 중 적어도 하나를 포함할 수 있다. 구성자 기반 Wi-Fi 스캔 필터링 방식은 구성자에 의해 수행되는 Wi-Fi 스캔 동작에 대한 Wi-Fi 스캔 결과를 기반으로 하는 Wi-Fi 스캔 필터링 방식을 나타낼 수 있다. 등록자 기반 Wi-Fi 스캔 필터링 방식은 등록자에 의해 수행되는 Wi-Fi 스캔 동작에 대한 Wi-Fi 스캔 결과를 기반으로 하는 Wi-Fi 스캔 필터링 방식을 나타낼 수 있다.

[222] 도 9b는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 순서도이다.

[223] 도 9b를 참조하면, 동작 950에서, 전자 장치(예: 도 1의 전자 장치(101))는 외부 전자 장치(예: 도 1의 전자 장치(102) 또는 전자 장치(104))와 DPP 부트스트래핑 동작을 수행할 수 있다. 도 9b에서는 전자 장치는 구성자로서 동작하고, 외부 전자 장치는 등록자로서 동작한다고 가정하기로 한다. 구성자와 등록자간에 수행되는 DPP 부트스트래핑 동작에 대해서는 도 7에서 설명한 바 있으므로, 전자 장치와 외부 전자 장치간에 수행되는 DPP 부트스트래핑 동작에 대한 설명은 생략하기로 한다.

[224] 동작 952에서 전자 장치는 외부 전자 장치와 DPP 인증 동작을 수행할 수 있다. 구성자와 등록자간에 수행되는 DPP 인증 동작에 대해서는 도 7에서 설명한 바 있으므로, 전자 장치와 외부 전자 장치간에 수행되는 DPP 인증 동작에 대한 설명은 생략하기로 한다.

[225] 동작 954에서 전자 장치는 DPP 인증 동작이 완료됨에 따라 외부 전자 장치로부터 DPP 구성 요청 프레임을 수신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 요청하는 메시지가 될 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 도 7에서 설명한 바와 같이 $\{\text{E-nonce, configRequest}\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, E-nonce는 E-nonce 어트리뷰트를 나타내고, configRequest 는 DPP 구성 요청 오브젝트 어트리뷰트를 나타내고, ke는 인크립션 키를 나타낼 수 있다. 본 개시의 일 실시 예에서, $\{\text{E-nonce, configRequest}\}_{ke}$는 ke로 인크립트된 E-nonce 및 configRequest를 나타낼 수 있다.

[226] 동작 956에서 DPP 구성 요청 프레임을 수신한 전자 장치는 DPP 구성 오브젝트 필터링 동작을 수행할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작은 구성자에 저장되어 있는 적어도 하나의 DPP 구성 오브젝트에

대해서 설정되어 있는 적어도 하나의 필터링 방식을 적용하여 적어도 하나의 DPP 구성 오브젝트를 선택하는 동작을 의미할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트는 크리덴셜 오브젝트를 포함하므로 DPP 구성 오브젝트 필터링 동작은 크리덴셜 필터링 동작으로도 칭해질 수 있다.

[227] 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작에 사용되는 적어도 하나의 필터링 방식은 Wi-Fi 스캔 필터링 방식 또는 세컨더리 필터링 방식 중 적어도 하나를 포함할 수 있다. Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식에 대해서는 상기에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다.

[228] 본 개시의 일 실시 예에서, Wi-Fi 스캔 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식 또는 등록자 기반 Wi-Fi 스캔 필터링 방식 중 적어도 하나를 포함할 수 있다. 구성자 기반 Wi-Fi 스캔 필터링 방식 및 등록자 기반 Wi-Fi 스캔 필터링 방식에 대해서는 상기에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다.

[229] 동작 958에서 전자 장치는 DPP 구성 오브젝트 필터링 동작을 통해 선택된 적어도 하나의 AP에 대한 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 외부 전자 장치로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임은 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 포함하는 메시지가 될 수 있다.

[230] 도 10은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 구성자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 도면이다.

[231] 도 10을 참조하면, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자 장치, 예를 들어 제1 전자 장치(1000), 외부 전자 장치, 예를 들어 제2 전자 장치(1010)를 포함할 수 있다. DPP 네트워크는 다른 외부 전자 장치들, 예를 들어 제3 전자 장치(1031) 내지 제12 전자 장치(1044)를 포함할 수 있다. 도 10에서, 제1 전자 장치(1000) 내지 제12 전자 장치(1044) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(1000)는 구성자로서 동작하고, 제2 전자 장치(1010)는 클라이언트 등록자로서 동작하고, 제3 전자 장치(1031) 내지 제12 전자 장치(1044) 각각은 AP로서 동작한다고 가정하기로 한다.

[232] 본 개시의 일 실시 예에서, 제1 전자 장치(1000)(예: 도 1의 전자 장치(101))는 Wi-Fi 스캔 동작을 수행하여 AP 커버리지(coverage)(1020) 내의 AP들을 검출할 수 있다. 본 개시의 일 실시 예에서, AP 커버리지(1020)는 구성자, 예를 들어 제1 전자 장치(1000)가 AP들을 검출하는 것이 가능한 Wi-Fi 커버리지일 수 있다. 본 개시의 일 실시 예에서, 제1 전자 장치(1000)가 AP들을 검출하기 위한 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 제1 전자 장치(1000)가 제2 전자 장치(1010)(예: 도 1의 전자 장치(102) 또는 전자 장치(104))와 DPP 부트스트래핑

동작을 수행하기 전부터 제1 전자 장치(1000)가 DPP 구성 응답 프레임을 송신하기 전까지의 시간 기간 중 임의의 시점이 될 수 있다. 하지만, 이는 일 예일 뿐, 제1 전자 장치(1000)가 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 반드시 이로 제한되는 것은 아님에 유의하여야만 할 것이다.

[233] 제1 전자 장치(1000)가 Wi-Fi 스캔 동작을 수행함에 따라 AP 커버리지(1020) 내에서 다수의 AP들을 검출할 수 있다. 도 10에는 제1 전자 장치(1000)가 Wi-Fi 스캔 동작을 수행함에 따라 AP 커버리지(1020) 내에서 예를 들어 10개의 AP들, 예를 들어 제1 AP(1031), 제2 AP(1032), 제3 AP(1033), 제4 AP(1034), 제5 AP(1035), 제6 AP(1036), 제7 AP(1041), 제8 AP(1042), 제9 AP(1043), 및 제10 AP(1044)가 검출된 경우가 도시되어 있다. 검출된 10개의 AP들 중 6개의 AP들, 예를 들어 제1 AP(1031), 제2 AP(1032), 제3 AP(1033), 제4 AP(1034), 제5 AP(1035), 제6 AP(1036)는 제1 전자 장치(1000)에 등록되어 있는 AP들이고, 나머지 4개의 AP들, 예를 들어 제7 AP(1041), 제8 AP(1042), 제9 AP(1043), 및 제10 AP(1044)는 제1 전자 장치(1000)에 등록되어 있지 않은 AP들이라고 가정하기로 한다. 본 개시의 일 실시 예에서, 제1 전자 장치(1000)는 등록되어 있는 AP들 각각에 대한 보안 크리덴셜을 저장하고 있을 수 있다.

[234] 본 개시의 일 실시 예에 따르면, 동작 1050에서 제1 전자 장치(1000)가 제2 전자 장치(1010)로부터 DPP 구성 요청 프레임을 수신할 경우, 제1 전자 장치(1000)는 Wi-Fi 스캔 동작에 따라 검출된 다수의 AP들 중 그 AP ID가 제1 전자 장치(1000)가 저장하고 있는 크리덴셜 리스트에 포함되어 있는 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 제1 전자 장치(1000)는 구성자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 적어도 하나의 AP를 선택할 수 있다. 도 10에서는 Wi-Fi 스캔 동작에 따라 검출된 AP들이 10개이고, 그 중에서 제1 전자 장치(1000)에 등록되어 있는 AP들이 6개이므로 6개의 AP들이 선택될 수 있다.

[235] 본 개시의 일 실시 예에 따르면, 동작 1060에서 제1 전자 장치(1000)는 구성자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 선택된 적어도 하나의 AP중 세컨더리 필터링 방식을 적용하여 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식은 다음과 같은 조건들 중 적어도 하나를 포함할 수 있다.

[236] (1) 조건 1

[237] 세컨더리 필터링 방식이 적용되는 AP들이 모두 선택될 수 있다.

[238] (2) 조건 2

[239] 세컨더리 필터링 방식이 적용되는 AP들 중 구성자가 세컨더리 필터링 방식이 적용되는 시점부터 설정된 기간 내에 억세스한 기록이 있는 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 설정된 기간은 DPP 네트워크의 네트워크 상황에 따라 또는 구성자의 선택에 따라 변경될 수 있다.

[240] (3) 조건 3

[241] 세컨더리 필터링 방식이 적용되는 AP들 중 구성자와 설정된 거리 내에

존재하는 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 구성자와 특정 AP 간의 거리는 왕복 시간(round trip time: RTT)을 기반으로 검출될 수 있다. 본 개시의 일 실시 예에서, 구성자와 특정 AP 간의 거리는 구성자의 위치 정보 및 특정 AP의 위치 정보를 기반으로 검출될 수 있다. 본 개시의 일 실시 예에서, 구성자와 특정 AP간의 거리는 RTT 또는 위치 정보 뿐만 아니라 다양한 파라미터들을 기반으로 검출될 수 있음에 유의하여야만 할 것이다.

[242] (4) 조건 4

[243] 세컨더리 필터링 방식이 적용되는 AP들 중 상위 계층, 예를 들어 어플리케이션 계층을 통해 선택되는 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 구성자는 UI를 통해 세컨더리 필터링 방식이 적용되는 AP들에 대한 정보를 UI를 통해 출력하고, UI를 통해 세컨더리 필터링 방식이 적용되는 AP들 중 적어도 하나의 AP에 대한 선택을 지시하는 입력이 검출될 경우, 해당 입력에 상응하는 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 구성자는 UI를 통해 지도 상에 세컨더리 필터링 방식이 적용되는 AP들에 대한 정보를 출력하고, UI를 통해 AP들 중 적어도 하나의 AP에 대한 선택을 지시하는 입력이 검출될 경우, 해당 입력에 상응하는 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, UI를 통해 지도 상에 출력되는 AP들에 대한 정보는 구성자와 제1 거리 내에 존재하는 AP들에 대한 정보가 될 수 있거나, 또는 구성자와 제1 거리는 초과하지만 제2 거리 내에 존재하는 AP들에 대한 정보가 될 수 있거나, 또는 구성자와 제2 거리를 초과하여 존재하는 AP들에 대한 정보가 될 수 있다. 본 개시의 일 실시 예에서, 제1 거리 및 제2 거리에 대한 정보는 UI를 통해 입력될 수 있다. 본 개시의 일 실시 예에서, UI를 통해 지도 상에 출력되는 AP들에 대한 정보는 구성자의 위치와는 관계없이 UI를 통해 입력되는 위치 정보를 기반으로 할 수 있다. 예를 들어, UI를 통해 지도 상에 출력되는 AP들에 대한 정보는 UI를 통해 입력되는 위치 정보에 상응하는 위치로부터 제1 거리 내에 존재하는 AP들에 대한 정보가 될 수 있거나, 또는 상응하는 위치로부터 제1 거리는 초과하지만 제2 거리 내에 존재하는 AP들에 대한 정보가 될 수 있거나, 또는 상응하는 위치로부터 제2 거리를 초과하여 존재하는 AP들에 대한 정보가 될 수 있다.

[244] (5) 조건 5

[245] 세컨더리 필터링 방식이 적용되는 AP들 중 채널 품질을 기반으로 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식이 적용되는 AP들 중 채널 품질이 양호한 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 채널 품질이 양호하다는 것은 해당 AP로부터 수신되는 수신 신호의 채널 품질이 임계 품질 이상이라는 것을 의미할 수 있다. 본 개시의 일 실시 예에서, 채널 품질을 지시하는 파라미터들은 수신 신호 세기 지시자(received signal strength indicator: RSSI), 채널 품질 지시자(channel quality

indicator: CQI), 신호 대 잡음비(signal to noise ratio: SNR), 신호 대 간섭비(signal to interference ratio: SIR), 신호 대 간섭 잡음비(signal to interference and noise ratio: SINR), 기준 신호 수신 전력(reference signal received power: RSRP), 또는 기준 신호 수신 품질(reference signal received quality: RSRQ) 등 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식이 적용되는 AP들 중 RSSI 값이 임계값 이상인 적어도 하나의 AP가 선택될 수 있다.

[246] (6) 조건 6

[247] 세컨더리 필터링 방식이 적용되는 AP들 중 네트워크 품질을 기반으로 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 네트워크 품질은 인터넷이 사용 가능한지 여부에 의해 결정될 수 있다. 본 개시의 일 실시 예에서, 구성자는 세컨더리 필터링 방식이 적용되는 AP들 중 인터넷이 사용 가능한 적어도 하나의 AP를 선택할 수 있다.

[248] (7) 조건 7

[249] 세컨더리 필터링 방식이 적용되는 AP들 중 구성자와 설정된 거리 내에 존재하면서도, 세컨더리 필터링 방식이 적용되는 시점부터 설정된 기간 내에 구성자에 의한 억세스 기록이 있는 적어도 하나의 AP가 선택될 수 있다. 구성자와 특정 AP 간의 거리에 대해서는 조건 3에서 설명하였으므로 여기서는 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 설정된 기간은 DPP 네트워크의 네트워크 상황에 따라 또는 구성자의 선택에 따라 변경될 수 있다.

[250] (8) 조건 8

[251] 세컨더리 필터링 방식이 적용되는 AP들 중에서 구성자와 설정된 거리 내에 존재하는 AP들 중 상위 계층, 예를 들어 어플리케이션 계층을 통해 선택되는 적어도 하나의 AP가 선택될 수 있다. 본 개시의 일 실시 예에서, 구성자는 UI를 통해 세컨더리 필터링 방식이 적용되는 AP들 중에서 구성자와 설정된 거리 내에 존재하는 AP들에 대한 정보를 UI를 통해 출력하고, UI를 통해 구성자와 설정된 거리 내에 존재하는 AP들 중 적어도 하나의 AP에 대한 선택을 지시하는 입력이 검출될 경우, 해당 입력에 상응하는 적어도 하나의 AP를 선택할 수 있다.

[252] 본 개시의 일 실시 예에서, 조건 1 내지 조건 8 이외의 다양한 조건들이 세컨더리 필터링 방식에 포함될 수 있음은 물론이며, 세컨더리 필터링 방식은 조건 1 내지 조건 8만을 포함하는 것으로 제한되는 것은 아님에 유의하여야만 할 것이다. 본 개시의 일 실시 예에서, 조건 1 내지 조건 8 중 적어도 두 개가 조합되어 새로운 조건이 될 수 있다.

[253] 본 개시의 일 실시 예에 따르면, 동작 1070에서 제1 전자 장치(1000)는 세컨더리 필터링 방식을 적용하여 선택된 적어도 하나의 AP 각각에 대한 크리덴셜 오브젝트를 포함하는 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, 적어도 하나의 AP 각각에 대한 DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 제2 전자 장치(1010)로 송신할 수 있다.

[254] 본 개시의 일 실시 예에서, 제1 전자 장치(1000)는 구성자 기반 Wi-Fi 스캔 필터링 방식을 기반으로 선택된 AP들, 예를 들어 제1 AP(1031), 제2 AP(1032), 제3 AP(1033), 제4 AP(1034), 제5 AP(1035), 및 제6 AP(1036)에 대해 세컨더리 필터링 방식을 적용하여 제4 AP(1034), 제5 AP(1035), 및 제6 AP(1036)를 선택할 수 있다. 제1 전자 장치(1000)는 선택된 제4 AP(1034), 제5 AP(1035), 및 제6 AP(1036) 각각에 대한 크리덴셜 오브젝트를 포함하는 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, 제4 AP(1034), 제5 AP(1035), 및 제6 AP(1036) 각각에 대한 DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 제2 전자 장치(1010)로 송신할 수 있다.

[255] 도 11은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 구성자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 신호 흐름도이다.

[256] 도 11을 참조하면, 전자 장치(예: 제1 전자 장치(1110))와 외부 전자 장치(예: 제2 전자 장치(1100)) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(1110)는 구성자이면서 개시자로서 동작하고, 제2 전자 장치(1100)는 클라이언트 등록자이면서 응답자로서 동작한다고 가정하기로 한다.

