(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0121546
(43) 공개일자 2016년10월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *G06F 21/34* (2013.01)
G06F 21/41 (2013.01) *H04L 29/06* (2006.01)
H04L 9/14 (2006.01)
(52) CPC특허분류
H04L 9/30 (2013.01)
G06F 21/34 (2013.01)
(21) 출원번호 10-2016-7024475
(22) 출원일자(국제) 2015년02월09일
심사청구일자 없음
(85) 번역문제출일자 2016년09월05일
(86) 국제출원번호 PCT/US2015/014992
(87) 국제공개번호 WO 2015/120373
국제공개일자 2015년08월13일
(30) 우선권주장
61/937,891 2014년02월10일 미국(US)
(뒷면에 계속)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
베노이트, 오리비어 진
미국 92121-1714 캘리포니아 샌 디에고 모어하우스 드라이브 5775
마리넨, 주니 카레비
미국 92121-1714 캘리포니아 샌 디에고 모어하우스 드라이브 5775
티나코른스리서파프, 피라폴
미국 92121-1714 캘리포니아 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

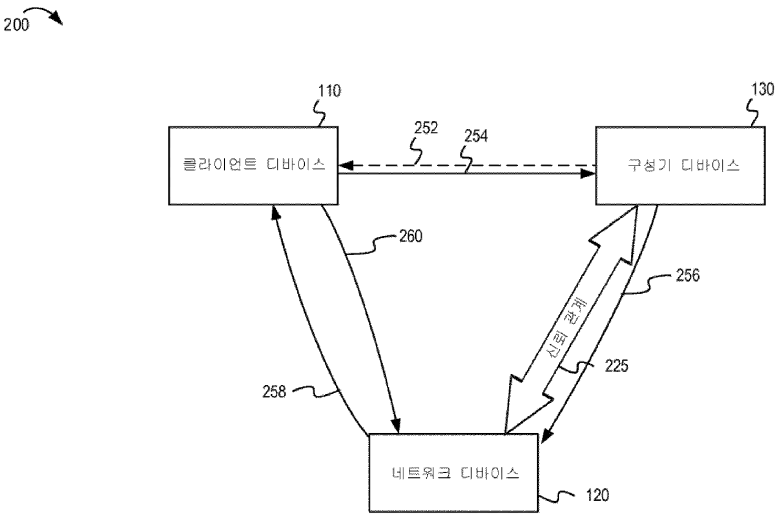
전체 청구항 수 : 총 92 항

(54) 발명의 명칭 **네트워크에서의 지원된 디바이스 프로비져닝**

(57) 요 약

네트워크 디바이스로의 클라이언트 디바이스의 디바이스 프로비져닝(예를 들어, 등록, 구성 및/또는 인증)은 구성기 디바이스를 사용하여 지원될 수 있다. 구성기 디바이스는 클라이언트 디바이스와 관련된 클라이언트 공개키를 획득하고 클라이언트 공개 디바이스를 네트워크 디바이스레 전송할 수 있다. 네트워크 디바이스는, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증 프로세스에서 클라이언트 공개키를 사용할 수 있다. 인증 프로세스 이후, 클라이언트 디바이스는, 다른 네트워크 리소스들에 액세스를 획득하기 위해, 네트워크 디바이스에 사용하기 위해 구성될 수 있다. 이러한 방식으로, 네트워크 디바이스로의 액세스를 획득하기 위한 허가가, 종종 사용자가 코드들 또는 패스워드들을 입력할 필요 없이, 사용자에게 투명할 수 있다.

대 표 도



(52) CPC특허분류
G06F 21/41 (2013.01)
H04L 63/0823 (2013.01)
H04L 63/0853 (2013.01)
H04L 63/0869 (2013.01)
H04L 63/18 (2013.01)
H04L 9/14 (2013.01)
H04L 2209/24 (2013.01)

(30) 우선권주장
61/996,812 2014년05월14일 미국(US)
14/616,551 2015년02월06일 미국(US)

명 세 서

청구범위

청구항 1

클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법으로서,

상기 네트워크의 네트워크 디바이스와 신뢰 관계를 구축하는 단계;

상기 클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차 이전에, 상기 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하는 단계; 및

상기 등록 절차를 가능하게 하기 위해 상기 클라이언트 공개 키를, 상기 신뢰 관계에 따라 상기 구성기 디바이스로부터 상기 네트워크 디바이스로 전송하는 단계를 포함하며,

상기 등록 절차는, 상기 클라이언트 공개 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 2

제 1 항에 있어서,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 상기 구성기 디바이스 또는 상기 네트워크 디바이스로부터 상기 클라이언트 디바이스로 전송하는 단계를 더 포함하며,

상기 제 1 인증은 상기 네트워크 공개 키에 적어도 부분적으로 추가로 기초하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 3

제 1 항에 있어서,

상기 신뢰 관계를 구축하는 단계는,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 단계;

구성기 공개 키 －상기 구성기 공개 키는 구성기 개인 키에 대응함－를 상기 네트워크 디바이스에 전송하는 단계; 및

상기 네트워크 공개 키 및 상기 구성기 개인 키에 적어도 부분적으로 기초하여 상기 신뢰 관계와 관련된 신뢰 관계 키를 결정하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 4

제 3 항에 있어서,

상기 구성기 디바이스로부터 상기 네트워크 디바이스로 상기 클라이언트 공개 키를 전송하기 전에, 상기 신뢰 관계 키로 상기 클라이언트 공개 키를 암호화하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 5

제 3 항에 있어서,

상기 네트워크 디바이스와 관련된 상기 네트워크 공개 키를 결정하는 단계는, 상기 네트워크 디바이스와의 보안 연결을 통해 상기 네트워크 공개 키를 수신하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 6

제 3 항에 있어서,

상기 네트워크 디바이스와 관련된 상기 네트워크 공개 키를 결정하는 단계는, 상기 클라이언트 디바이스가 상기 네트워크 디바이스와 구축할 연결과 상이한 상기 네트워크 디바이스와의 대역 외 연결을 통해 상기 네트워크 공개 키를 결정하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 7

제 3 항에 있어서,

상기 신뢰 관계를 구축하는 단계는, 상기 네트워크 디바이스와 관련된 상기 네트워크 공개 키를 결정하기 전에, 상기 네트워크 디바이스로부터 구성기 지원 서비스 통지를 수신하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 8