[257] 동작 1113에서, 클라이언트 등록자이면서, 응답자로 동작하는 제2 전자 장치(1100)는 DPP 존재 안내 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 존재 안내 프레임에 대한 해쉬는 SHA256("chirp" | B_R)일 수 있다. 본 개시의 일 실시 예에서, B_R은 제2 전자 장치(1100)의 공중 부트스트래핑 키를 나타낼 수 있다. 일 실시 예에서, DPP 존재 안내 프레임은 도 7에서 설명한 DPP 존재 안내 프레임과 유사할 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1100)는 DPP 부트스트래핑 동작 동안 명시된 채널에서 청취 동작을 수행할 수 있다. 구성자이면서 개시자로서 동작하는 제1 전자 장치(1110)는 OOB 메카니즘, 예를 들어, QR 코드 스캔, NFC 탭, 또는 BLE 교환을 사용하여 제2 전자 장치(1100)로부터 부트스트래핑 정보를 획득할 수 있다. 본 개시의 일 실시 예에서, 부트스트래핑 정보는 DPP 인증을 위한 제2 전자 장치(1100)의 공중 부트스트래핑 키(B_R), 전세계 동작 클래스 채널, 및/또는 채널 리스트를 포함할 수 있다. DPP 부트스트래핑 동작 동안, 제2 전자 장치(1100)는 제1 전자 장치(1110)가 제2 전자 장치(1100)를 발견하는 것을 도와주도록 제2 전자 장치(1100)의 존재를 선택적으로 안내할 수 있다. 본 개시의 일 실시 예에서, 동작 1115에서, 제2 전자 장치(1100)는 DPP 존재 안내 프레임을 송신할 수 있다. 예를 들어, 제 2 전자 장치(1100)는 주기적으로 DPP 존재 안내 프레임을 송신할 수 있다.

[258] 본 개시의 일 실시 예에 따르면, 제1 전자 장치(1110)는 DPP 인증 요청 프레임을 브로드캐스트함으로써 DPP 부트스트래핑 동작 동안 수신되는 채널 정보를 기반으로 하는 채널에서 동작을 시작할 수 있다. 예를 들어, 제1 전자 장치(1110)는 동작 1117에서 DPP 인증 요청 프레임을 브로드캐스트할 수 있다.

본 개시의 일 실시 예에서, DPP 인증 요청 프레임은 SHA256(B_R), SHA256(B_I), P_I 및 {I-nonce, I-capabilities}$_{k1}$을 포함할 수 있다. 예를 들어, SHA256(B_R)는 B_R에 대한 SHA256 해쉬를 나타내고, B_I는 제1 전자 장치(1110)의 공중 부트스트래핑 키를 나타내고, SHA256(B_I)는 B_I에 대한 SHA256 해쉬를 나타내고, P_I는 제1 전자 장치(1110)의 공중 프로토콜 키를 나타내고, I-nonce는 개시자 넌스 어트리뷰트를 나타내고, I-capabilities는 개시자 능력들 어트리뷰트를 나타내고, k1은 제1 중개키를 나타낼 수 있다. 일 실시 예에서, DPP 인증 요청 프레임에 포함되는 제2 전자 장치(1100)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1110)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1110)의 공중 프로토콜 키, 또는 제1 중개키로 인크립트된 개시자 넌스 어트리뷰트와 개시자 능력들 어트리뷰트 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[259] 본 개시의 일 실시 예에 따르면, 제1 전자 장치(1110)가 DPP 인증 요청 프레임을 브로드캐스트하고, 제2 전자 장치(1100)가 이 DPP 인증 요청 프레임을 성공적으로 수신하게 되면, B_R 에 대한 해쉬 함수 값인 H(B_R)과 매치할 수 있다. 동작 1119에서, 제2 전자 장치(1100)는 DPP 인증 요청 프레임에 대한 응답 프레임인 DPP 인증 응답 프레임을 제1 전자 장치(1110)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임은 DPP status 필드, SHA256(B_R), [SHA256(B_I)], P_R 및 {R-nonce, I-nonce, R-capabilities, {R-auth}$_{ke}$}$_{k2}$을 포함할 수 있다. 본 개시의 일 실시 예에서, P_R은 제2 전자 장치(1100)의 공중 프로토콜 키를 나타내고, R-nonce는 응답자 넌스 어트리뷰트를 나타내고, R-capabilities는 응답자 능력들 어트리뷰트를 나타내고, R-auth는 응답자, 예를 들어 제2 전자 장치(1100)의 인증 태그를 나타내고, ke는 인크립션 키를 나타내고, k2는 제2 중개키를 나타내고, [ ]는 선택적으로 존재하는 값을 나타낼 수 있다. 예를 들어, [SHA256(B_I)]는 특정 조건이 만족되거나, 또는 선택적으로 DPP 인증 응답 프레임에 포함될 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임에 포함되는 제2 전자 장치(1100)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1110)의 공중 부트스트래핑 키에 대한 해쉬, 제2 전자 장치(1100)의 공중 프로토콜 키, 또는 제2 중개키로 인크립트된 응답자 넌스 어트리뷰트, 응답자 능력들 어트리뷰트, 및 응답자의 인증 태그 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다. DPP status 필드는 표 1에서 설명한 바 있으므로 여기서는 그 상세한 설명을 생략하기로 한다.

[260] 동작 1121에서, 제2 전자 장치(1100)로부터 DPP 인증 응답 프레임을 수신한 제1 전자 장치(1110)는 제2 전자 장치(1100)로 DPP 인증 확인 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 확인 프레임은 DPP status 필드, SHA256(B_R), [SHA256(B_I)] 및 {I-auth}$_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, I-auth는 제1 전자 장치(1110)의 인증 태그를 나타내며, ke는 인크립션 키를 나타낼 수 있다.

[261] 동작 1123에서, 제1 전자 장치(1110)로부터 DPP 인증 확인 프레임을 수신한 제2 전자 장치(1100)는 제1 전자 장치(1110)로 DPP 구성 요청 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 {E-nonce, configuration attributes}$_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, E-nonce는 E-nonce 어트리뷰트를 나타내며, configuration attributes는 구성 어트리뷰트 오브젝트들을 나타낼 수 있다. 구성 어트리뷰트 오브젝트는 디바이스 이름(device name) 어트리뷰트, Wi-Fi 기술(Wi-Fi technology) 어트리뷰트, 또는 네트워크 역할 어트리뷰트 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 요청하는 메시지일 수 있다.

[262] 이렇게, 제2 전자 장치(1100)로부터 DPP 구성 요청 프레임을 수신한 제1 전자 장치(1110)는 동작 1125에서 DPP 구성 오브젝트 필터링 동작을 수행할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작은 구성자에 저장되어 있는 적어도 하나의 DPP 구성 오브젝트에 대해서 설정되어 있는 적어도 하나의 필터링 방식을 적용하여 적어도 하나의 DPP 구성 오브젝트를 선택하는 동작을 의미할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트는 크리덴셜 오브젝트를 포함하므로 DPP 구성 오브젝트 필터링 동작은 크리덴셜 필터링 동작으로도 칭해질 수 있다.

[263] 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작에 사용되는 적어도 하나의 필터링 방식은 Wi-Fi 스캔 필터링 방식 또는 세컨더리 필터링 방식 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식 또는 등록자 기반 Wi-Fi 스캔 필터링 방식 중 적어도 하나를 포함할 수 있다. Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식에 대해서는 상기에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 동작1125에서 제1 전자 장치(1110)는 도 10에서 설명한 바와 같이 구성자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 적용하여 DPP 구성 오브젝트 필터링 동작을 수행한다고 가정하기로 한다.

[264] 본 개시의 일 실시 예에서, 제1 전자 장치(1110)는 동작 1111에서 Wi-Fi 스캔 동작을 수행하여 AP 커버리지 내의 AP들을 검출할 수 있다. 본 개시의 일 실시 예에서, AP 커버리지는 제1 전자 장치(1100)가 AP들을 검출하는 것이 가능한 Wi-Fi 커버리지일 수 있다. 본 개시의 일 실시 예에서, 제1 전자 장치(1110)가 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 제1 전자 장치(1110)가 제2 전자 장치(1100)와 DPP 부트스트래핑 동작을 수행하기 전부터 제1 전자 장치(1110)가 DPP 구성 응답 프레임을 송신하기 전까지의 시간 기간 중 임의의 시점이 될 수 있다. 하지만, 이는 일 예일 뿐, 제1 전자 장치(1110)가 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 이로 제한되는 것은 아님에 유의하여야만 할 것이다. 제1 전자 장치(1110)는 동작 1111에서 Wi-Fi 스캔 동작을 통해 검출된 다수의

AP들 중 그 AP ID가 제1 전자 장치(1110)가 저장하고 있는 크리덴셜 리스트에 포함되어 있는 적어도 하나의 AP를 선택할 수 있다. 예를 들어, 도 10을 참조하여, 도 11에서는 Wi-Fi 스캔 동작에 따라 검출된 AP들이 10개이고, 그 중에서 제1 전자 장치(1110)에 등록되어 있는 AP들, 예를 들어 제1 전자 장치(1110)의 크리덴셜 리스트에 포함되어 있는 AP ID들에 대응될 수 있는 AP들이 6개라고 가정하기로 한다. 이 경우, 구성자 기반 Wi-Fi 스캔 필터링 방식이 적용됨에 따라 수행된 Wi-Fi 스캔 동작을 통해 검출된 10개의 AP들 중 제1 전자 장치(1110)에 등록되어 있는 6개의 AP들이 선택될 수 있다.

[265] 본 개시의 일 실시 예에서, 제1 전자 장치(1110)는 동작 1125에서 구성자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 선택된 6개의 AP들에 대해 세컨더리 필터링 방식을 적용하여 최종적으로 DPP 구성 오브젝트를 제공할 적어도 하나의 AP를 선택할 수 있다. 세컨더리 필터링 방식이 포함할 수 있는 조건들에 대해서는 도 10에서 설명한 바 있으므로 여기서는 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 도 10을 참조하여, 제1 전자 장치(1110)는 세컨더리 필터링 방식까지 적용하여 최종적으로 3개의 AP들을 선택하였다고 가정하기로 한다.

[266] 동작 1127에서 제1 전자 장치(1110)는 제2 전자 장치(1100)로 DPP 구성 요청 프레임에 대한 응답인 DPP 구성 응답 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임은 선택된 3개의 AP들에 대한 DPP 구성 오브젝트들을 포함할 수 있다. 따라서, DPP 구성 응답 프레임은 DPP status 필드와, $\{\text{E-nonce, configuration object, configuration object, configuration object}\}_{ke}$를 포함할 수 있다. 그리고, 3개의 DPP 구성 오브젝트는 각각 JSON 인코딩될 수 있다.

[267] 동작 1129에서, DPP 구성 응답 프레임을 수신한 제2 전자 장치(1100)는 DPP 구성 결과 프레임을 제1 전자 장치(1110)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 결과 프레임은 $\{\text{DPP Status, E-nonce}\}_{ke}$를 포함할 수 있다. 도 11에 별도로 도시되어 있지는 않으나, 이후 제2 전자 장치(1100)는 DPP 구성 응답 프레임을 통해 수신한 DPP 구성 오브젝트를 기반으로 DPP 억세스 동작을 수행하여 제2 전자 장치(1100)에 적합한 AP를 선택하고, 선택한 AP와 보안 연결을 설정할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임을 통해 3개의 DPP 구성 오브젝트들이 수신되었으므로 제2 전자 장치(1100)는 3개의 DPP 구성 오브젝트들에 기반하여 제2 전자 장치(1100)에 적합한 1개의 AP를 선택하고, 선택한 AP와 보안 연결을 설정할 수 있다. 제2 전자 장치(1100)가 보안 연결을 설정할 AP를 선택하는 기준은 다양한 형태로 구현될 수 있다.

[268] 도 12는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 등록자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 도면이다.

[269] 도 12를 참조하면, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자

장치(예: 제1 전자 장치(1200)), 외부 전자 장치(예: 제2 전자 장치(1210))를 포함할 수 있다. DPP 네트워크는 다른 외부 전자 장치들, 예를 들어 제3 전자 장치(1231) 내지 제12 전자 장치(1244)를 포함할 수 있다. 도 12에서, 제1 전자 장치(1200) 내지 제12 전자 장치(1244) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(1200)는 구성자로서 동작하고, 제2 전자 장치(1210)는 클라이언트 등록자로서 동작하고, 제3 전자 장치(1231) 내지 제12 전자 장치(1244) 각각은 AP로서 동작한다고 가정하기로 한다.

[270] 본 개시의 일 실시 예에서, 제2 전자 장치(1210)(예: 도 1의 전자 장치(102) 또는 전자 장치(104))는 제1 전자 장치(1200)(예: 도 1의 전자 장치(101))와 DPP 부트스트래핑 동작 및 DPP 인증 동작을 완료한 후, 예를 들어 제1 전자 장치(1200)로부터 DPP 인증 확인 프레임을 수신한 후, 동작 1250에서 Wi-Fi 스캔 결과를 제1 전자 장치(1200)로 송신할 수 있다. 이에 대해서 설명하면 다음과 같다.

[271] 본 개시의 일 실시 예에서, 제2 전자 장치(1210)는 Wi-Fi 스캔 동작을 수행하여 AP 커버리지(1220) 내의 AP들을 검출할 수 있다. 본 개시의 일 실시 예에서, AP 커버리지(1220)는 제2 전자 장치(1210)가 AP들을 검출하는 것이 가능한 Wi-Fi 커버리지일 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1210)가 AP들을 검출하기 위한 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은, 제2 전자 장치(1210)가 제1 전자 장치(1200)와 DPP 부트스트래핑 동작을 수행하기 전부터 제2 전자 장치(1210)가 DPP 구성 요청 프레임을 송신하기 전까지의 시간 기간 중 임의의 시점이 될 수 있다. 하지만, 이는 일 예일 뿐, 제2 전자 장치(1210)가 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 반드시 이로 제한되는 것은 아님에 유의하여야만 할 것이다.

[272] 제2 전자 장치(1210)가 Wi-Fi 스캔 동작을 수행함에 따라 AP 커버리지(1220) 내에서 다수의 AP들을 검출할 수 있다. 도 12에는 제2 전자 장치(1210)가 Wi-Fi 스캔 동작을 수행함에 따라 AP 커버리지(1220) 내에서 예를 들어 10개의 AP들, 예를 들어 제1 AP(1231), 제2 AP(1232), 제3 AP(1233), 제4 AP(1234), 제5 AP(1235), 제6 AP(1236), 제7 AP(1241), 제8 AP(1242), 제9 AP(1243), 및 제10 AP(1244)가 검출된 경우가 도시되어 있다.

[273] 제2 전자 장치(1210)는 이렇게 검출된 10개의 AP들에 대한 Wi-Fi 스캔 결과를 동작 1250에서 제1 전자 장치(1200)로 송신할 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1210)는 다양한 방식들을 기반으로 Wi-Fi 스캔 결과를 제1 전자 장치(1200)로 송신할 수 있으며, Wi-Fi 스캔 결과를 송신하는 방식들에 대해서 설명하면 다음과 같다.

[274] 본 개시의 일 실시 예에 따르면, 제2 전자 장치(1210)는 벤더 특정 정보 엘리먼트(vendor specific information element: VSIE)를 기반으로 Wi-Fi 스캔 결과를 제1 전자 장치(1200)로 송신할 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1210)는 Wi-Fi 스캔 결과를 송신하기 위해 VSIE ID를 설정하고,

설정된 VSIE ID에 상응하는 VSIE에 Wi-Fi 스캔 결과를 포함시켜, Wi-Fi 스캔 결과가 포함된 VSIE를 DPP 구성 요청 프레임에 포함시킬 수 있다. 본 개시의 일 실시 예에서, VSIE는 벤더 별로 사용될 수 있는 정보 엘리먼트(information element: IE)로서, 벤더 별로 상이하게 설정될 수 있다.

[275] 본 개시의 일 실시 예에 따르면, 제2 전자 장치(1210)는 액션 프레임(action frame)을 기반으로 Wi-Fi 스캔 결과를 제1 전자 장치(1200)로 송신할 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1210)는 DPP 프로비저닝 프로세스에서 사용되고 있는 Wi-Fi 채널에서 별도의 액션 프레임을 통해 Wi-Fi 스캔 결과를 송신할 수 있다. 여기서, Wi-Fi 스캔 결과를 송신하기 위해 사용되는 액션 프레임은 기존의 DPP에서 사용되고 있는 액션 프레임들 중 하나일 수도 있고, 또는 새롭게 정의되는 액션 프레임일 수도 있다.

[276] 본 개시의 일 실시 예에 따르면, 제 2 전자 장치(1210)는 OOB 방식으로 Wi-Fi 스캔 결과를 제1 전자 장치(1200)로 송신할 수 있다. 일 예로 OOB 방식은 BLE 또는 Bluetooth와 같은 다른 통신 방식들을 사용하여 Wi-Fi 스캔 결과를 송신하는 방식이다.

[277] 본 개시의 일 실시 예에서, Wi-Fi 스캔 결과를 송신하는 방식들은 상기에서 설명한 방식들 중 어느 하나로 제한되는 것은 아니며, 상기에서 설명한 방식들 이외에도 다양한 방식들로 Wi-Fi 스캔 결과가 송신될 수 있음에 유의하여야만 할 것이다.