제 3 항에 있어서,

상기 네트워크 디바이스와 관련된 상기 네트워크 공개 키를 결정하는 단계는,

카메라, 마이크로폰, 광 검출기, 센서 및 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 사용하여 상기 네트워크 공개 키를 검출하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 9

제 8 항에 있어서,

상기 카메라를 사용하여 상기 네트워크 공개 키를 검출하는 단계는, 상기 네트워크 디바이스와 관련된 이미지를 검출하기 위해 상기 카메라를 사용하는 단계를 포함하며,

상기 이미지의 적어도 일부는 네트워크 공개 키를 포함하는,

클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 10

제 1 항에 있어서,

상기 클라이언트 디바이스와 관련된 상기 클라이언트 공개 키를 결정하는 단계는, 카메라, 마이크로폰, 광 검출기, 센서 및 상기 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 사용하여 상기 클라이언트 공개 키를 검출하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 11

제 10 항에 있어서,

상기 카메라를 사용하여 상기 클라이언트 공개 키를 검출하는 단계는, 상기 클라이언트 디바이스와 관련된 이미지를 검출하기 위해 상기 카메라를 사용하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 12

제 1 항에 있어서,

상기 클라이언트 디바이스와 관련된 상기 클라이언트 공개 키를 전송하는 단계는,

요청 메시지를 상기 네트워크 디바이스에 전송하는 단계;

상기 네트워크 디바이스로부터 넌스를 수신하는 단계; 및

등록 메시지를 상기 네트워크 디바이스에 전송하는 단계를 포함하며,

상기 등록 메시지는, 상기 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 상기 클라이언트 공개 키를 포함하며, 상기 구성기 서명은, 상기 구성기 디바이스가 상기 등록 메시지를 전송하도록 인가되었다는 제 2 인증을 상기 네트워크 디바이스에 제공하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 13

제 12 항에 있어서,

상기 구성기 서명은 상기 넌스 및 구성기 개인 키로부터 도출되거나 상기 신뢰 관계와 관련된 신뢰 관계 키에 적어도 부분적으로 기초하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 14

제 12 항에 있어서,

상기 네트워크 디바이스로부터 등록 키를 수신하는 단계; 및

상기 등록 키를 상기 클라이언트 디바이스에 전송하는 단계를 더 포함하며,

상기 등록 키는 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 제 1 인증을 위해 상기 클라이언트 공개 키와 함께 사용되는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 15

제 1 항에 있어서,

상기 신뢰 관계를 구축한 후, 구성 데이터를 상기 구성기 디바이스로부터 상기 네트워크 디바이스로 전송하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 16

제 1 항에 있어서,

상기 네트워크 디바이스와 관련하여 상기 클라이언트 디바이스를 돕기 위해 구성 데이터를 상기 구성기 디바이스로부터 상기 클라이언트 디바이스로 전송하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 17

제 16 항에 있어서,

상기 구성 데이터를 전송하는 단계는, 상기 클라이언트 디바이스에 의해 액세스 가능한 디폴트 채널을 통해 제 1 메시지를 송신하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 18

제 17 항에 있어서,

상기 제 1 메시지는, 상기 네트워크 디바이스와 관련된 네트워크 공개 키나 상기 클라이언트 공개 키에 적어도 부분적으로 기초한 아이덴티티 정보를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 19

제 1 항에 있어서,

상기 클라이언트 디바이스는 제 1 클라이언트 디바이스이고, 상기 네트워크 디바이스는 제 2 클라이언트 디바이스이고, 상기 구성기 디바이스는 액세스 포인트인, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 20

제 1 항에 있어서,

상기 네트워크 디바이스는 상기 네트워크의 액세스 포인트이고, 상기 구성기 디바이스는 상기 액세스 포인트와 관련되는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 21

제 1 항에 있어서,

네트워크 디바이스들의 리스트 및 상기 네트워크 디바이스들의 리스트 각각에 대한 대응하는 네트워크 공개 키를 유지하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 구성기 디바이스에 의해 수행되는 방법.

청구항 22

클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법으로서,

상기 네트워크 디바이스에서, 구성기 디바이스와 신뢰 관계를 구축하는 단계;

상기 클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차 이전에, 상기 신뢰 관계에 따라 상기 구성기 디바이스로부터, 상기 클라이언트 디바이스와 관련된 클라이언트 공개 키를 수신하는 단계; 및

상기 등록 절차를 위해 상기 클라이언트 공개 키를 사용하는 단계를 포함하며,

상기 등록 절차는, 상기 클라이언트 공개 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 23

제 22 항에 있어서,

상기 신뢰 관계를 구축하는 단계는, 상기 네트워크 디바이스와 관련된 네트워크 공개 키를 상기 구성기 디바이스 또는 상기 클라이언트 디바이스에 제공하는 단계를 포함하며, 상기 네트워크 공개 키는 대응하는 네트워크 개인 키를 갖는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 24

제 23 항에 있어서,

상기 네트워크 디바이스와 관련된 상기 네트워크 공개 키를 제공하는 단계는, 상기 네트워크 디바이스의 디스플레이 또는 단거리 라디오 주파수 인터페이스를 이용하여 상기 네트워크 공개 키를 제공하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 25

제 22 항에 있어서,

디폴트 채널을 통해 제 1 메시지를 송신하는 단계를 더 포함하며,

상기 제 1 메시지는 상기 네트워크 디바이스와 관련된 네트워크 공개 키나 상기 클라이언트 공개 키로부터 도출되는 정보를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 26

제 22 항에 있어서,

상기 클라이언트 디바이스에 사용할 공유 키를 결정하는 단계를 더 포함하며, 상기 공유 키는 상기 클라이언트 공개 키 및 네트워크 개인 키에 적어도 부분적으로 기초하는,

클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 27

제 22 항에 있어서,

상기 구성기 디바이스로부터 구성기 공개 키를 수신하는 단계; 및

네트워크 개인 키 및 상기 구성기 공개 키에 적어도 부분적으로 기초하여 상기 신뢰 관계와 관련된 신뢰 관계 키를 결정하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 28

제 27 항에 있어서,

상기 클라이언트 공개 키를 수신하는 단계는, 상기 신뢰 관계 키로 암호화된 상기 클라이언트 공개 키를 수신하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 29

제 22 항에 있어서,

상기 신뢰 관계를 구축하는 단계는,

상기 네트워크 디바이스로부터 구성기 지원 서비스 통지를 송신하는 단계를 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 30

제 22 항에 있어서,

상기 클라이언트 디바이스와 관련된 상기 클라이언트 공개 키를 수신하는 단계는,

상기 구성기 디바이스로부터 요청 메시지를 수신하는 단계;

상기 구성기 디바이스에 넌스를 전송하는 단계; 및

상기 구성기 디바이스로부터 등록 메시지를 수신하는 단계를 포함하며,

상기 등록 메시지는 상기 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 상기 클라이언트 공개 키를 포함하며,

상기 구성기 서명은, 상기 구성기 디바이스가 상기 등록 메시지를 전송하도록 인가되었다는 제 2 인증을 상기 네트워크 디바이스에 제공하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 31

제 30 항에 있어서,

구성기 공개 키 및 상기 구성기 서명에 적어도 부분적으로 기초하여 상기 등록 메시지를 인증하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 32

제 30 항에 있어서,

상기 네트워크 디바이스로부터 등록 키를 전송하는 단계; 및

상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 상기 제 1 인증을 위해 상기 클라이언트 공개 키와 함께 상기 등록 키를 사용하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 33

제 22 항에 있어서,

상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 상기 제 1 인증을 위해 상기 클라이언트 공개 키를 사용한 후, 상기 네트워크 디바이스로부터 상기 클라이언트 디바이스로 구성 데이터를 전송하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 34

제 22 항에 있어서,

상기 네트워크 디바이스에서, 클라이언트 디바이스들의 리스트 및 상기 클라이언트 디바이스들의 리스트 각각에 대한 대응하는 클라이언트 공개 키를 유지하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 35

제 34 항에 있어서,

상기 클라이언트 디바이스들의 리스트에 대한 변경을 결정 시, 상기 변경의 통보를 다른 네트워크 디바이스로 전송하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 36

제 22 항에 있어서,

상기 네트워크 디바이스에서, 구성기 디바이스들의 리스트 및 상기 구성기 디바이스들의 리스트 각각에 대한 대응하는 신뢰 관계 키를 유지하는 단계를 더 포함하는, 클라이언트 디바이스를 네트워크에 등록하기 위해 네트워크 디바이스에 의해 수행되는 방법.

청구항 37

네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법으로서,

상기 클라이언트 디바이스와 네트워크 디바이스 사이의 등록 절차 이전에, 상기 클라이언트 디바이스와 관련된 클라이언트 공개 키를, 상기 네트워크의 상기 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 제공하는 단계;

상기 네트워크 디바이스와 관련된 네트워크 공개 키 및 제 1 넌스를 상기 구성기 디바이스로부터 수신하는 단계;

제 2 넌스를 생성하는 단계;

상기 제 1 넌스, 상기 제 2 넌스, 상기 네트워크 공개 키, 및 상기 클라이언트 디바이스와 관련된 클라이언트 개인 키에 적어도 부분적으로 기초하여 공유 키를 결정하는 단계 －상기 클라이언트 개인 키는 상기 클라이언트 공개 키에 대응함－; 및

상기 등록 절차를 위해 상기 공유 키를 사용하는 단계를 포함하며,

상기 등록 절차는 상기 공유 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법.

청구항 38

제 37 항에 있어서,

상기 공유 키는 상기 네트워크 디바이스에서 대응하는 공유 키와 매칭되며,

상기 대응하는 공유 키는 상기 제 1 넌스, 상기 제 2 넌스, 네트워크 개인 키 및 상기 클라이언트 공개 키를 포함하는, 상기 네트워크 디바이스에서의 대응하는 계산에 적어도 부분적으로 기초하는, 네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법.

청구항 39

제 37 항에 있어서,

상기 제 1 인증은, 상기 공유 키로부터 도출되는 적어도 일부를 갖는 인증 응답을 전송하는 단계를 포함하며, 상기 인증 응답은 또한 상기 제 2 넌스를 포함하는, 네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법.

청구항 40

제 39 항에 있어서,

상기 인증 응답은, 상기 클라이언트 디바이스가 상기 네트워크 공개 키를 획득했다는 것을, 상기 네트워크 디바이스에게 확인해 주는, 네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법.

청구항 41

제 37 항에 있어서,

구성 데이터를 가진 제 1 메시지에 대해 디폴트 채널을 모니터링하는 단계; 및

상기 디폴트 채널 상에서 상기 제 1 메시지를 수신하는 단계를 더 포함하며,

상기 구성 데이터는 상기 네트워크 디바이스와 관련시키기 위해 상기 클라이언트 디바이스에 대한 정보를 포함하는, 네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법.

청구항 42

제 41 항에 있어서,

상기 제 1 메시지는 상기 클라이언트 공개 키나 상기 네트워크 공개 키에 적어도 부분적으로 기초하는 아이덴티티 정보를 포함하는, 네트워크에 등록하기 위해 클라이언트 디바이스에 의해 수행되는 방법.

청구항 43

구성기 디바이스에 의해 수행되는 방법으로서,

클라이언트 디바이스 또는 네트워크 디바이스 중 하나와 관련된 제 1 공개 키를 상기 구성기 디바이스에서 수신하는 단계;

상기 구성기 디바이스에서, 상기 제 1 공개 키 및 구성기 개인 키에 기초하여 제 1 증명서를 생성하는 단계; 및

상기 클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차를 가능하게 하기 위해 상기 클라이언트 디바이스 또는 상기 네트워크 디바이스 중 하나에 상기 제 1 증명서를 전송하는 단계를 포함하며,

상기 등록 절차는 상기 제 1 증명서에 적어도 부분적으로 기초한, 상기 클라이언트 디바이스와 상기 네트워크 디바이스 사이의 적어도 인증 프로세스를 포함하는,

구성기 디바이스에 의해 수행되는 방법.

청구항 44

제 43 항에 있어서,

상기 클라이언트 디바이스 또는 상기 네트워크 디바이스 중 나머지 하나와 관련된 제 2 공개 키를 상기 구성기 디바이스에서 수신하는 단계;

상기 구성기 디바이스에서, 상기 제 2 공개 키 및 상기 구성기 개인 키에 기초하여 제 2 증명서를 생성하는 단계; 및

상기 클라이언트 디바이스와 상기 네트워크 디바이스 사이의 인증 프로세스를 가능하게 하기 위해 상기 클라이언트 디바이스 또는 상기 네트워크 디바이스 중 나머지 하나에 상기 제 2 증명서를 전송하는 단계를 더 포함하는, 구성기 디바이스에 의해 수행되는 방법.