[278] Wi-Fi 스캔 결과를 송신한 후, 제2 전자 장치(1210)는 DPP 구성 요청 프레임을 제1 전자 장치(1200)로 송신할 수 있다. 본 개시의 일 실시 예에 따르면, 동작 1260에서 제1 전자 장치(1200)가 제2 전자 장치(1210)로부터 DPP 구성 요청 프레임을 수신함에 따라, 제1 전자 장치(1200)는 제2 전자 장치(1210)로부터 수신한 Wi-Fi 스캔 결과를 기반으로 제1 전자 장치(1200)가 저장하고 있는 크리덴셜 리스트에 포함되어 있는 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 제1 전자 장치(1200)는 등록자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 적어도 하나의 AP를 선택할 수 있다.

[279] 도 12에서는 제2 전자 장치(1210)가 검출한 10개의 AP들 중 6개의 AP들, 예를 들어 제1 AP(1231), 제2 AP(1232), 제3 AP(1233), 제4 AP(1234), 제5 AP(1235), 제6 AP(1236)는 제1 전자 장치(1200)에 등록되어 있는 AP들이고, 나머지 4개의 AP들, 예를 들어 제7 AP(1241), 제8 AP(1242), 제9 AP(1243), 및 제10 AP(1244)는 제1 전자 장치(1200)에 등록되어 있지 않은 AP들이라고 가정하기로 한다. 제1 전자 장치(1200)는 등록되어 있는 AP들 각각에 대한 보안 크리덴셜을 저장하고 있을 수 있다. 제2 전자 장치(1210)의 Wi-Fi 스캔 동작에 따라 검출된 AP들이 10개이고, 그 중에서 제1 전자 장치(1200)에 등록되어 있는 AP들이 6개이므로 6개의 AP들이 선택될 수 있다.

[280] 본 개시의 일 실시 예에 따르면, 동작 1260에서 제1 전자 장치(1200)는 등록자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 선택된 적어도 하나의 AP중 세컨더리

필터링 방식을 적용하여 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식은 도 10에서 설명한 바와 같은 조건들, 예를 들어 조건 1, 조건 2, 조건 3, 조건 4, 조건 5, 조건 6, 조건 7, 또는 조건 8 중 적어도 하나를 포함할 수 있다. 조건 1 내지 조건 8에 대해서는 도 10에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다.

[281] 본 개시의 일 실시 예에 따르면, 동작 1270에서 제1 전자 장치(1200)는 세컨더리 필터링 방식을 적용하여 선택된 적어도 하나의 AP 각각에 대한 크리덴셜 오브젝트를 포함하는 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, 적어도 하나의 AP 각각에 대한 DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 제2 전자 장치(1210)로 송신할 수 있다.

[282] 본 개시의 일 실시 예에서, 제1 전자 장치(1200)는 등록자 기반 Wi-Fi 스캔 필터링 방식을 기반으로 선택된 AP들, 예를 들어 제1 AP(1231), 제2 AP(1232), 제3 AP(1233), 제4 AP(1234), 제5 AP(1235), 및 제6 AP(1236)에 대해 세컨더리 필터링 방식을 적용하여 제1 AP(1231), 제2 AP(1232), 및 제3 AP(1233)를 선택할 수 있다. 제1 전자 장치(1200)는 선택된 제1 AP(1231), 제2 AP(1232), 및 제3 AP(1233) 각각에 대한 크리덴셜 오브젝트를 포함하는 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, 제1 AP(1231), 제2 AP(1232), 및 제3 AP(1233) 각각에 대한 DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 제2 전자 장치(1210)로 송신할 수 있다.

[283] 도 13은 본 개시의 일 실시 예에 따른 DPP 네트워크에서 등록자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 신호 흐름도이다.

[284] 도 13을 참조하면, 전자 장치(예: 제1 전자 장치(1310))와 외부 전자 장치(예: 제2 전자 장치(1300)) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(1310)는 구성자이면서 개시자로서 동작하고, 제2 전자 장치(1300)는 클라이언트 등록자이면서 응답자로서 동작한다고 가정하기로 한다.

[285] 동작 1313에서, 클라이언트 등록자이면서 응답자로 동작하는 제2 전자 장치(1300)는 DPP 존재 안내 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 존재 안내 프레임에 대한 해쉬는 SHA256("chirp" | B_R)일 수 있다. 본 개시의 일 실시 예에서, B_R은 제2 전자 장치(1300)의 공중 부트스트래핑 키를 나타낼 수 있다. 본 개시의 일 실시 예에서, DPP 존재 안내 프레임은 도 7에서 설명한 DPP 존재 안내 프레임과 유사할 수 있다. 일 본 개시의 실시 예에서, 제2 전자 장치(1300)는 DPP 부트스트래핑 동작 동안 명시된 채널에서 청취 동작을 수행할 수 있다. 구성자이면서 개시자자로 동작하는 제1 전자 장치(1310)는 OOB 메카니즘, 예를 들어, QR 코드 스캔, NFC 탭, 또는 BLE 교환을 사용하여 제2 전자 장치(1300)로부터 부트스트래핑 정보를 획득할 수 있다. 본 개시의 일 실시 예에서, 부트스트래핑 정보는 DPP 인증을 위한 제2 전자 장치(1300)의 공중 부트스트래핑 키(B_R), 전세계 동작 클래스 채널, 및/또는 채널 리스트를 포함할

수 있다. DPP 부트스트래핑 동작 동안, 제2 전자 장치(1300)는 제1 전자 장치(1310)가 제2 전자 장치(1300)를 발견하는 것을 도와주도록 제2 전자 장치(1300)의 존재를 선택적으로 안내할 수 있다. 본 개시의 일 실시 예에서, 동작 1315에서, 제2 전자 장치(1300)는 DPP 존재 안내 프레임을 송신할 수 있다. 예를 들어, 제2 전자 장치(1300)는 주기적으로 DPP 존재 안내 프레임을 송신할 수 있다.

[286] 본 개시의 일 실시 예에 따르면, 제1 전자 장치(1310)는 DPP 인증 요청 프레임을 브로드캐스트함으로써 DPP 부트스트래핑 동작 동안 수신되는 채널 정보를 기반으로 하는 채널에서 동작을 시작할 수 있다. 예를 들어, 제1 전자 장치(1310)는 동작 1317에서 DPP 인증 요청 프레임을 브로드캐스트할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임은 SHA256(B_R), SHA256(B_I), P_I 및 {I-nonce, I-capabilities}$_{k1}$을 포함할 수 있다. 예를 들어, SHA256(B_R)는 B_R에 대한 SHA256 해쉬를 나타내고, B_I는 제1 전자 장치(1310)의 공중 부트스트래핑 키를 나타내고, SHA256(B_I)는 B_I에 대한 SHA256 해쉬를 나타내고, P_I는 제1 전자 장치(1310)의 공중 프로토콜 키를 나타내고, I-nonce는 개시자 넌스 어트리뷰트를 나타내고, I-capabilities는 개시자 능력들 어트리뷰트를 나타내고, k1은 제1 중개키를 나타낼 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임에 포함되는 제2 전자 장치(1300)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1310)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1310)의 공중 프로토콜 키, 또는 제1 중개키로 인크립트된 개시자 넌스 어트리뷰트와 개시자 능력들 어트리뷰트 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[287] 본 개시의 일 실시 예에 따르면, 제1 전자 장치(1310)가 DPP 인증 요청 프레임들을 브로드캐스트하고, 제2 전자 장치(1300)가 이 DPP 인증 요청 프레임을 성공적으로 수신하게 되면, B_R 에 대한 해쉬 함수 값인 H(B_R)과 매치할 수 있다. 동작 1319에서, 제2 전자 장치(1300)는 DPP 인증 요청 프레임에 대한 응답 프레임인 DPP 인증 응답 프레임을 제1 전자 장치(1310)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임은 DPP status 필드, SHA256(B_R), [SHA256(B_I)], P_R 및 {R-nonce, I-nonce, R-capabilities, {R-auth}$_{ke}$}$_{k2}$을 포함할 수 있다. 예를 들어, P_R은 제2 전자 장치(1300)의 공중 프로토콜 키를 나타내고, R-nonce는 응답자 넌스 어트리뷰트를 나타내고, R-capabilities는 응답자 능력들 어트리뷰트를 나타내고, R-auth는 응답자, 예를 들어 제2 전자 장치(1300)의 인증 태그를 나타내고, ke는 인크립션 키를 나타내고, k2는 제2 중개키를 나타내고, [ ]는 선택적으로 존재하는 값을 나타낼 수 있다. 예를 들어, [SHA256(B_I)]는 특정 조건이 만족되거나, 또는 선택적으로 DPP 인증 응답 프레임에 포함될 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임에 포함되는 제2 전자 장치(1300)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1310)의 공중 부트스트래핑 키에 대한 해쉬, 제2 전자 장치(1300)의 공중 프로토콜 키, 또는 제2

중개키로 인크립트된 응답자 넌스 어트리뷰트, 응답자 능력들 어트리뷰트, 및 응답자의 인증 태그 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다. DPP status 필드는 표 1에서 설명한 바 있으므로 여기서는 그 상세한 설명을 생략하기로 한다.

[288] 동작 1321에서, 제2 전자 장치(1300)로부터 DPP 인증 응답 프레임을 수신한 제1 전자 장치(1310)는 제2 전자 장치(1300)로 DPP 인증 확인 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 확인 프레임은 DPP status 필드, $SHA256(B_R)$, $[SHA256(B_I)]$ 및 $\{I\text{-}auth\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, I-auth는 제1 전자 장치(1310)의 인증 태그를 나타내며, ke는 인크립션 키를 나타낼 수 있다.

[289] 제1 전자 장치(1310)로부터 DPP 인증 확인 프레임을 수신한 제2 전자 장치(1300)는 동작 1323에서 Wi-Fi 스캔 결과를 제1 전자 장치(1310)로 송신할 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1300)가 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 제2 전자 장치(1300)가 제1 전자 장치(1310)와 DPP 부트스트래핑 동작을 수행하기 전부터 제2 전자 장치(1300)가 DPP 구성 요청 프레임을 송신하기 전까지의 시간 기간 중 임의의 시점이 될 수 있다. 하지만, 이는 일 예일 뿐, 제2 전자 장치(1300)가 Wi-Fi 스캔 동작을 수행하기 시작하는 시점은 반드시 이로 제한되는 것은 아님에 유의하여야만 할 것이다. 제2 전자 장치(1300)는 동작 1311에서 Wi-Fi 스캔 동작을 수행함에 따라 AP 커버리지 내에서 다수의 AP들을 검출할 수 있다. 본 개시의 일 실시 예에서, AP 커버리지는 제2 전자 장치(1300)가 AP들을 검출하는 것이 가능한 Wi-Fi 커버리지일 수 있다. 도 13에서는 도 12를 참조하여, 제2 전자 장치(1300)가 Wi-Fi 스캔 동작을 수행함에 따라 AP 커버리지 내에서 예를 들어 10개의 AP들, 예를 들어 제1 AP 내지 제10 AP가 검출되었다고 가정하기로 한다.

[290] 본 개시의 일 실시 예에서, 제2 전자 장치(1300)는 도 12에서 설명한 바와 같이 다양한 방식들 중 어느 한 방식으로 Wi-Fi 스캔 결과를 제1 전자 장치(1310)로 송신할 수 있으며, 도 13에서는 별도의 액션 프레임을 통해 Wi-Fi 스캔 결과를 송신한다고 가정하기로 한다. 본 개시의 일 실시 예에서, 동작 1323에서 등록자(1300)는 동작 1311에서 검출된 10개의 AP들에 대한 Wi-Fi 스캔 결과를 포함하는 액션 프레임을 제1 전자 장치(1310)로 송신할 수 있다.

[291] 이렇게 Wi-Fi 스캔 결과를 송신한 후, 동작 1325에서 제2 전자 장치(1300)는 제1 전자 장치(1310)로 DPP 구성 요청 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 $\{E\text{-}nonce, configuration\ attributes\}_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, E-nonce는 E-nonce 어트리뷰트를 나타내며, configuration attributes는 구성 어트리뷰트 오브젝트들을 나타낼 수 있다. 구성 어트리뷰트 오브젝트는 디바이스 이름(device name) 어트리뷰트, Wi-Fi 기술(Wi-Fi technology) 어트리뷰트, 또는 네트워크 역할 어트리뷰트 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은

네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 요청하는 메시지일 수 있다.

[292] 이렇게, 제2 전자 장치(1300)로부터 DPP 구성 요청 프레임을 수신한 제1 전자 장치(1310)는 동작 1327에서 DPP 구성 오브젝트 필터링 동작을 수행할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작에 사용되는 적어도 하나의 필터링 방식은 Wi-Fi 스캔 필터링 방식 또는 세컨더리 필터링 방식 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, Wi-Fi 스캔 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식 또는 등록자 기반 Wi-Fi 스캔 필터링 방식 중 적어도 하나를 포함할 수 있다. Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식에 대해서는 상기에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 동작 1327에서 제1 전자 장치(1310)는 도 12에서 설명한 바와 같이 등록자 기반 Wi-Fi 스캔 필터링 방식 및 세컨더리 필터링 방식을 적용하여 DPP 구성 오브젝트 필터링 동작을 수행한다고 가정하기로 한다.

[293] 본 개시의 일 실시 예에서, 제1 전자 장치(1310)는 제2 전자 장치(1300)로부터 수신한 Wi-Fi 스캔 결과를 기반으로 제1 전자 장치(1310)가 저장하고 있는 크리덴셜 리스트에 포함되어 있는 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 제1 전자 장치(1310)는 등록자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 적어도 하나의 AP를 선택할 수 있다.

[294] 도 13에서는, 도 12를 참조하여, 제2 전자 장치(1300)가 검출한 10개의 AP들 중 6개의 AP들, 예를 들어 제1 AP 내지 제6 AP는 제1 전자 장치(1310)에 등록되어 있는 AP들이고, 나머지 4개의 AP들, 예를 들어 제7 AP 내지 제10 AP는 제1 전자 장치(1310)에 등록되어 있지 않은 AP들이라고 가정하기로 한다. 본 개시의 일 실시 예에서, 제1 전자 장치(1310)는 등록되어 있는 AP들 각각에 대한 보안 크리덴셜을 저장하고 있을 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1300)의 Wi-Fi 스캔 동작에 따라 검출된 AP들이 10개이고, 그 중에서 제1 전자 장치(1310)에 등록되어 있는 AP들이 6개이므로 6개의 AP들이 선택될 수 있다.

[295] 본 개시의 일 실시 예에서, 제1 전자 장치(1310)는 동작 1327에서 등록자 기반 Wi-Fi 스캔 필터링 방식을 적용하여 선택된 6개의 AP들에 대해 세컨더리 필터링 방식을 적용하여 최종적으로 DPP 구성 오브젝트를 제공할 적어도 하나의 AP를 선택할 수 있다. 세컨더리 필터링 방식이 포함할 수 있는 조건들에 대해서는 도 10에서 설명한 바 있으므로 여기서는 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 제1 전자 장치(1310)는 세컨더리 필터링 방식까지 적용하여 최종적으로 3개의 AP들을 선택하였다고 가정하기로 한다.

[296] 동작 1329에서 제1 전자 장치(1310)는 제2 전자 장치(1300)로 DPP 구성 요청 프레임에 대한 응답인 DPP 구성 응답 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임은 선택된 3개의 AP들에 대한 DPP 구성

오브젝트들을 포함할 수 있다. 따라서, DPP 구성 응답 프레임은 DPP status 필드와, {E-nonce, configuration object, configuration object, configuration object}$_{ke}$를 포함할 수 있다. 그리고, 3개의 DPP 구성 오브젝트는 각각 JSON 인코딩될 수 있다.

[297] 동작 1331에서, DPP 구성 응답 프레임을 수신한 제2 전자 장치(1300)는 DPP 구성 결과 프레임을 제1 전자 장치(1310)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 결과 프레임은 {DPP Status, E-nonce}$_{ke}$를 포함할 수 있다. 도 13에 별도로 도시되어 있지는 않으나, 이후 제2 전자 장치(1300)는 DPP 구성 응답 프레임을 통해 수신한 DPP 구성 오브젝트를 기반으로 DPP 억세스 동작을 수행하여 제2 전자 장치(1300)에 적합한 AP를 선택하고, 선택한 AP와 보안 연결을 설정할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임을 통해 3개의 DPP 구성 오브젝트들이 수신되었으므로 제2 전자 장치(1300)는 3개의 DPP 구성 오브젝트들에 기반하여 제2 전자 장치(1300)에 적합한 1개의 AP를 선택하고, 선택한 AP와 보안 연결을 설정할 수 있다. 제2 전자 장치(1300)가 보안 연결을 설정할 AP를 선택하는 기준은 다양한 형태로 구현될 수 있다.

[298] 도 14는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 도면이다.