청구항 45

제 43 항에 있어서,

상기 제 1 증명서는 상기 클라이언트 디바이스 또는 상기 네트워크 디바이스 중 하나의 아이덴티티를 검증하고, 상기 인증 프로세스는 상기 제 1 증명서로부터 적어도 부분적으로 도출된 공유 키에 기초하는, 구성기 디바이스에 의해 수행되는 방법.

청구항 46

구성기 디바이스로서,

프로세서; 및

명령들을 저장하기 위한 메모리를 포함하며,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

상기 구성기 디바이스에서, 네트워크 디바이스와 신뢰 관계를 구축하게 하고;

클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차 이전에, 상기 구성기 디바이스에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하게 하고; 그리고

상기 등록 절차를 가능하게 하기 위해 상기 클라이언트 공개 키를, 상기 신뢰 관계에 따라 상기 구성기 디바이스로부터 상기 네트워크 디바이스로 전송하게 하며,

상기 등록 절차는, 상기 클라이언트 공개 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

구성기 디바이스.

청구항 47

제 46 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 상기 구성기 디바이스 또는 상기 네트워크 디바이스로부터 상기 클라이언트 디바이스로 전송하게 하며,

상기 제 1 인증은 상기 네트워크 공개 키에 적어도 부분적으로 추가로 기초하는, 구성기 디바이스.

청구항 48

제 46 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하게 하고;

구성기 공개 키 －상기 구성기 공개 키는 구성기 개인 키에 대응함－를 상기 네트워크 디바이스에 전송하게 하고; 그리고

상기 네트워크 공개 키 및 상기 구성기 개인 키에 적어도 부분적으로 기초하여 상기 신뢰 관계와 관련된 신뢰 관계 키를 결정하게 하는, 구성기 디바이스.

청구항 49

제 48 항에 있어서,

상기 클라이언트 디바이스가 상기 네트워크 디바이스와 구축할 연결과 상이한 상기 네트워크 디바이스와의 대역 외 연결을 구축하기 위한 인터페이스를 더 포함하며,

상기 네트워크 공개 키를 결정하기 위한 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금, 상기 네트워크 디바이스와의 상기 대역 외 연결을 통해 상기 네트워크 공개 키를 결정하게 하는 명령들을 포함하는, 구성기 디바이스.

청구항 50

제 49 항에 있어서,

상기 인터페이스는, 카메라, 마이크로폰, 광 검출기, 센서 및 단거리 라디오 주파수 인터페이스로 구성된 그룹의 멤버를 포함하는, 구성기 디바이스.

청구항 51

제 46 항에 있어서,

카메라, 마이크로폰, 광 검출기, 센서 및 상기 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 포함하는 인터페이스를 포함하며,

상기 클라이언트 공개 키를 결정하기 위한 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금, 상기 인터페이스를 이용하여 상기 클라이언트 공개 키를 검출하게 하는 명령들을 포함하는, 구성기 디바이스.

청구항 52

제 46 항에 있어서,

상기 클라이언트 공개 키를 전송하기 위한 명령들은, 상기 프로세서에 의해 실행될 때 상기 구성기 디바이스로 하여금,

요청 메시지를 상기 네트워크 디바이스에 전송하게 하고;

상기 네트워크 디바이스로부터 넌스를 수신하게 하고; 그리고

등록 메시지를 상기 네트워크 디바이스에 전송하게 하는 명령들을 포함하며,

상기 등록 메시지는, 상기 제 1 넌스 및 구성기 공개키로부터 적어도 부분적으로 도출되는 구성기 서명 및 상기 클라이언트 공개 키를 포함하며, 상기 구성기 서명은, 상기 구성기 디바이스가 상기 등록 메시지를 전송하도록 인가되었다는 제 2 인증을 상기 네트워크 디바이스에 제공하는, 구성기 디바이스.

청구항 53

제 52 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때 상기 구성기 디바이스로 하여금,

상기 네트워크 디바이스로부터 등록 키를 수신하게 하고; 그리고

상기 등록 키를 상기 클라이언트 디바이스에 전송하게 하며,

상기 등록 키는 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 제 1 인증을 위해 상기 클라이언트 공개 키와 함께 사용되는, 구성기 디바이스.

청구항 54

제 46 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때 상기 구성기 디바이스로 하여금, 상기 네트워크 디바이스와 관련하여 상기 클라이언트 디바이스를 돕기 위해 구성 데이터를 상기 구성기 디바이스로부터 상기 클라이언트 디바이스로 전송하게 하는, 구성기 디바이스.

청구항 55

제 54 항에 있어서,

상기 구성 데이터를 전송하기 위한 명령들은, 상기 프로세서에 의해 실행될 때 상기 구성기 디바이스로 하여금, 상기 클라이언트 디바이스에 의해 액세스 가능한 디폴트 채널을 통해 제 1 메시지를 송신하게 하는 명령들을 포함하는, 구성기 디바이스.

청구항 56

제 55 항에 있어서,

상기 제 1 메시지는, 상기 네트워크 디바이스와 관련된 네트워크 공개 키나 상기 클라이언트 공개 키에 적어도 부분적으로 기초한 아이덴티티 정보를 포함하는, 구성기 디바이스.

청구항 57

제 46 항에 있어서,

네트워크 디바이스들의 리스트 및 상기 네트워크 디바이스들의 리스트 각각에 대한 대응하는 네트워크 공개 키를 유지하기 위한 메모리를 더 포함하는, 구성기 디바이스.

청구항 58

네트워크 디바이스로서,

프로세서; 및

명령들을 저장하기 위한 메모리를 포함하며,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 네트워크 디바이스에서, 구성기 디바이스와 신뢰 관계를 구축하게 하고;

클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차 이전에, 상기 클라이언트 디바이스와 관련된 클라이언트 공개 키를 상기 신뢰 관계에 따라 상기 구성기 디바이스로부터 수신하게 하고; 그리고

상기 등록 절차를 위해 상기 클라이언트 공개 키를 사용하게 하며,

상기 등록 절차는, 상기 클라이언트 공개 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

네트워크 디바이스.

청구항 59

제 58 항에 있어서,

상기 신뢰 관계를 구축하기 위한 명령들은, 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금, 상기 네트워크 디바이스와 관련된 네트워크 공개 키를 상기 구성기 디바이스 또는 상기 클라이언트 디바이스에 제공하게 하는 명령들을 포함하며,

상기 네트워크 공개 키는 대응하는 네트워크 개인 키를 갖는, 네트워크 디바이스.