[299] 도 14를 참조하면, DPP 네트워크는 다수의 전자 장치들, 예를 들어, 전자 장치, 예를 들어 제1 전자 장치(1400), 외부 전자 장치, 예를 들어 제2 전자 장치(1410)를 포함할 수 있다. 도 14에서, 제1 전자 장치(1400) 및 제2 전자 장치(1410) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(1400)는 구성자로서 동작하고, 제2 전자 장치(1410)는 클라이언트 등록자로서 동작한다고 가정하기로 한다.

[300] 본 개시의 일 실시 예에 따르면, 동작 1420에서, 제1 전자 장치(1400)(예: 도 1의 전자 장치(101))는 적어도 하나의 AP에 대한 DPP 구성 오브젝트를 저장하고 있다. 도 14에서는 제1 전자 장치(1400)가 6개의 AP들, 예를 들어 제1 AP 내지 제6 AP에 대한 DPP 구성 오브젝트를 저장하고 있고, 따라서 제1 AP 내지 제6 AP에 대한 보안 크리덴셜을 저장하고 있다고 가정하기로 한다.

[301] 본 개시의 일 실시 예에 따르면, 동작 1460에서 제1 전자 장치(1400)가 외부 전자 장치(예: 도 1의 전자 장치(102 또는 104)), 예를 들어 제2 전자 장치(1410)로부터 DPP 구성 요청 프레임을 수신할 경우, 제1 전자 장치(1400)는 제1 전자 장치(1400)에 DPP 구성 오브젝트가 저장되어 있는 6개의 AP들에 대해 세컨더리 필터링 방식을 적용하여 적어도 하나의 AP를 선택할 수 있다. 본 개시의 일 실시 예에서, 세컨더리 필터링 방식은 도 10에서 설명한 바와 같은 조건들, 예를 들어 조건 1, 조건 2, 조건 3, 조건 4, 조건 5, 조건 6, 조건 7, 조건 8, 또는 조건 9 중 적어도 하나를 포함할 수 있다. 조건 1 내지 조건 9에 대해서는 도 10에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다.

[302] 본 개시의 일 실시 예에 따르면, 동작 1470에서 제1 전자 장치(1400)는 세컨더리

필터링 방식을 적용하여 선택된 적어도 하나의 AP 각각에 대한 크리덴셜 오브젝트를 포함하는 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, 적어도 하나의 AP 각각에 대한 DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 제2 전자 장치(1410)로 송신할 수 있다.

[303] 본 개시의 일 실시 예에서, 제1 전자 장치(1400)는 세컨더리 필터링 방식을 기반으로 제1 AP, 제3 AP, 및 제5AP를 선택할 수 있다. 제1 전자 장치(1400)는 선택된 제1 AP, 제3 AP, 및 제5AP 각각에 대한 크리덴셜 오브젝트를 포함하는 DPP 구성 오브젝트를 DPP 구성 응답 프레임에 포함시키고, 제1 AP, 제3 AP, 및 제5AP 각각에 대한 DPP 구성 오브젝트가 포함된 DPP 구성 응답 프레임을 제2 전자 장치(1410)로 송신할 수 있다.

[304] 도 15는 본 개시의 일 실시 예에 따른 DPP 네트워크에서 세컨더리 필터링 방식을 기반으로 DPP 구성 오브젝트를 제공하는 동작을 개략적으로 도시한 신호 흐름도이다.

[305] 도 15를 참조하면, 전자 장치(예: 제1 전자 장치(1510))와 외부 전자 장치(예: 제2 전자 장치(1500)) 각각은 DPP 장치일 수 있으며, 제1 전자 장치(1510)는 구성자이면서 개시자로서 동작하고, 제2 전자 장치(1500)는 클라이언트 등록자이면서 응답자로서 동작한다고 가정하기로 한다.

[306] 동작 1513에서, 클라이언트 등록자이면서 응답자로 동작하는 제2 전자 장치(1500)는 DPP 존재 안내 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 존재 안내 프레임에 대한 해쉬는 SHA256("chirp" | B_R)일 수 있다. 본 개시의 일 실시 예에서, B_R은 제2 전자 장치(1500)의 공중 부트스트래핑 키를 나타낼 수 있다. 본 개시의 일 실시 예에서, DPP 존재 안내 프레임은 도 7에서 설명한 DPP 존재 안내 프레임과 유사할 수 있다. 본 개시의 일 실시 예에서, 제2 전자 장치(1500)는 DPP 부트스트래핑 동작 동안 명시된 채널에서 청취 동작을 수행할 수 있다. 구성자이면서 개시자로서 동작하는 제1 전자 장치(1510)는 OOB 메카니즘, 예를 들어, QR 코드 스캔, NFC 탭, 또는 BLE 교환을 사용하여 제2 전자 장치(1500)로부터 부트스트래핑 정보를 획득할 수 있다. 본 개시의 일 실시 예에서, 부트스트래핑 정보는 DPP 인증을 위한 제2 전자 장치(1500)의 공중 부트스트래핑 키(B_R), 전세계 동작 클래스 채널, 및/또는 채널 리스트를 포함할 수 있다. DPP 부트스트래핑 동작 동안, 제2 전자 장치(1500)는 제1 전자 장치(1510)가 제2 전자 장치(1500)를 발견하는 것을 도와주도록 제2 전자 장치(1500)의 존재를 선택적으로 안내할 수 있다. 본 개시의 일 실시 예에서, 동작 1515에서, 제2 전자 장치(1500)는 DPP 존재 안내 프레임을 송신할 수 있다. 예를 들어, 제2 전자 장치(1500)는 주기적으로 DPP 존재 안내 프레임을 송신할 수 있다.

[307] 본 개시의 일 실시 예에 따르면, 제1 전자 장치(1510)는 DPP 인증 요청 프레임을 브로드캐스트함으로써 DPP 부트스트래핑 동작 동안 수신되는 채널 정보를 기반으로 하는 채널에서 동작을 시작할 수 있다. 예를 들어, 제1 전자

장치(1510)는 동작 1517에서 DPP 인증 요청 프레임을 브로드캐스트할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임은 SHA256(B_R), SHA256(B_I), P_I 및 {I-nonce, I-capabilities}$_{k1}$을 포함할 수 있다. 예를 들어, SHA256(B_R)는 B_R에 대한 SHA256 해쉬를 나타내고, B_I는 제1 전자 장치(1510)의 공중 부트스트래핑 키를 나타내고, SHA256(B_I)는 B_I에 대한 SHA256 해쉬를 나타내고, P_I는 제1 전자 장치(1510)의 공중 프로토콜 키를 나타내고, I-nonce는 개시자 넌스 어트리뷰트를 나타내고, I-capabilities는 개시자 능력들 어트리뷰트를 나타내고, k1은 제1 중개키를 나타낼 수 있다. 본 개시의 일 실시 예에서, DPP 인증 요청 프레임에 포함되는 제2 전자 장치(1500)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1510)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1510)의 공중 프로토콜 키, 또는 제1 중개키로 인크립트된 개시자 넌스 어트리뷰트와 개시자 능력들 어트리뷰트 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[308] 본 개시의 일 실시 예에 따르면, 제1 전자 장치(1510)가 DPP 인증 요청 프레임들을 브로드캐스트하고, 제2 전자 장치(1500)가 이 DPP 인증 요청 프레임을 성공적으로 수신하게 되면, B_R 에 대한 해쉬 함수 값인 H(B_R)과 매치할 수 있다. 동작 1519에서, 제2 전자 장치(1500)는 DPP 인증 요청 프레임에 대한 응답 프레임인 DPP 인증 응답 프레임을 제1 전자 장치(1510)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임은 DPP status 필드, SHA256(B_R), [SHA256(B_I)], P_R 및 {R-nonce, I-nonce, R-capabilities, {R-auth}$_{ke}$}$_{k2}$을 포함할 수 있다. 본 개시의 일 실시 예에서, P_R은 제2 전자 장치(1500)의 공중 프로토콜 키를 나타내고, R-nonce는 응답자 넌스 어트리뷰트를 나타내고, R-capabilities는 응답자 능력들 어트리뷰트를 나타내고, R-auth는 응답자, 예를 들어 제2 전자 장치(1500)의 인증 태그를 나타내고, ke는 인크립션 키를 나타내고, k2는 제2 중개키를 나타내고, [ ]는 선택적으로 존재하는 값을 나타낼 수 있다. 예를 들어, [SHA256(B_I)]는 특정 조건이 만족되거나, 또는 선택적으로 DPP 인증 응답 프레임에 포함될 수 있다. 본 개시의 일 실시 예에서, DPP 인증 응답 프레임에 포함되는 제2 전자 장치(1500)의 공중 부트스트래핑 키에 대한 해쉬, 제1 전자 장치(1510)의 공중 부트스트래핑 키에 대한 해쉬, 제2 전자 장치(1500)의 공중 프로토콜 키, 또는 제2 중개키로 인크립트된 응답자 넌스 어트리뷰트, 응답자 능력들 어트리뷰트, 및 응답자의 인증 태그 중 적어도 하나는 DPP 인증 동작에서 사용되는 보안 정보일 수 있다. DPP status 필드는 표 1에서 설명한 바 있으므로 여기서는 그 상세한 설명을 생략하기로 한다.

[309] 동작 1521에서, 제2 전자 장치(1500)로부터 DPP 인증 응답 프레임을 수신한 제1 전자 장치(1510)는 제2 전자 장치(1500)로 DPP 인증 확인 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 인증 확인 프레임은 DPP status 필드, SHA256(B_R), [SHA256(B_I)] 및 {I-auth}$_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, I-auth는 제1 전자 장치(1510)의 인증 태그를 나타내며, ke는 인크립션

키를 나타낼 수 있다.

[310] 동작 1523에서, 제1 전자 장치(1510)로부터 DPP 인증 확인 프레임을 수신한 제2 전자 장치(1500)는 제1 전자 장치(1510)로 DPP 구성 요청 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 {E-nonce, configuration attributes}$_{ke}$를 포함할 수 있다. 본 개시의 일 실시 예에서, E-nonce는 E-nonce 어트리뷰트를 나타내며, configuration attributes는 구성 어트리뷰트 오브젝트들을 나타낼 수 있다. 구성 어트리뷰트 오브젝트는 디바이스 이름(device name) 어트리뷰트, Wi-Fi 기술(Wi-Fi technology) 어트리뷰트, 또는 네트워크 역할 어트리뷰트 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 요청 프레임은 네트워크 구성 정보, 예를 들어 DPP 구성 오브젝트를 요청하는 메시지일 수 있다.

[311] 이렇게, 제2 전자 장치(1500)로부터 DPP 구성 요청 프레임을 수신한 제1 전자 장치(1510)는 동작 1525에서 DPP 구성 오브젝트 필터링 동작을 수행할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작은 구성자에 저장되어 있는 적어도 하나의 DPP 구성 오브젝트에 대해서 설정되어 있는 적어도 하나의 필터링 방식을 적용하여 적어도 하나의 DPP 구성 오브젝트를 선택하는 동작을 의미할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 오브젝트 필터링 동작에 사용되는 적어도 하나의 필터링 방식은 세컨더리 필터링 방식을 포함할 수 있다. 세컨더리 필터링 방식에 대해서는 상기에서 설명한 바 있으므로 여기서는 그 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 동작1525에서 제1 전자 장치(1510)는 도 14에서 설명한 바와 같이 세컨더리 필터링 방식을 적용하여 DPP 구성 오브젝트 필터링 동작을 수행한다고 가정하기로 한다.

[312] 본 개시의 일 실시 예에서, 제1 전자 장치(1510)는 동작 1525에서 제1 전자 장치(1510)가 DPP 구성 오브젝트를 저장하고 있는 6개의 AP들, 예를 들어 제1 AP 내지 제6 AP에 대해 세컨더리 필터링 방식을 적용하여 최종적으로 DPP 구성 오브젝트를 제공할 적어도 하나의 AP를 선택할 수 있다. 세컨더리 필터링 방식이 포함할 수 있는 조건들에 대해서는 도 10에서 설명한 바 있으므로 여기서는 구체적인 설명을 생략하기로 한다. 본 개시의 일 실시 예에서, 제1 전자 장치(1510)는 세컨더리 필터링 방식까지 적용하여 최종적으로 3개의 AP들을 선택하였다고 가정하기로 한다.

[313] 동작 1527에서 제1 전자 장치(1510)는 제2 전자 장치(1500)로 DPP 구성 요청 프레임에 대한 응답인 DPP 구성 응답 프레임을 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임은 선택된 3개의 AP들에 대한 DPP 구성 오브젝트들을 포함할 수 있다. 따라서, DPP 구성 응답 프레임은 DPP status 필드와, {E-nonce, configuration object, configuration object, configuration object}$_{ke}$를 포함할 수 있다. 그리고, 3개의 DPP 구성 오브젝트는 각각 JSON 인코딩될 수 있다.

[314] 동작 1529에서, DPP 구성 응답 프레임을 수신한 제2 전자 장치(1500)는 DPP

구성 결과 프레임을 제1 전자 장치(1510)로 송신할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 결과 프레임은 $\{\text{DPP Status, E-nonce}\}_{ke}$를 포함할 수 있다. 도 15에 별도로 도시되어 있지는 않으나, 이후 제2 전자 장치(1500)는 DPP 구성 응답 프레임을 통해 수신한 DPP 구성 오브젝트를 기반으로 DPP 억세스 동작을 수행하여 제2 전자 장치(1500)에 적합한 AP를 선택하고, 선택한 AP와 보안 연결을 설정할 수 있다. 본 개시의 일 실시 예에서, DPP 구성 응답 프레임을 통해 3개의 DPP 구성 오브젝트들이 수신되었으므로 제2 전자 장치(1500)는 3개의 DPP 구성 오브젝트들에 기반하여 제2 전자 장치(1500)에 적합한 1개의 AP를 선택하고, 선택한 AP와 보안 연결을 설정할 수 있다. 제2 전자 장치(1500)가 보안 연결을 설정할 AP를 선택하는 기준은 다양한 형태로 구현될 수 있다.

[315] 다양한 실시 예들은 DPP 네트워크에서 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[316] 다양한 실시 예들은 DPP 네트워크에서 다수의 네트워크 구성 정보들을 송수신하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[317] 다양한 실시 예들은 DPP 네트워크에서 등록자에 적합한 네트워크 구성 정보를 송수신하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[318] 다양한 실시 예들은 DPP 네트워크에서 제공할 네트워크 구성 정보들을 필터링하는 기준을 제공하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[319] 다양한 실시 예들은 DPP 네트워크에서 설정되어 있는 조건들을 기반으로 다수의 DPP 구성 오브젝트들을 제공하는 전자 장치 및 그 동작 방법을 제공할 수 있다.

[320] 본 개시의 다양한 실시 예들에 따르면, 전자 장치(예: 도 1의 전자 장치(101))에 의해 수행되는 방법은 외부 전자 장치(예: 도 1의 전자 장치(102) 또는 전자 장치(104))로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하는 동작, 설정되어 있는 필터링 방식을 기반으로 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치(102 또는 104)로 송신할 적어도 하나의 네트워크 구성 정보를 선택하는 동작, 및 상기 외부 전자 장치로 상기 선택한 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 송신하는 동작을 포함할 수 있다.

[321] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식은 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식 또는 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있으며, 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식은 등록자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있다.

[322] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식은 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식, 상기 외부 전자 장치(102

또는 104)의 스캔 결과를 기반으로 하는 필터링 방식, 또는 적어도 하나의 필터링 조건을 포함하는 세컨더리 필터링 방식 중 적어도 하나를 포함할 수 있다.

[323] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 외부 전자 장치(102 또는 104)로 송신할 적어도 하나의 네트워크 구성 정보를 선택하는 동작은, 스캔 동작을 수행하여 다른 외부 전자 장치들(예: 도 1의 전자 장치(102) 또는 전자 장치(104))을 검출하는 동작, 상기 검출된 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)를 선택하는 동작, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 동작을 포함할 수 있다.

[324] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 외부 전자 장치(102 또는 104)로 송신할 적어도 하나의 네트워크 구성 정보를 선택하는 동작은, 상기 외부 전자 장치(102 또는 104)로부터 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 수신하는 동작, 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 다른 외부 전자 장치들(102 또는 104)을 확인하는 동작, 상기 확인된 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)를 선택하는 동작, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 전자 장치(101)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 동작을 포함할 수 있다.

[325] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 적어도 하나의 필터링 조건을 포함하는 세컨더리 필터링 방식일 경우, 상기 외부 전자 장치(102 또는 104)로 송신할 적어도 하나의 네트워크 구성 정보를 선택하는 동작은, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 적어도 하나의 필터링 조건을 만족하는 적어도 하나의 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 동작을 포함할 수 있다.