청구항 60

제 58 항에 있어서,

네트워크 인터페이스를 더 포함하며,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금, 상기 네트워크 인터페이스를 통해, 디폴트 채널 상에서 제 1 메시지를 송신하게 하며,

상기 제 1 메시지는 상기 네트워크 디바이스와 관련된 네트워크 공개 키나 상기 클라이언트 공개 키로부터 도출되는 정보를 포함하는, 네트워크 디바이스.

청구항 61

제 58 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금, 상기 클라이언트 디바이스에 사용할 공유 키를 결정하게 하고,

상기 공유 키는 상기 클라이언트 공개 키 및 네트워크 개인 키에 적어도 부분적으로 기초하는,

네트워크 디바이스.

청구항 62

제 58 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 구성기 디바이스로부터 요청 메시지를 수신하게 하고;

상기 구성기 디바이스에 넌스를 전송하게 하고; 그리고

상기 구성기 디바이스로부터 등록 메시지를 수신하게 하며,

상기 등록 메시지는 상기 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 상기 클라이언트 공개 키를 포함하며,

상기 구성기 서명은 상기 구성기 디바이스가 상기 등록 메시지를 전송하도록 인가되었다는 제 2 인증을 상기 네트워크 디바이스에 제공하는,

네트워크 디바이스.

청구항 63

제 62 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 네트워크 디바이스로부터 등록 키를 전송하게 하고; 그리고

상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 제 1 인증을 위해 상기 클라이언트 공개 키와 함께 상기 등록 키를 사용하게 하는, 네트워크 디바이스.

청구항 64

제 58 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 제 1 인증을 위해 상기 클라이언트 공개 키를 사용한 후, 상기 네트워크 디바이스로부터 상기 클라이언트 디바이스로 구성 데이터를 전송하게 하는, 네트워크 디바이스.

청구항 65

제 58 항에 있어서,

상기 네트워크 디바이스에서, 클라이언트 디바이스들의 리스트 및 상기 클라이언트 디바이스들의 리스트 각각에 대한 대응하는 클라이언트 공개 키를 유지하기 위한 메모리를 더 포함하는, 네트워크 디바이스.

청구항 66

제 65 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금, 상기 클라이언트 디바이스들의 리스트에 대한 변경을 결정 시, 상기 변경의 통보를 다른 네트워크 디바이스로 전송하게 하는, 네트워크 디바이스.

청구항 67

제 58 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금, 상기 네트워크 디바이스에서, 구성기 디바이스들의 리스트 및 상기 구성기 디바이스들의 리스트 각각에 대한 대응하는 신뢰 관계 키를 유지하도록 메모리하게 하는, 네트워크 디바이스.

청구항 68

클라이언트 디바이스로서,

프로세서; 및

명령들을 저장하기 위한 메모리를 포함하며,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 클라이언트 디바이스로 하여금,

상기 클라이언트 디바이스와 네트워크 디바이스 사이의 등록 절차 이전에, 상기 클라이언트 디바이스와 관련된 클라이언트 공개 키를, 상기 네트워크의 상기 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 제공하게 하고;

네트워크 디바이스와 관련된 네트워크 공개 키 및 제 1 넌스를 상기 구성기 디바이스로부터 수신하게 하고;

제 2 넌스를 생성하게 하고;

상기 제 1 넌스, 상기 제 2 넌스, 상기 네트워크 공개 키, 및 상기 클라이언트 디바이스와 관련된 클라이언트 개인 키에 적어도 부분적으로 기초하여 공유 키를 결정하게 하고 －상기 클라이언트 개인 키는 상기 클라이언트 공개 키에 대응함－; 그리고

상기 등록 절차를 위해 상기 공유 키를 사용하게 하며,

상기 등록 절차는 상기 공유 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

클라이언트 디바이스.

청구항 69

제 68 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 클라이언트 디바이스로 하여금, 상기 공유 키로부터 도출되는 적어도 일부를 갖는 인증 응답을 전송하게 하며,

상기 인증 응답은 또한 상기 제 2 넌스를 포함하는, 클라이언트 디바이스.

청구항 70

제 68 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 클라이언트 디바이스로 하여금,

구성 데이터를 가진 제 1 메시지에 대해 디폴트 채널을 모니터링하게 하고; 그리고

상기 디폴트 채널 상에서 상기 제 1 메시지를 수신하게 하며,

상기 구성 데이터는 상기 네트워크 디바이스와 관련시키기 위해 상기 클라이언트 디바이스에 대한 정보를 포함

하는, 클라이언트 디바이스.

청구항 71

제 70 항에 있어서,

상기 제 1 메시지는 상기 클라이언트 공개 키나 상기 네트워크 공개 키에 적어도 부분적으로 기초하는 아이덴티티 정보를 포함하는, 클라이언트 디바이스.

청구항 72

구성기 디바이스의 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금 동작들을 수행하게 하는 명령들이 저장된 컴퓨터 판독 가능 매체로서,

상기 동작들은,

상기 구성기 디바이스에서, 네트워크 디바이스와 신뢰 관계를 구축하는 것;

클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차 이전에, 상기 구성기 디바이스에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하는 것; 및

상기 등록 절차를 가능하게 하기 위해 상기 클라이언트 공개 키를, 상기 신뢰 관계에 따라 상기 구성기 디바이스로부터 상기 네트워크 디바이스로 전송하는 것을 포함하며,

상기 등록 절차는, 상기 클라이언트 공개 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

컴퓨터 판독 가능 매체.

청구항 73

제 72 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 상기 구성기 디바이스 또는 상기 네트워크 디바이스로부터 상기 클라이언트 디바이스로 전송하는 것을 포함하는 동작들을 수행하게 하며,

상기 제 1 인증은 상기 네트워크 공개 키에 적어도 부분적으로 추가로 기초하는, 컴퓨터 판독 가능 매체.

청구항 74

제 72 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 것;

구성기 공개 키 -상기 구성기 공개 키는 구성기 개인 키에 대응함-를 상기 네트워크 디바이스에 전송하는 것; 및

상기 네트워크 공개 키 및 상기 구성기 개인 키에 적어도 부분적으로 기초하여 상기 신뢰 관계와 관련된 신뢰 관계 키를 결정하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 75

제 74 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

카메라, 마이크로폰, 광 검출기, 센서 및 상기 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 사용하여 상기 클라이언트 공개 키 및 상기 네트워크 공개 키 중 적어도 하나를 검출하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 76

제 72 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

요청 메시지를 상기 네트워크 디바이스에 전송하는 것;

상기 네트워크 디바이스로부터 넌스를 수신하는 것; 및

등록 메시지를 상기 네트워크 디바이스에 전송하는 것을 포함하는 동작들을 수행하게 하고,

상기 등록 메시지는, 상기 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 상기 클라이언트 공개 키를 포함하며, 상기 구성기 서명은, 상기 구성기 디바이스가 상기 등록 메시지를 전송하도록 인가되었다는 제 2 인증을 상기 네트워크 디바이스에 제공하는, 컴퓨터 판독 가능 매체.