[326] 본 개시의 다양한 실시 예들에 따르면, 상기 적어도 하나의 필터링 조건은, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 세컨더리 필터링 방식이 적용되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제1 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성

정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)가 설정되어 있는 기간 내에 억세스한 기록을 가지는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제2 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)와 설정되어 있는 거리 내에 존재하는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제3 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상위 계층을 통해 선택되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제4 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 채널 품질이 임계 채널 품질 이상인 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제5 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 네트워크 품질을 기반으로 선택되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제6 조건, 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)와 설정되어 있는 거리 내에 존재하고, 상기 전자 장치(101)가 설정되어 있는 기간 내에 억세스한 기록을 가지는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제7 조건, 또는 상기 전자 장치(101)에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들(102 또는 104) 중 상기 전자 장치(101)와 설정되어 있는 거리 내에 존재하고, 상위 계층을 통해 선택되는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치(102 또는 104)로 송신할 네트워크 구성 정보로 선택하는 제8 조건 중 적어도 하나를 포함할 수 있다.

[327] 본 개시의 다양한 실시 예들에 따르면, 상기 방법은 상기 외부 전자 장치(102 또는 104)와 보안 정보를 기반으로 인증 동작을 수행하는 동작을 더 포함할 수 있다. 본 개시의 일 실시 예에서, 인증 동작은 상기 전자 장치(101)와 외부 전자 장치(102 또는 104)간에 DPP 인증 요청 프레임 및 DPP 인증 응답 프레임이 송수신되는 동작을 포함할 수 있다. 본 개시의 일 실시 예에서, 상기 DPP 인증

요청 프레임에 포함되는 응답자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 프로토콜 키, 또는 제1 중개키로 인크립트된 개시자 넌스 어트리뷰트와 개시자 능력들 어트리뷰트중 적어도 하나는 인증 동작, 예를 들어 DPP 인증 동작에서 사용되는 보안 정보일 수 있다. 본 개시의 일 실시 예에서, 상기 DPP 인증 응답 프레임에 포함되는 응답자의 공중 부트스트래핑 키에 대한 해쉬, 개시자의 공중 부트스트래핑 키에 대한 해쉬, 응답자의 공중 프로토콜 키, 또는 제2 중개키로 인크립트된 응답자 넌스 어트리뷰트, 응답자 능력들 어트리뷰트, 및 개시자 능력들 어트리뷰트 중 적어도 하나는 인증 동작, 예를 들어 DPP 인증 동작에서 사용되는 보안 정보일 수 있다.

[328] 본 개시의 다양한 실시 예들에 따르면, 전자 장치(예: 도 1의 전자 장치(101))에 의해 수행되는 방법은 외부 전자 장치(예: 도 1의 전자 장치(102) 또는 전자 장치(104))와 보안 정보를 기반으로 인증 동작을 수행하는 동작, 상기 외부 전자 장치(102 또는 104)로 네트워크 구성 정보를 요청하는 제1 메시지를 송신하는 동작, 상기 외부 전자 장치(102 또는 104)로부터 상기 외부 전자 장치(102 또는 104)에 저장되어 있는 다수의 네트워크 구성 정보들 중 설정되어 있는 필터링 방식을 기반으로 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 수신하는 동작을 포함할 수 있다.

[329] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식은 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식, 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식, 또는 적어도 하나의 필터링 조건을 포함하는 세컨더리 필터링 방식 중 적어도 하나를 포함할 수 있다. 본 개시의 일 실시 예에서, 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식은 구성자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있으며, 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식은 등록자 기반 Wi-Fi 스캔 필터링 방식이 될 수 있다.

[330] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 전자 장치(101)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 방법은 상기 외부 전자 장치(102 또는 104)로 상기 전자 장치(101)의 스캔 결과를 송신하는 동작을 더 포함할 수 있고, 상기 제2 메시지에 포함되어 있는 적어도 하나의 네트워크 구성 정보는 상기 외부 전자 장치(102 또는 104)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 스캔 결과에 상응하는 다른 외부 전자 장치들(예: 도 1의 전자 장치(102) 또는 도 1의 전자 장치(104)) 중 상기 외부 전자 장치(102 또는 104)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보일 수 있다.

[331] 본 개시의 다양한 실시 예들에 따르면, 상기 필터링 방식이 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 제2 메시지에 포함되어 있는 적어도 하나의 네트워크 구성 정보는, 상기 외부 전자

장치(102 또는 104)에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치(102 또는 104)의 스캔 결과를 기반으로 검출된 다른 외부 전자 장치들(102 또는 104) 중 상기 외부 전자 장치(102 또는 104)에 등록되어 있는 적어도 하나의 다른 외부 전자 장치(102 또는 104)에 상응하는 네트워크 구성 정보일 수 있다.

[332] 본 개시의 특정 예제들은 프로그램이 컴퓨터 또는 프로세서에 의해 실행될 때, 컴퓨터 또는 프로세서가 여기에 개시되어 있는 임의의 예제, 실시 예, 측면 및/또는 청구항에 따른 방법을 수행하게 하는 인스트럭션들을 포함하는 컴퓨터 프로그램을 제공한다.

[333] 본 개시의 특정 예제들은 선행 예제에 따른 컴퓨터 프로그램을 저장하고 있는 컴퓨터 또는 프로세서-리드 가능 데이터 캐리어를 제공한다.

[334] 본 개시가 다양한 실시 예들을 참조하여 도시되고 설명되고 있지만, 형태 및 세부 사항들의 다양한 변경들은 첨부 청구항들 및 그 균등물들에 의해 정의되는 바와 같은 본 개시의 사상 및 범위를 벗어남이 없이 이루어질 수 있다는 것이 해당 기술 분야의 당업자들에 의해 이해될 것이다.

청구범위

[청구항 1] 전자 장치에 있어서,
통신 회로;
적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는:
상기 통신 회로를 통해, 외부 전자 장치로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하고,
설정되어 있는 필터링 방식을 기반으로 상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치로 송신할 적어도 하나의 네트워크 구성 정보를 선택하고, 및
상기 통신 회로를 통해, 상기 외부 전자 장치로 상기 선택한 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 송신하도록 설정되는 전자 장치.

[청구항 2] 제1항에 있어서,
상기 필터링 방식은 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식 또는 상기 외부 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식 중 적어도 하나를 포함하는 전자 장치.

[청구항 3] 제1항에 있어서,
상기 필터링 방식은 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식, 상기 외부 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식, 또는 적어도 하나의 필터링 조건을 포함하는 세컨더리(secondary) 필터링 방식 중 적어도 하나를 포함하는 전자 장치.

[청구항 4] 제1항에 있어서,
상기 필터링 방식이 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식일 경우,
상기 적어도 하나의 프로세서는:
상기 통신 회로를 통해, 스캔 동작을 수행하여 다른 외부 전자 장치들을 검출하고,
상기 검출된 다른 외부 전자 장치들 중 상기 전자 장치에 등록되어 있는 적어도 하나의 다른 외부 전자 장치를 선택하고, 및
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 전자 장치에 등록되어 있는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하도록 설정되는 전자 장치.

[청구항 5] 제1항에 있어서,
상기 필터링 방식이 상기 외부 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식일 경우,
상기 적어도 하나의 프로세서는:

상기 통신 회로를 통해, 상기 외부 전자 장치로부터 상기 외부 전자 장치의 스캔 결과를 수신하고,
상기 외부 전자 장치의 스캔 결과를 기반으로 다른 외부 전자 장치들을 확인하고,
상기 확인된 다른 외부 전자 장치들 중 상기 전자 장치에 등록되어 있는 적어도 하나의 다른 외부 전자 장치를 선택하고, 및
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 전자 장치에 등록되어 있는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하도록 설정되는 전자 장치.

[청구항 6] 제1항에 있어서,
상기 필터링 방식이 적어도 하나의 필터링 조건을 포함하는 세컨더리(secondary) 필터링 방식일 경우,
상기 적어도 하나의 프로세서는:
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 적어도 하나의 필터링 조건을 만족하는 적어도 하나의 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하도록 설정되는 전자 장치.

[청구항 7] 제6항에 있어서,
상기 적어도 하나의 필터링 조건은:
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 상기 세컨더리 필터링 방식이 적용되는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제1 조건;
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 상기 전자 장치가 설정되어 있는 기간 내에 억세스한 기록을 가지는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제2 조건;
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 상기 전자 장치와 설정되어 있는 거리 내에 존재하는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제3 조건;
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 상위 계층을 통해 선택되는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부

전자 장치로 송신할 네트워크 구성 정보로 선택하는 제4 조건;
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 채널 품질이 임계 채널 품질 이상인 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제5 조건;
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 네트워크 품질을 기반으로 선택되는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제6 조건;
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 상기 전자 장치와 설정되어 있는 거리 내에 존재하고, 상기 전자 장치가 설정되어 있는 기간 내에 억세스한 기록을 가지는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제7 조건; 또는
상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들에 상응하는 다른 외부 전자 장치들 중 상기 전자 장치와 설정되어 있는 거리 내에 존재하고, 상위 계층을 통해 선택되는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보를 상기 외부 전자 장치로 송신할 네트워크 구성 정보로 선택하는 제8 조건 중 적어도 하나를 포함하는 전자 장치.

[청구항 8] 제1항 내지 제7항 중 어느 한 항에 있어서,
상기 적어도 하나의 프로세서는:
상기 통신 회로를 통해, 상기 외부 전자 장치와 보안 정보를 기반으로 인증 동작을 수행하도록 더 설정되는 전자 장치.

[청구항 9] 전자 장치에 있어서,
통신 회로;
적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는:
상기 통신 회로를 통해, 외부 전자 장치와 보안 정보를 기반으로 인증 동작을 수행하고,
상기 통신 회로를 통해, 상기 외부 전자 장치로 네트워크 구성 정보를 요청하는 제1 메시지를 송신하고, 및
상기 통신 회로를 통해, 상기 외부 전자 장치로부터 상기 외부 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 설정되어 있는 필터링 방식을 기반으로 선택된 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 수신하도록 설정되는 전자 장치.

[청구항 10] 제9항에 있어서,
상기 필터링 방식은 상기 외부 전자 장치의 스캔 결과를 기반으로 하는

필터링 방식, 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식, 또는 적어도 하나의 필터링 조건을 포함하는 세컨더리(secondary) 필터링 방식 중 적어도 하나를 포함하는 전자 장치.

[청구항 11] 제9항에 있어서,
상기 필터링 방식이 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식일 경우,
상기 적어도 하나의 프로세서는:
상기 통신 회로를 통해, 상기 외부 전자 장치로 상기 전자 장치의 스캔 결과를 송신하도록 더 설정되고,
상기 제2 메시지에 포함되어 있는 적어도 하나의 네트워크 구성 정보는 상기 외부 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 스캔 결과에 상응하는 다른 외부 전자 장치들 중 상기 외부 전자 장치에 등록되어 있는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보인 전자 장치.

[청구항 12] 제9항에 있어서,
상기 필터링 방식이 상기 외부 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식일 경우, 상기 제2 메시지에 포함되어 있는 적어도 하나의 네트워크 구성 정보는, 상기 외부 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치의 스캔 결과를 기반으로 확인된 다른 외부 전자 장치들 중 상기 외부 전자 장치에 등록되어 있는 적어도 하나의 다른 외부 전자 장치에 상응하는 네트워크 구성 정보인 전자 장치.

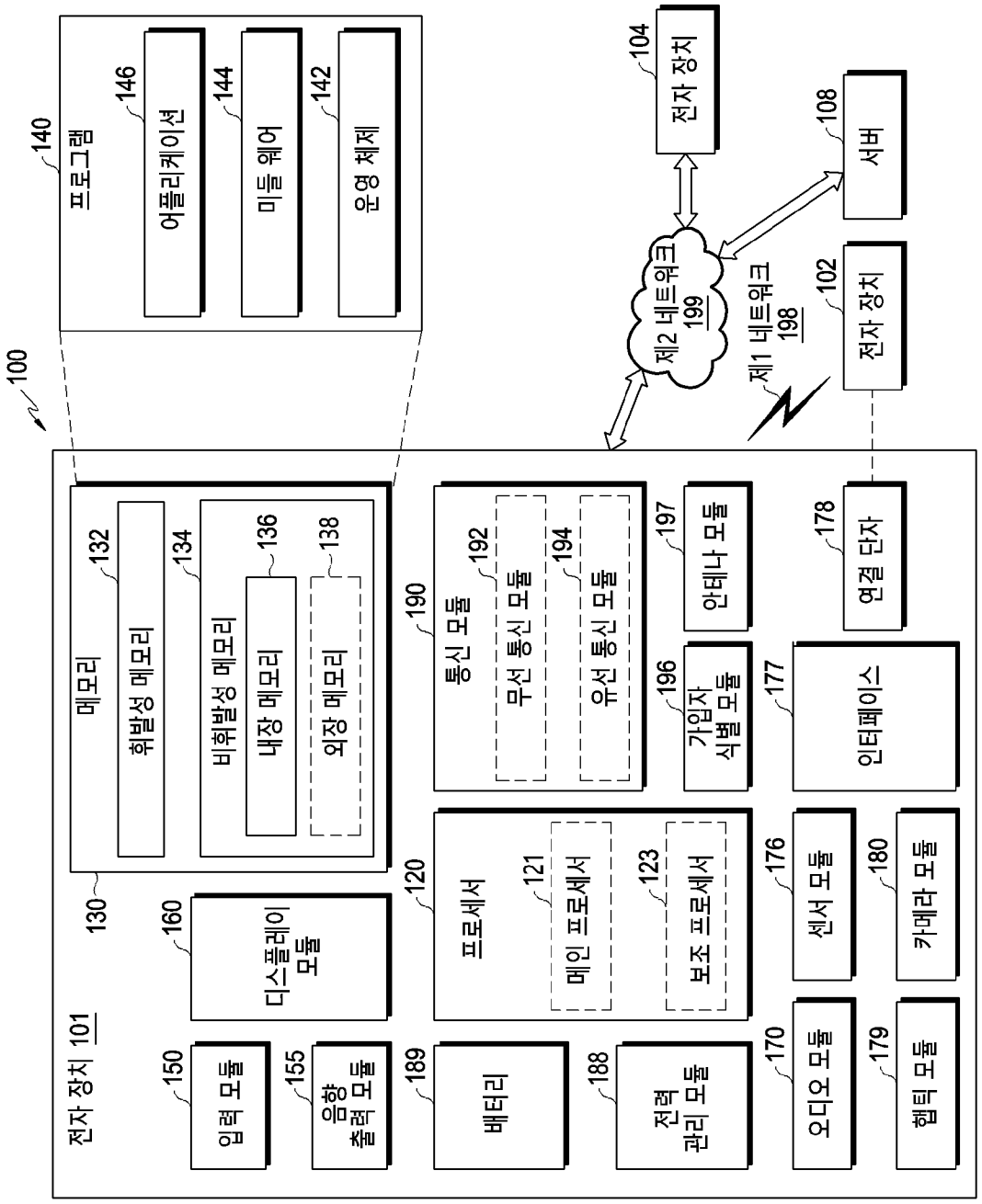
[청구항 13] 전자 장치에 의해 수행되는 방법에 있어서,
외부 전자 장치로부터 네트워크 구성 정보를 요청하는 제1 메시지를 수신하는 동작;
설정되어 있는 필터링 방식을 기반으로 상기 전자 장치에 저장되어 있는 다수의 네트워크 구성 정보들 중 상기 외부 전자 장치로 송신할 적어도 하나의 네트워크 구성 정보를 선택하는 동작; 및
상기 외부 전자 장치로 상기 선택한 적어도 하나의 네트워크 구성 정보를 포함하는 제2 메시지를 송신하는 동작을 포함하는 전자 장치에 의해 수행되는 방법.

[청구항 14] 제13항에 있어서,
상기 필터링 방식은 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식 또는 상기 외부 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식 중 적어도 하나를 포함하는 전자 장치에 의해 수행되는 방법.

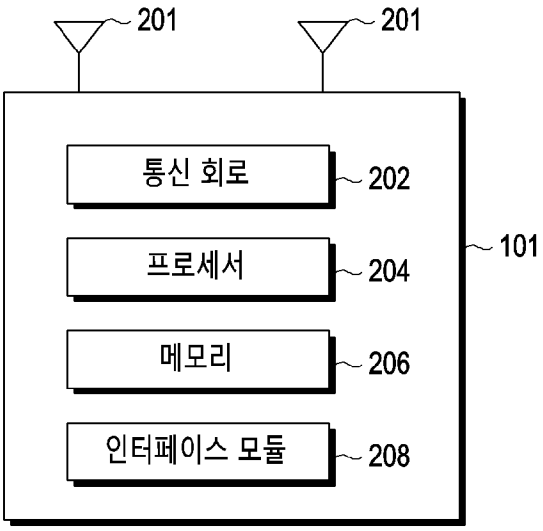
[청구항 15] 제13항에 있어서,
상기 필터링 방식은 상기 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식, 상기 외부 전자 장치의 스캔 결과를 기반으로 하는 필터링 방식,

또는 적어도 하나의 필터링 조건을 포함하는 세컨더리(secondary) 필터링 방식 중 적어도 하나를 포함하는 전자 장치에 의해 수행되는 방법.