청구항 77

제 76 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금,

상기 네트워크 디바이스로부터 등록 키를 수신하는 것; 및

상기 등록 키를 상기 클라이언트 디바이스에 전송하는 것을 포함하는 동작들을 수행하게 하며,

상기 등록 키는 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 제 1 인증을 위해 상기 클라이언트 공개 키와 함께 사용되는, 컴퓨터 판독 가능 매체.

청구항 78

제 72 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금, 상기 클라이언트 디바이스에 의해 액세스 가능한 디폴트 채널을 통해 제 1 메시지를 송신하는 것을 포함하는 동작들을 수행하게 하며,

상기 제 1 메시지는 상기 네트워크 디바이스와 관련하여 상기 클라이언트 디바이스를 돕기 위한 구성 데이터를 포함하는, 컴퓨터 판독 가능 매체.

청구항 79

제 72 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 구성기 디바이스로 하여금, 네트워크 디바이스들의 리스트 및 상기 네트워크 디바이스들의 리스트 각각에 대한 대응하는 네트워크 공개 키를 유지하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 80

네트워크 디바이스의 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금 동작들을 수행하게 하는 명령들이 저장된 컴퓨터 판독 가능 매체로서,

상기 동작들은,

상기 네트워크 디바이스에서, 구성기 디바이스와 신뢰 관계를 구축하는 것;

클라이언트 디바이스와 상기 네트워크 디바이스 사이의 등록 절차 이전에, 클라이언트 디바이스와 관련된 클라이언트 공개 키를, 상기 신뢰 관계에 따라 상기 구성기 디바이스로부터 수신하는 것; 및

상기 등록 절차를 위해 상기 클라이언트 공개 키를 사용하는 것을 포함하며,

상기 등록 절차는, 상기 클라이언트 공개 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

컴퓨터 판독 가능 매체.

청구항 81

제 80 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 네트워크 디바이스와 관련된 네트워크 공개 키를 상기 구성기 디바이스 또는 상기 클라이언트 디바이스에 제공하는 것을 포함하는 동작들을 수행하게 하며, 상기 네트워크 공개 키는 대응하는 네트워크 개인 키를 갖는, 컴퓨터 판독 가능 매체.

청구항 82

제 81 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 클라이언트 디바이스에 사용할 공유 키를 결정하는 것을 포함하는 동작들을 수행하게 하며, 상기 공유 키는 상기 클라이언트 공개 키 및 네트워크 개인 키에 적어도 부분적으로 기초하는,

컴퓨터 판독 가능 매체.

청구항 83

제 80 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 구성기 디바이스로부터 요청 메시지를 수신하는 것;

상기 구성기 디바이스에 넌스를 전송하는 것; 및

상기 구성기 디바이스로부터 등록 메시지를 수신하는 것을 포함하는 동작들을 수행하게 하고,

상기 등록 메시지는 상기 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 상기 클라이언트 공개 키를 포함하며,

상기 구성기 서명은, 상기 구성기 디바이스가 상기 등록 메시지를 전송하도록 인가되었다는 제 2 인증을 상기 네트워크 디바이스에 제공하는, 컴퓨터 판독 가능 매체.

청구항 84

제 83 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 네트워크 디바이스로부터 등록 키를 전송하는 것; 및

상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 제 1 인증을 위해 상기 클라이언트 공개 키와 함께 상기 등록 키를 사용하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 85

제 84 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 상기 제 1 인증을 위해 상기 클라이언트 공개 키를 사용한 후, 상기 네트워크 디바이스로부터 상기 클라이언트 디바이스로 구성 데이터를 전송하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 86

제 84 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 네트워크 디바이스에서, 클라이언트 디바이스들의 리스트 및 상기 클라이언트 디바이스들의 리스트 각각에 대한 대응하는 클라이언트 공개 키를 유지하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 87

제 86 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 네트워크 디바이스로 하여금,

상기 클라이언트 디바이스들의 리스트에 대한 변경을 결정 시, 상기 변경의 통보를 다른 네트워크 디바이스로 전송하는 것을 포함하는 동작들을 수행하게 하는, 컴퓨터 판독 가능 매체.

청구항 88

클라이언트 디바이스의 프로세서에 의해 실행될 때, 상기 클라이언트 디바이스로 하여금 동작들을 수행하게 하는 명령들이 저장된 컴퓨터 판독 가능 매체로서,

상기 동작들은,

상기 클라이언트 디바이스와 네트워크 디바이스 사이의 등록 절차 이전에, 상기 클라이언트 디바이스와 관련된 클라이언트 공개 키를, 상기 클라이언트 디바이스로부터 상기 네트워크의 상기 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 제공하는 것;

네트워크 디바이스와 관련된 네트워크 공개 키 및 제 1 넌스를 상기 구성기 디바이스로부터 수신하는 것;

제 2 넌스를 생성하는 것;

상기 제 1 넌스, 상기 제 2 넌스, 상기 네트워크 공개 키, 및 상기 클라이언트 디바이스와 관련된 클라이언트 개인 키에 적어도 부분적으로 기초하여 공유 키를 결정하는 것 -상기 클라이언트 개인 키는 상기 클라이언트 공개 키에 대응함-; 및

상기 등록 절차를 위해 상기 공유 키를 사용하는 것을 포함하며,

상기 등록 절차는 상기 공유 키에 적어도 부분적으로 기초한, 상기 네트워크 디바이스와 상기 클라이언트 디바이스 사이의 적어도 제 1 인증을 포함하는,

컴퓨터 판독 가능 매체.

청구항 89

제 88 항에 있어서,

상기 공유 키는 상기 네트워크 디바이스에서 대응하는 공유 키와 매칭되며,

상기 대응하는 공유 키는 상기 제 1 넌스, 상기 제 2 넌스, 네트워크 개인 키 및 상기 클라이언트 공개 키를 포함하는, 상기 네트워크 디바이스에서의 대응하는 계산에 적어도 부분적으로 기초하는, 컴퓨터 판독 가능 매체.