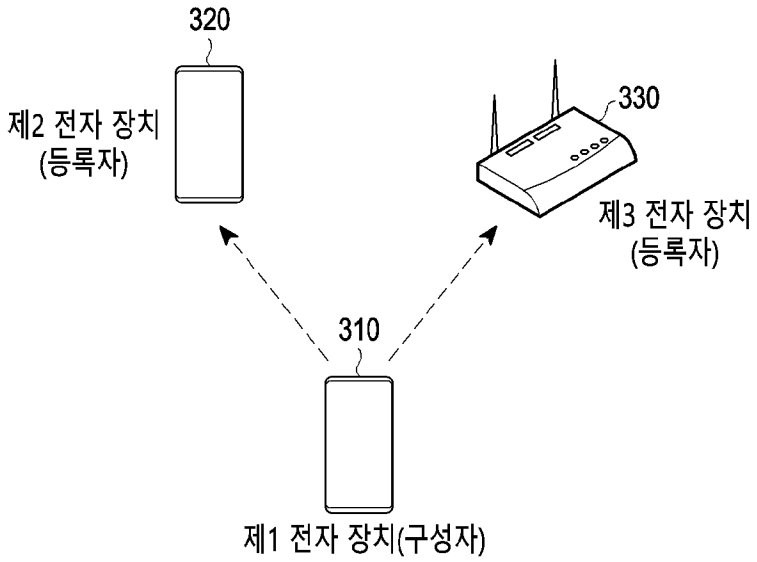
[도1]


100
전자 장치 101
프로그램 140
어플리케이션 146
미들 웨어 144
운영 체제 142
메모리 130
휘발성 메모리 132
비휘발성 메모리 134
내장 메모리 136
외장 메모리 138
디스플레이 모듈 160
입력 모듈 150
음향 출력 모듈 155
프로세서 120
메인 프로세서 121
보조 프로세서 123
통신 모듈 190
무선 통신 모듈 192
유선 통신 모듈 194
가입자 식별 모듈 196
안테나 모듈 197
인터페이스 177
연결 단자 178
센서 모듈 176
카메라 모듈 180
배터리 189
전력 관리 모듈 188
오디오 모듈 170
햅틱 모듈 179
전자 장치 104
서버 108
제2 네트워크 199
제1 네트워크 198
전자 장치 102

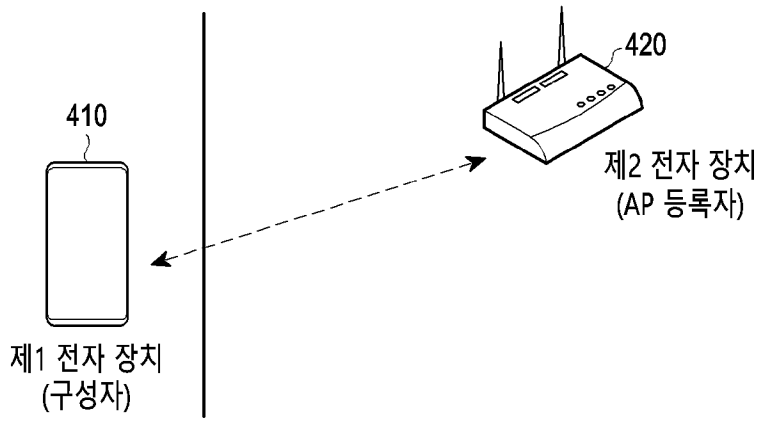
[도2]


201
201
통신 회로
202
프로세서
204
메모리
206
인터페이스 모듈
208
101

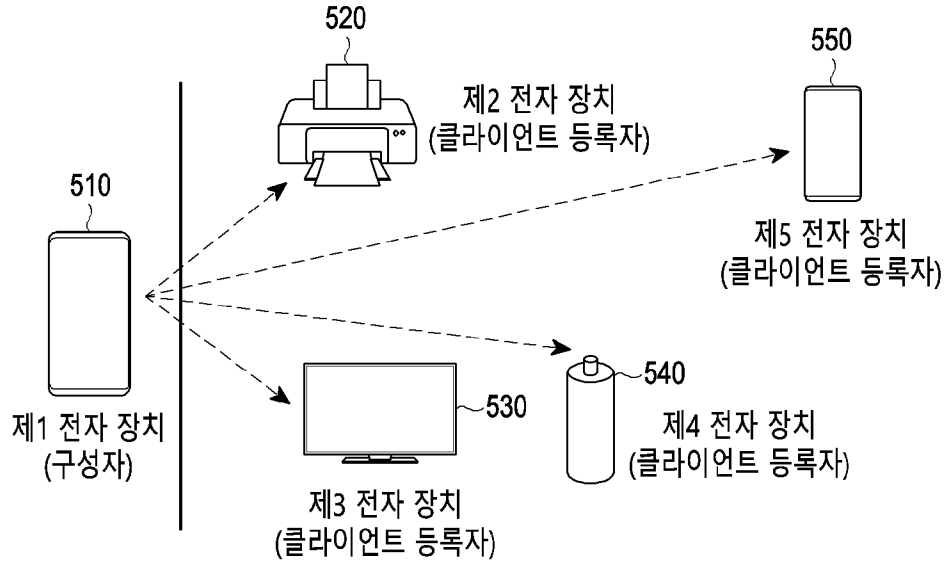
[도3]


320
제2 전자 장치
(등록자)
330
제3 전자 장치
(등록자)
310
제1 전자 장치(구성자)

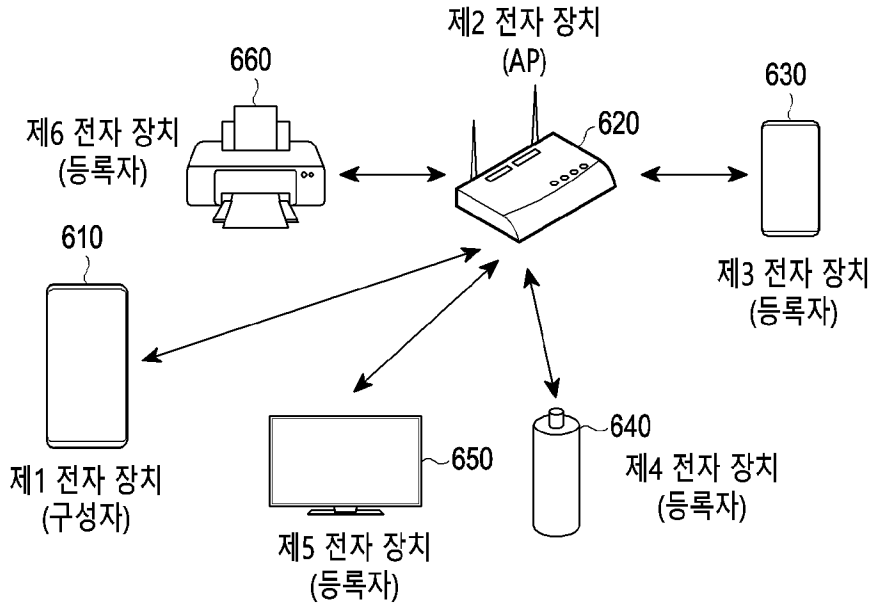
[도4]


420
410
제2 전자 장치
(AP 등록자)
제1 전자 장치
(구성자)

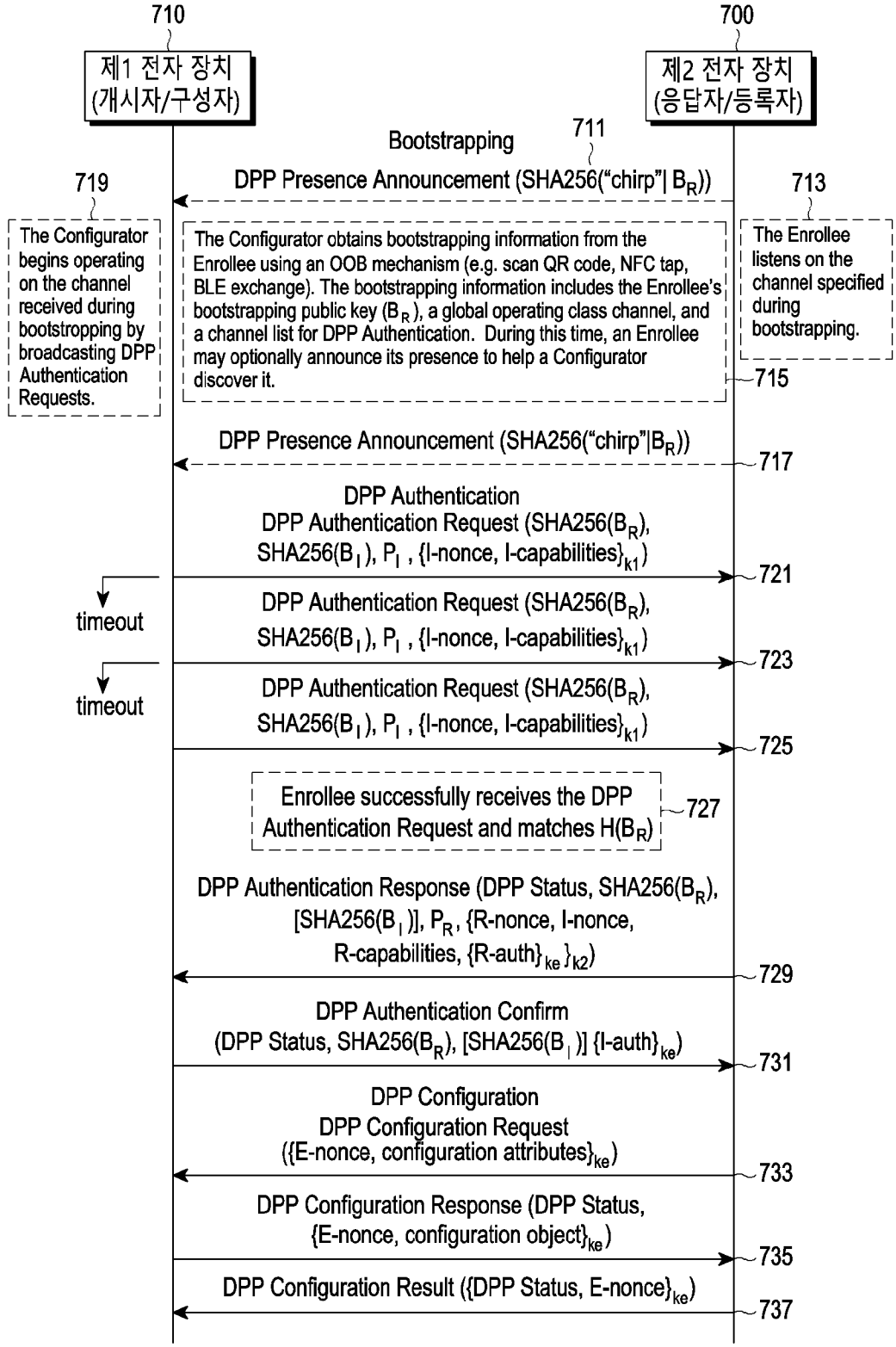
[도5]


520
제2 전자 장치
(클라이언트 등록자)
550
510
제5 전자 장치
(클라이언트 등록자)
540
530
제4 전자 장치
(클라이언트 등록자)
제1 전자 장치
(구성자)
제3 전자 장치
(클라이언트 등록자)

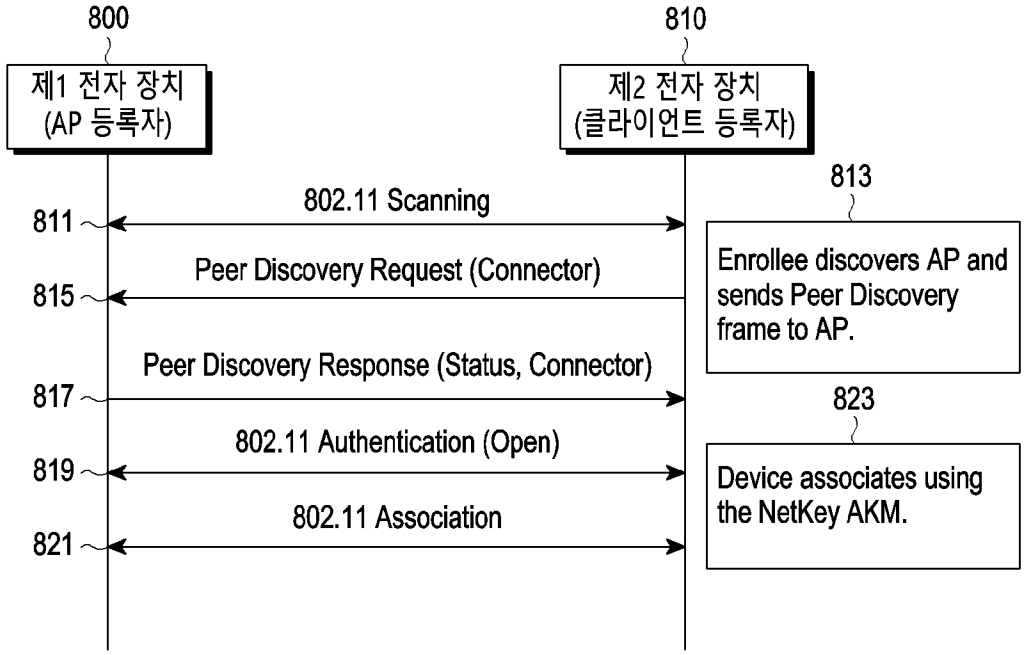
[도6]


제2 전자 장치
(AP)
660
630
제6 전자 장치
(등록자)
620
610
제3 전자 장치
(등록자)
640
650
제4 전자 장치
(등록자)
제1 전자 장치
(구성자)
제5 전자 장치
(등록자)

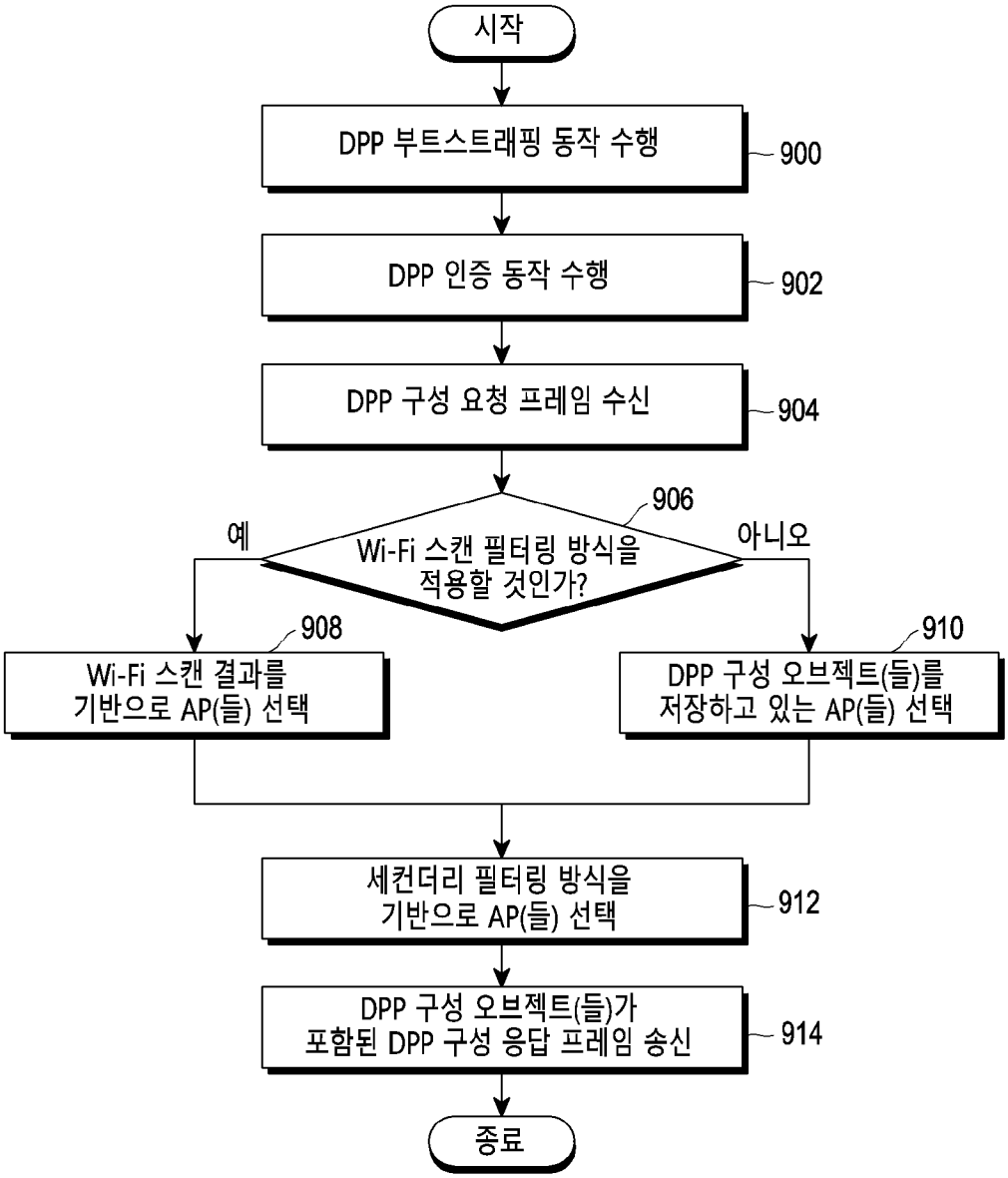
[도7]


710
제1 전자 장치
(개시자/구성자)
700
제2 전자 장치
(응답자/등록자)
Bootstrapping
711
DPP Presence Announcement (SHA256("chirp"| B_R))
719
713
The Configurator begins operating on the channel received during bootstropping by broadcasting DPP Authentication Requests.
The Configurator obtains bootstrapping information from the Enrollee using an OOB mechanism (e.g. scan QR code, NFC tap, BLE exchange). The bootstrapping information includes the Enrollee's bootstrapping public key (B_R), a global operating class channel, and a channel list for DPP Authentication. During this time, an Enrollee may optionally announce its presence to help a Configurator discover it.
The Enrollee listens on the channel specified during bootstrapping.
715
DPP Presence Announcement (SHA256("chirp"|B_R))
717
DPP Authentication
DPP Authentication Request (SHA256(B_R), SHA256(B_I), P_I , {I-nonce, I-capabilities}$_{k1}$)
721
timeout
DPP Authentication Request (SHA256(B_R), SHA256(B_I), P_I , {I-nonce, I-capabilities}$_{k1}$)
723
timeout
DPP Authentication Request (SHA256(B_R), SHA256(B_I), P_I , {I-nonce, I-capabilities}$_{k1}$)
725
Enrollee successfully receives the DPP Authentication Request and matches H(B_R)
727
DPP Authentication Response (DPP Status, SHA256(B_R), [SHA256(B_I)], P_R, {R-nonce, I-nonce, R-capabilities, {R-auth}$_{ke}$}$_{k2}$)
729
DPP Authentication Confirm
(DPP Status, SHA256(B_R), [SHA256(B_I)] {I-auth}$_{ke}$)
731
DPP Configuration
DPP Configuration Request
({E-nonce, configuration attributes}$_{ke}$)
733
DPP Configuration Response (DPP Status, {E-nonce, configuration object}$_{ke}$)
735
DPP Configuration Result ({DPP Status, E-nonce}$_{ke}$)
737

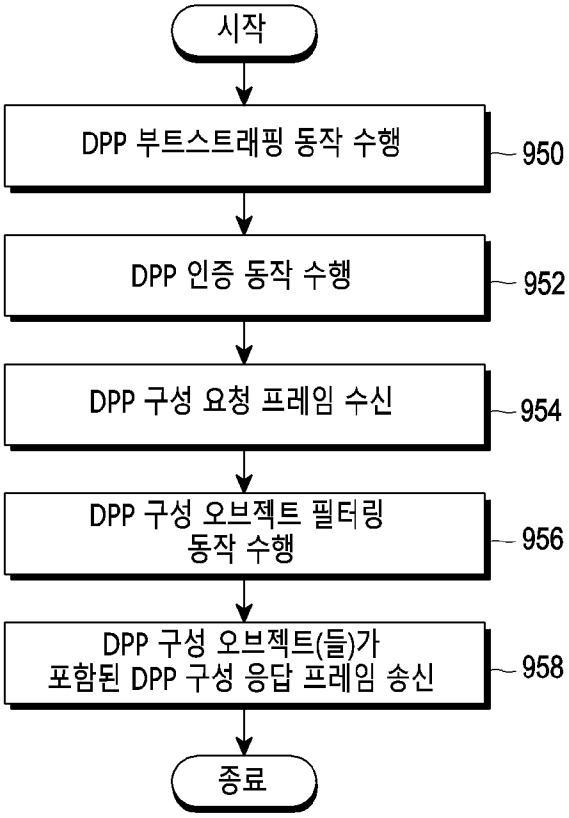
[도8]


800
제1 전자 장치
(AP 등록자)
810
제2 전자 장치
(클라이언트 등록자)
813
802.11 Scanning
811
Peer Discovery Request (Connector)
815
Enrollee discovers AP and sends Peer Discovery frame to AP.
Peer Discovery Response (Status, Connector)
817
823
802.11 Authentication (Open)
819
Device associates using the NetKey AKM.
802.11 Association
821

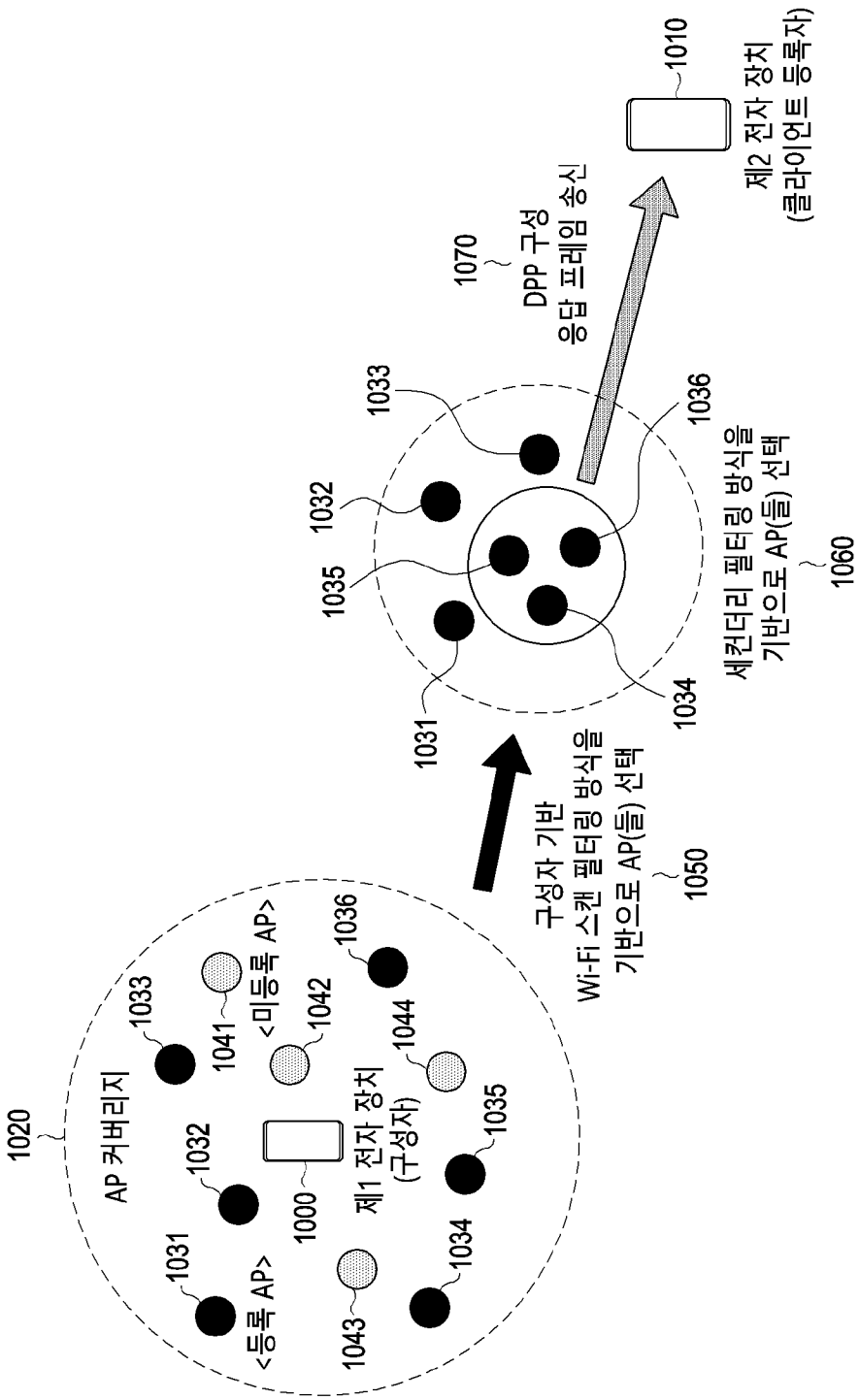
[도9a]


시작
DPP 부트스트래핑 동작 수행
900
DPP 인증 동작 수행
902
DPP 구성 요청 프레임 수신
904
906
Wi-Fi 스캔 필터링 방식을 적용할 것인가?
예
아니오
908
Wi-Fi 스캔 결과를 기반으로 AP(들) 선택
910
DPP 구성 오브젝트(들)를 저장하고 있는 AP(들) 선택
세컨더리 필터링 방식을 기반으로 AP(들) 선택
912
DPP 구성 오브젝트(들)가 포함된 DPP 구성 응답 프레임 송신
914
종료

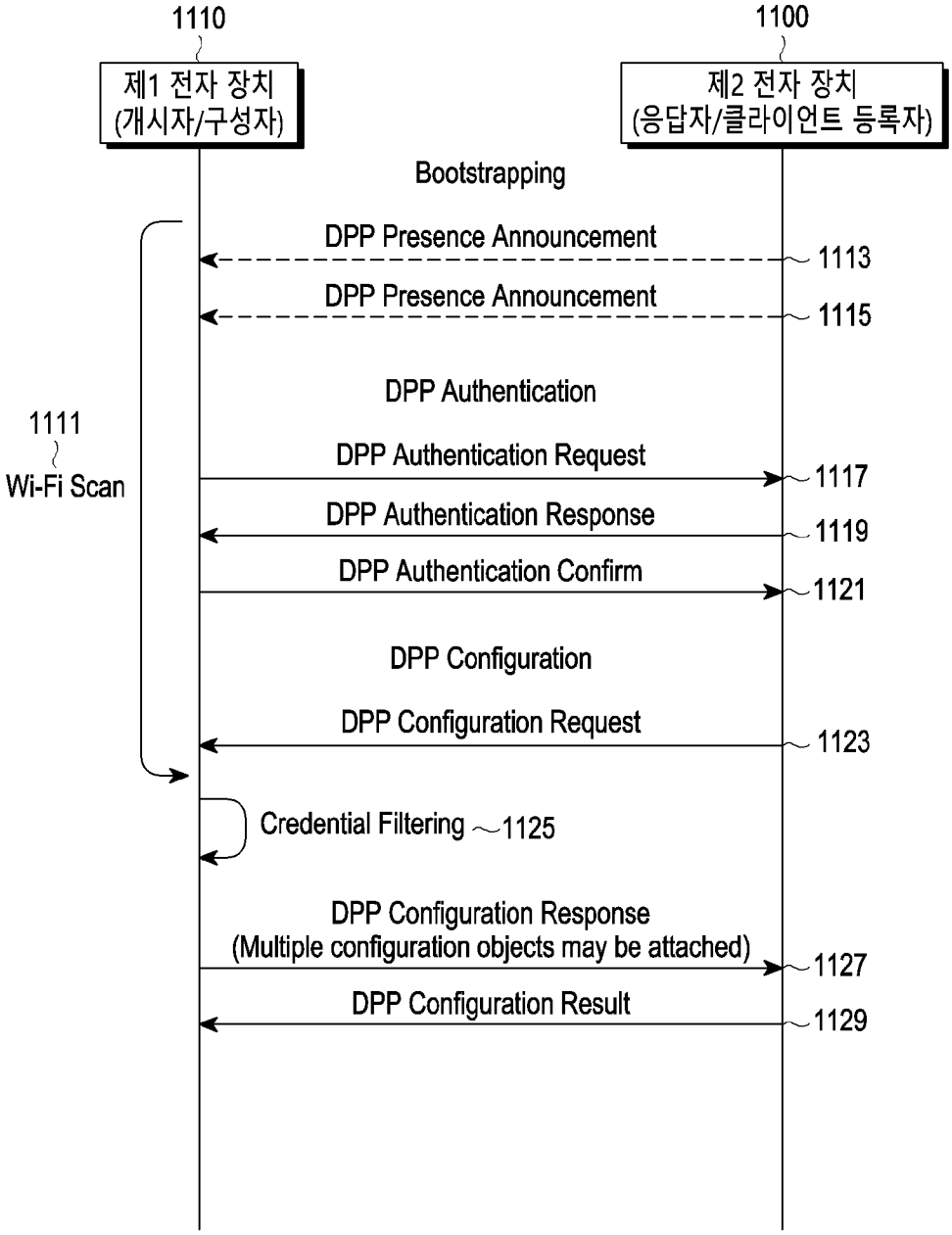
[도9b]


시작
DPP 부트스트래핑 동작 수행
950
DPP 인증 동작 수행
952
DPP 구성 요청 프레임 수신
954
DPP 구성 오브젝트 필터링
동작 수행
956
DPP 구성 오브젝트(들)가
포함된 DPP 구성 응답 프레임 송신
958
종료

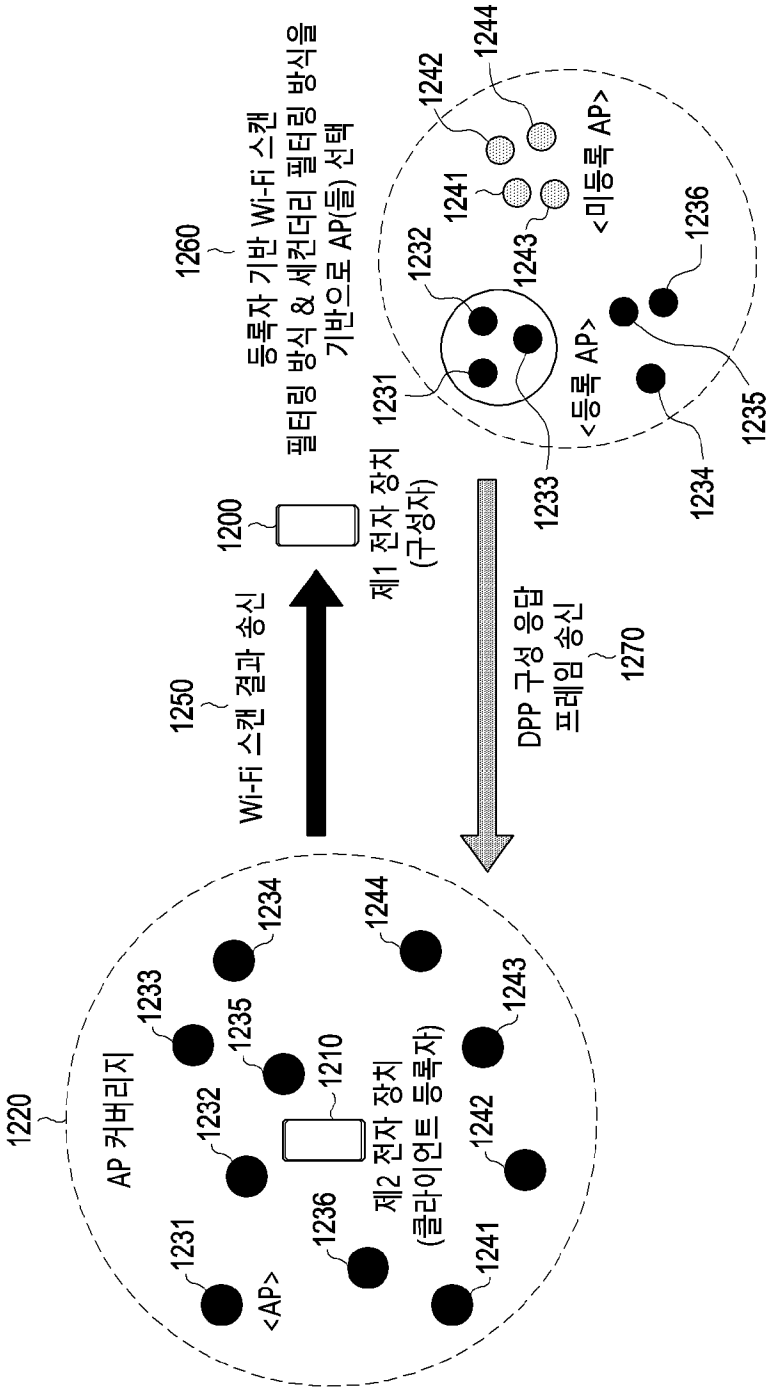
[도10]


1020
AP 커버리지
1033
1041
<미등록 AP>
1042
1036
1044
1032
1035
1031
<등록 AP>
1000
제1 전자 장치
(구성자)
1043
1034
구성자 기반
Wi-Fi 스캔 필터링 방식을
기반으로 AP(들) 선택
1050
1033
1032
1035
1031
1036
1034
세컨더리 필터링 방식을
기반으로 AP(들) 선택
1060
1070
DPP 구성
응답 프레임 송신
1010
제2 전자 장치
(클라이언트 등록자)