청구항 90

제 88 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 클라이언트 디바이스로 하여금, 상기 공유 키로부터 도출되는 적어도 일부를 갖는 인증 응답을 전송하게 하며,

상기 인증 응답은 또한 상기 제 2 넌스를 포함하는, 컴퓨터 판독 가능 매체.

청구항 91

제 88 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 상기 클라이언트 디바이스로 하여금,

구성 데이터를 가진 제 1 메시지에 대해 디폴트 채널을 모니터링하는 것; 및

상기 디폴트 채널 상에서 상기 제 1 메시지를 수신하는 것을 포함하는 동작들을 수행하게 하며,

상기 구성 데이터는 상기 네트워크 디바이스와 관련시키기 위해 상기 클라이언트 디바이스에 대한 정보를 포함하는, 컴퓨터 판독 가능 매체.

청구항 92

제 91 항에 있어서,

상기 제 1 메시지는 상기 클라이언트 공개 키나 상기 네트워크 공개 키에 적어도 부분적으로 기초하는 아이덴티티 정보를 포함하는, 컴퓨터 판독 가능 매체.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 2014년 2월 10일 출원된, 미국 가출원 일련 번호 제 61/937,891호 및 2014년 5월 14일 출원된 미국 가출원 일련 번호 제 61/996,812호 및 2015년 2월 6일 출원된 미국 출원 일련 번호 제 14/616,551호를 우선권으로 주장한다.

[0002] [0002] 본 개시의 실시예들은 일반적으로, 통신 시스템들의 분야에 관련되며, 특히 통신 네트워크에서 디바이스 프로비져닝과 관련된다.

배 경 기 술

[0003] [0003] 많은 통신 시스템들(예를 들어, 위성 통신 시스템들, 무선 통신 시스템들, PLC(powerline communication) 시스템들, 동축 케이블 통신 시스템들, 전화선 시스템들 등)에서, 네트워크는 통신 매체를 통해 서로 통신하는 디바이스로 구성된다. 전형적으로, 디바이스가 통신 매체를 통해 통신할 수 있기 전에, 디바이스는 네트워크에 대한 액세스가 그랜트되어야 한다. 액세스를 그랜트하는 프로세스는 디바이스 프로비져닝으로 지칭될 수 있으며, 연계, 등록, 인증을 위한 동작들 및/또는 다른 동작들을 포함할 수 있다.

[0004] [0004] 그러나 네트워크에 대해 새로운 디바이스를 프로비져닝하는 것은, 사용자에게 기술적으로 복잡하거나 어려울 수 있다. 예를 들어, 새로운 디바이스는, 네트워크 디바이스를 통해 이용가능한 네트워크 리소스들에 액세스하기 위해, 네트워크 디바이스(이를테면, 액세스 포인트)에 대해 등록 및/또는 인증하도록 요구될 수 있다. 전통적인 통신 시스템들에서, 등록 절차는, 액세스를 제어하고 비인가 사용을 방지하기 위해 사용자에 의해 제공되는 보안 크리덴셜들을 사용할 수 있다. 전형적인 등록 단계들은, 클라이언트 디바이스가 네트워크 디바이스의 통신 범위 내에 들어감에 따라 사용자가 코드들 또는 다른 정보를 입력하는 단계를 포함할 수 있다. 그러나 이러한 구성 단계들은 일부 사용자들에게는 상당히 복잡하게 생각될 수 있고, 네트워크들 및 이들의 리소스들의 사용을 단념하게 할 수 있다.

[0005] [0005] 더욱이, 일부 디바이스들은 "헤드리스(headless)" 디바이스로 간주될 수 있다. 헤드리스 디바이스들은 그래픽 사용자 인터페이스를 가지고 있지 않은 디바이스들이다. 헤드리스 디바이스들의 예들은, 센서들, 전구들, 카메라들, 액추에이터들, 전기 기기, 게임 제어기들, 오디오 장비 또는 통신 네트워크를 통해 통신할 수 있지만 상업적 또는 기술적 제한들로 인해 그래픽 사용자 인터페이스를 갖고 있지 않은 다른 통신 디바이스들을 포함할 수 있다. 헤드리스 디바이스의 최초 네트워크 구성은 그래픽 사용자 인터페이스의 결여로 인해 어려울 수 있다.

[0006] [0006] 디바이스 프로비져닝을 간략화하는 것은 사용자 경험을 강화하고 통신 시스템에서 더 많은 타입의 디바이스들의 채택을 조장할 수 있다.

발명의 내용

[0007] [0007] 본 개시는 네트워크로 안내되고 있는 디바이스의 등록을 용이하게 하기 위한 디바이스 프로비져닝의 다양한 실시예들을 개시한다. 디바이스 프로비져닝은 공개 키 암호방식으로부터의 개념들을 이용하여 확장될 수 있으며, 여기서 공개 키들이 디바이스 프로비져닝 프로토콜을 사용하여 디바이스들 사이에 교환된다. 디바이스 프로비져닝 프로토콜은 두 디바이스들 사이에서 직접적일 수 있거나, 구성기 디바이스로 지칭되는 제 3 디바이

스가 관여할 수 있다.

[0008] [0008] 구성기 디바이스는 새로운 클라이언트 디바이스와 네트워크 디바이스 사이에서 중재자로서 역할을 할 수 있다. 예를 들어, 클라이언트 디바이스와 네트워크 디바이스 사이의 공개 키들의 교환은 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 의해 용이하게 될 수 있다. 신뢰 관계는 대역 외 통신을 사용하여 구축될 수 있다. 새로운 클라이언트 디바이스의 등록은, 신뢰된 대역 외 채널을 통해 구성기 디바이스와 하나 이상의 공개 키들을 공유함으로서 지원될 수 있다.

[0009] [0009] 일 실시예에서, 방법은 구성기 디바이스에서, 네트워크의 네트워크 디바이스와 신뢰 관계를 구축하는 단계를 포함할 수 있다. 구성기 디바이스는 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하고, 신뢰 관계에 따라 클라이언트 공개 키를 구성기 디바이스로부터 네트워크 디바이스로 전송할 수 있다. 클라이언트 디바이스와 관련된 클라이언트 공개 키는 네트워크 디바이스와 클라이언트 디바이스 사이의 등록 프로세스를 위해 사용될 수 있다.

[0010] [0010] 다른 실시예에서, 구성기 디바이스는 신뢰된 구성기 서비스의 적어도 일부를 포함할 수 있다. 예를 들어, 신뢰된 구성기 서비스는, 클라이언트 디바이스와 네트워크 디바이스 사이의 프로비져닝을 용이하게 하기 위해 키 교환 및 키 서명(예를 들어, 증명서) 특성들을 제공할 수 있다.