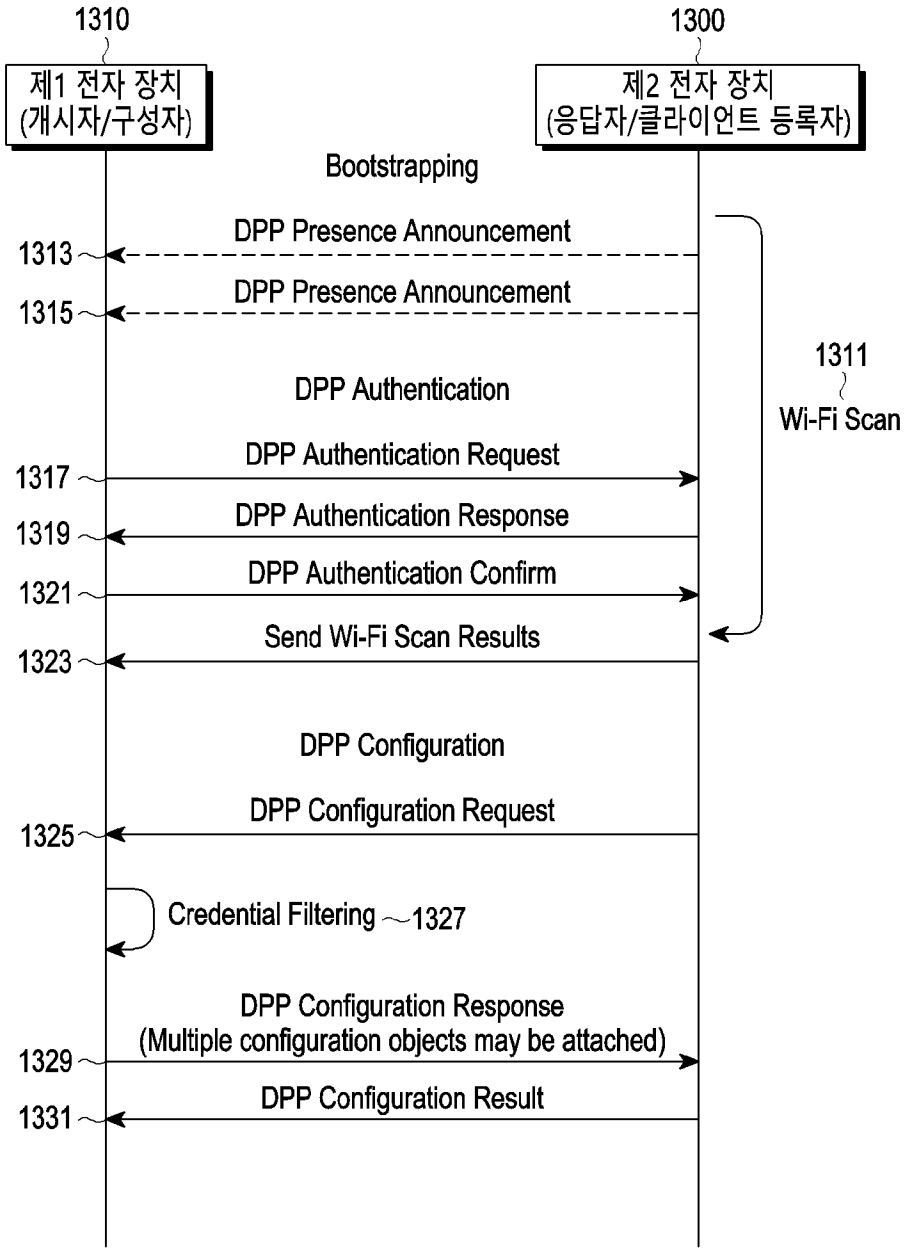
[도11]


1110
제1 전자 장치
(개시자/구성자)
1100
제2 전자 장치
(응답자/클라이언트 등록자)
Bootstrapping
DPP Presence Announcement
1113
DPP Presence Announcement
1115
DPP Authentication
1111
Wi-Fi Scan
DPP Authentication Request
1117
DPP Authentication Response
1119
DPP Authentication Confirm
1121
DPP Configuration
DPP Configuration Request
1123
Credential Filtering
1125
DPP Configuration Response
(Multiple configuration objects may be attached)
1127
DPP Configuration Result
1129

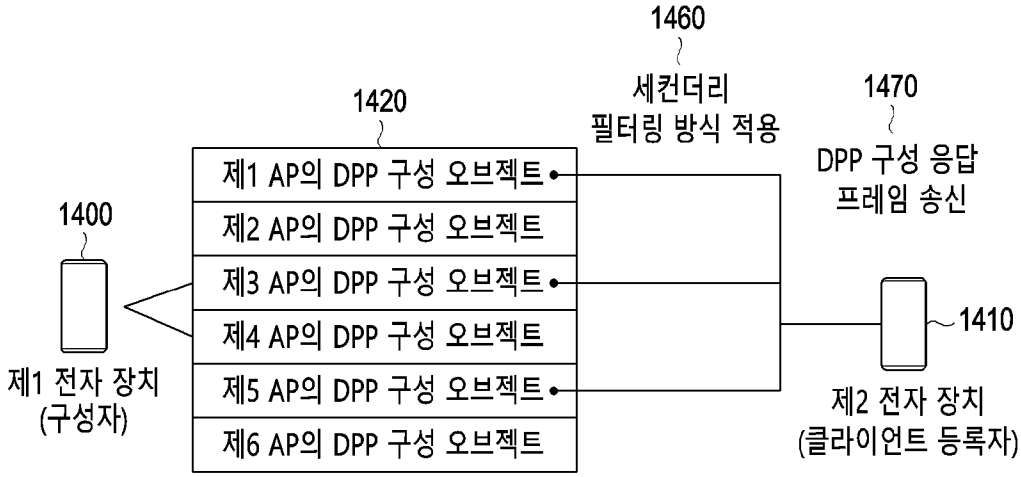
[도12]


1260
등록자 기반 Wi-Fi 스캔
필터링 방식 & 세컨더리 필터링 방식을
기반으로 AP(들) 선택
1200
제1 전자 장치
(구성자)
1250
Wi-Fi 스캔 결과 송신
1270
DPP 구성 응답
프레임 송신
1220
AP 커버리지
제2 전자 장치
(클라이언트 등록자)
1210
<AP>
<등록 AP>
<미등록 AP>
1231
1232
1233
1234
1235
1236
1241
1242
1243
1244

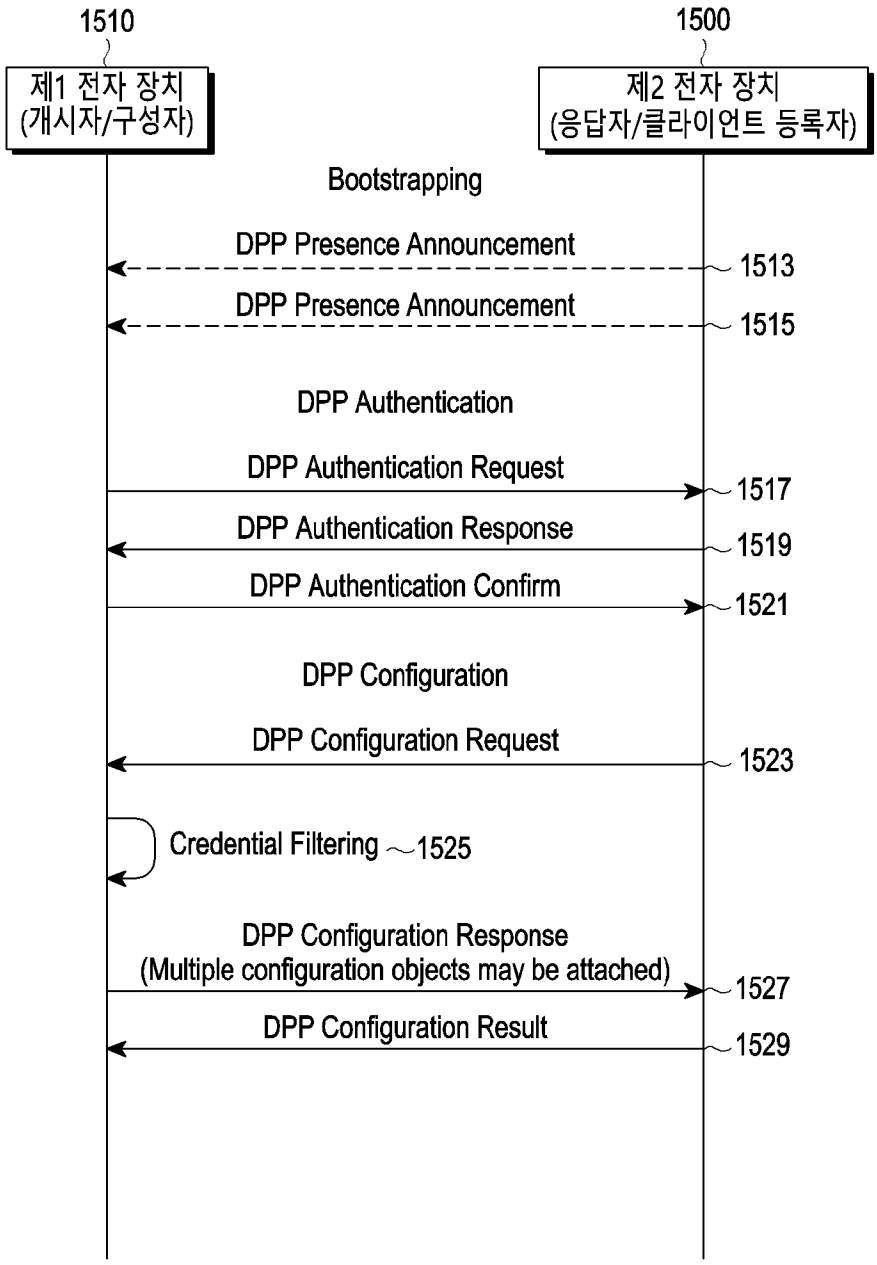
[도13]


1310
제1 전자 장치
(개시자/구성자)
1300
제2 전자 장치
(응답자/클라이언트 등록자)
Bootstrapping
DPP Presence Announcement
1313
DPP Presence Announcement
1315
1311
Wi-Fi Scan
DPP Authentication
DPP Authentication Request
1317
DPP Authentication Response
1319
DPP Authentication Confirm
1321
Send Wi-Fi Scan Results
1323
DPP Configuration
DPP Configuration Request
1325
Credential Filtering
1327
DPP Configuration Response
(Multiple configuration objects may be attached)
1329
DPP Configuration Result
1331

[도14]


1460
세컨더리
필터링 방식 적용
1420
1470
DPP 구성 응답
프레임 송신
제1 AP의 DPP 구성 오브젝트
제2 AP의 DPP 구성 오브젝트
제3 AP의 DPP 구성 오브젝트
제4 AP의 DPP 구성 오브젝트
제5 AP의 DPP 구성 오브젝트
제6 AP의 DPP 구성 오브젝트
1400
1410
제1 전자 장치
(구성자)
제2 전자 장치
(클라이언트 등록자)

[도15]


1510
제1 전자 장치
(개시자/구성자)
1500
제2 전자 장치
(응답자/클라이언트 등록자)
Bootstrapping
DPP Presence Announcement
1513
DPP Presence Announcement
1515
DPP Authentication
DPP Authentication Request
1517
DPP Authentication Response
1519
DPP Authentication Confirm
1521
DPP Configuration
DPP Configuration Request
1523
Credential Filtering
1525
DPP Configuration Response
(Multiple configuration objects may be attached)
1527
DPP Configuration Result
1529

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2022/001609

A. CLASSIFICATION OF SUBJECT MATTER

H04W 4/50(2018.01)i; **H04W 48/16**(2009.01)i; **H04W 48/14**(2009.01)i; **H04W 12/06**(2009.01)i; **H04W 84/12**(2009.01)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)

H04W 4/50(2018.01); H04L 12/24(2006.01); H04W 12/04(2009.01); H04W 12/06(2009.01); H04W 24/02(2009.01); H04W 36/08(2009.01); H04W 36/34(2009.01); H04W 76/02(2009.01); H04W 8/22(2009.01)

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: network configuration information request, filtering manner, select, network configuration information, network configuration information response

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2019-0306710 A1 (QUALCOMM INCORPORATED) 03 October 2019 (2019-10-03) See paragraphs [0056]-[0065]; and figure 2.	1-3,6-10,13-15
A		4-5,11-12
Y	US 2016-0165645 A1 (D&M HOLDINGS INC.) 09 June 2016 (2016-06-09) See paragraphs [0023]-[0059]; and figures 1-7C.	1-3,6-10,13-15
A	US 2019-0123964 A1 (BLACKBERRY LIMITED) 25 April 2019 (2019-04-25) See paragraphs [0035]-[0059]; and figures 1-3.	1-15
A	WO 2020-092971 A1 (GOOGLE LLC) 07 May 2020 (2020-05-07) See paragraphs [0034]-[0048]; and figures 3-5.	1-15
A	WO 2019-177231 A1 (LG ELECTRONICS INC.) 19 September 2019 (2019-09-19) See paragraphs [0150]-[0179]; and figure 10.	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
"D" document cited by the applicant in the international application
"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
04 May 2022	**04 May 2022**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2022/001609

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019-0306710 A1	03 October 2019	CN 111903181 A	06 November 2020
		EP 3777470 A1	17 February 2021
		TW 201943313 A	01 November 2019
		WO 2019-190867 A1	03 October 2019
US 2016-0165645 A1	09 June 2016	CN 105409261 A	16 March 2016
		EP 3025535 A1	01 June 2016
		EP 3025535 B1	15 May 2019
		JP 2016-533078 A	20 October 2016
		WO 2015-011520 A1	29 January 2015
US 2019-0123964 A1	25 April 2019	EP 3616426 A1	04 March 2020
		US 10171304 B2	01 January 2019
		US 2018-0316562 A1	01 November 2018
		WO 2018-197194 A1	01 November 2018
WO 2020-092971 A1	07 May 2020	CN 112673592 A	16 April 2021
		EP 3821568 A1	19 May 2021
		US 2021-0400502 A1	23 December 2021
WO 2019-177231 A1	19 September 2019	None	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2022/001609

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 4/50(2018.01)i; **H04W 48/16**(2009.01)i; **H04W 48/14**(2009.01)i; **H04W 12/06**(2009.01)i; **H04W 84/12**(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04W 4/50(2018.01); H04L 12/24(2006.01); H04W 12/04(2009.01); H04W 12/06(2009.01); H04W 24/02(2009.01); H04W 36/08(2009.01); H04W 36/34(2009.01); H04W 76/02(2009.01); H04W 8/22(2009.01)

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: network configuration information request, filtering manner, select, network configuration information, network configuration information response

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2019-0306710 A1 (QUALCOMM INCORPORATED) 2019.10.03 단락 [0056]-[0065]; 및 도면 2	1-3,6-10,13-15
A		4-5,11-12
Y	US 2016-0165645 A1 (D&M HOLDINGS INC.) 2016.06.09 단락 [0023]-[0059]; 및 도면 1-7C	1-3,6-10,13-15
A	US 2019-0123964 A1 (BLACKBERRY LIMITED) 2019.04.25 단락 [0035]-[0059]; 및 도면 1-3	1-15
A	WO 2020-092971 A1 (GOOGLE LLC) 2020.05.07 단락 [0034]-[0048]; 및 도면 3-5	1-15
A	WO 2019-177231 A1 (LG ELECTRONICS INC.) 2019.09.19 단락 [0150]-[0179]; 및 도면 10	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 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
2022년05월04일(04.05.2022)	**2022년05월04일(04.05.2022)**

ISA/KR의 명칭 및 우편주소

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

팩스 번호 **+82-42-481-8578**

심사관

양정록

전화번호 **+82-42-481-5709**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2022/001609

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2019-0306710 A1	2019/10/03	CN 111903181 A	2020/11/06
		EP 3777470 A1	2021/02/17
		TW 201943313 A	2019/11/01
		WO 2019-190867 A1	2019/10/03
US 2016-0165645 A1	2016/06/09	CN 105409261 A	2016/03/16
		EP 3025535 A1	2016/06/01
		EP 3025535 B1	2019/05/15
		JP 2016-533078 A	2016/10/20
		WO 2015-011520 A1	2015/01/29
US 2019-0123964 A1	2019/04/25	EP 3616426 A1	2020/03/04
		US 10171304 B2	2019/01/01
		US 2018-0316562 A1	2018/11/01
		WO 2018-197194 A1	2018/11/01
WO 2020-092971 A1	2020/05/07	CN 112673592 A	2021/04/16
		EP 3821568 A1	2021/05/19
		US 2021-0400502 A1	2021/12/23
WO 2019-177231 A1	2019/09/19	없음	