[0011] [0011] 일부 실시예들에서, 클라이언트 디바이스를 네트워크 디바이스에 프로비져닝하기 위한 방법은, 구성기 디바이스에서, 네트워크 디바이스와 신뢰 관계를 구축하는 단계; 구성기 디바이스에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하는 단계; 및 클라이언트 공개 키를 신뢰 관계에 따라 구성기 디바이스로부터 네트워크 디바이스로 전송하는 단계를 포함하며, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증은 클라이언트 공개 키에 적어도 부분적으로 기초한다.

[0012] [0012] 일부 실시예들에서, 이 방법은, 네트워크 디바이스와 관련된 네트워크 공개 키를 구성기 디바이스 또는 네트워크 디바이스로부터 클라이언트 디바이스로 전송하는 단계를 더 포함하며, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증은 네트워크 공개 키에 적어도 부분적으로 추가로 기초한다.

[0013] [0013] 일부 실시예들에서, 신뢰 관계를 구축하는 단계는, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 단계; 구성기 공개 키 – 구성기 공개 키는 구성기 개인 키에 대응함–를 네트워크 디바이스에 전송하는 단계; 및 네트워크 공개 키 및 구성기 개인 키에 적어도 부분적으로 기초하여 신뢰 관계와 관련된 신뢰 관계 키를 결정하는 단계를 포함한다.

[0014] [0014] 일부 실시예들에서, 이 방법은, 구성기 디바이스로부터 네트워크 디바이스로 클라이언트 공개 키를 전송하기 전에, 신뢰 관계 키로 클라이언트 공개 키를 암호화하는 단계를 더 포함한다.

[0015] [0015] 일부 실시예들에서, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 단계는, 네트워크 디바이스와의 보안 연결을 통해 네트워크 공개 키를 수신하는 단계를 포함한다.

[0016] [0016] 일부 실시예들에서, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 단계는, 클라이언트 디바이스가 네트워크 디바이스와 구축할 연결과 상이한 네트워크 디바이스와의 대역 외 연결을 통해 네트워크 공개 키를 결정하는 단계를 포함한다.

[0017] [0017] 일부 실시예들에서, 신뢰 관계를 구축하는 단계는, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하기 전에, 네트워크 디바이스로부터 구성기 지원 서비스 통지를 수신하는 단계를 포함한다.

[0018] [0018] 일부 실시예들에서, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 단계는, 카메라, 마이크로폰, 광 검출기, 센서 및 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 사용하여 네트워크 공개 키를 검출하는 단계를 포함한다.

[0019] [0019] 일부 실시예들에서, 카메라를 사용하여 네트워크 공개 키를 검출하는 단계는, 네트워크 디바이스와 관련된 이미지를 검출하기 위해 카메라를 사용하는 단계를 포함하며, 이미지의 적어도 일부는 네트워크 공개 키를 포함한다.

[0020] [0020] 일부 실시예들에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하는 단계는, 카메라, 마이크로폰, 광 검출기, 센서 및 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 사용하여 클라이언트 공개 키를 검출하는 단계를 포함한다.

[0021] [0021] 일부 실시예들에서, 카메라를 사용하여 클라이언트 공개 키를 검출하는 단계는, 클라이언트 디바이스와

관련된 이미지를 검출하기 위해 카메라를 사용하는 단계를 포함한다.

[0022] [0022] 일부 실시예들에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 전송하는 단계는, 요청 메시지를 네트워크 디바이스에 전송하는 단계; 네트워크 디바이스로부터 넌스를 수신하는 단계; 및 등록 메시지를 네트워크 디바이스에 전송하는 단계를 포함하며, 등록 메시지는 클라이언트 공개 키 및 구성기 서명을 포함하며, 구성기 서명은, 구성기 디바이스가 등록 메시지를 전송하도록 인가되었다는 인증을 네트워크 디바이스에 제공한다.

[0023] [0023] 일부 실시예들에서, 구성기 서명은 넌스 및 구성기 개인 키로부터 도출되거나 신뢰 관계와 관련된 신뢰 관계 키에 적어도 부분적으로 기초한다.

[0024] [0024] 일부 실시예들에서, 이 방법은, 네트워크 디바이스로부터 등록 키를 수신하는 단계; 및 등록 키를 클라이언트 디바이스에 전송하는 단계를 더 포함하며, 등록 키는 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키와 함께 사용된다.

[0025] [0025] 일부 실시예들에서, 이 방법은, 신뢰 관계를 구축한 후, 구성 데이터를 구성기 디바이스로부터 네트워크 디바이스로 전송하는 단계를 더 포함한다.

[0026] [0026] 일부 실시예들에서, 이 방법은, 네트워크 디바이스와 관련하여 클라이언트 디바이스를 돕기 위해 구성 데이터를 구성기 디바이스로부터 클라이언트 디바이스로 전송하는 단계를 더 포함한다.

[0027] [0027] 일부 실시예들에서, 구성 데이터를 전송하는 단계는, 클라이언트 디바이스에 의해 액세스 가능한 디폴트 채널을 통해 제 1 메시지를 송신하는 단계를 포함한다.

[0028] [0028] 일부 실시예들에서, 제 1 메시지는, 네트워크 디바이스와 관련된 네트워크 공개 키나 클라이언트 공개 키에 적어도 부분적으로 기초한 아이덴티티 정보를 포함한다.

[0029] [0029] 일부 실시예들에서, 클라이언트 디바이스는 제 1 클라이언트 디바이스이고, 네트워크 디바이스는 제 2 클라이언트 디바이스이고, 구성기 디바이스는 액세스 포인트이다.

[0030] [0030] 일부 실시예들에서, 네트워크 디바이스는 네트워크의 액세스 포인트이고, 구성기 디바이스는 액세스 포인트와 관련된다.

[0031] [0031] 일부 실시예들에서, 이 방법은, 네트워크 디바이스들의 리스트 및 네트워크 디바이스들의 리스트 각각에 대한 대응하는 네트워크 공개 키를 유지하는 단계를 더 포함한다.

[0032] [0032] 일부 실시예들에서, 네트워크 디바이스가 클라이언트 디바이스를 인증하기 위한 방법은, 네트워크 디바이스에서, 구성기 디바이스와 신뢰 관계를 구축하는 단계; 신뢰 관계에 따라 구성기 디바이스로부터, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 수신하는 단계; 및 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키를 사용하는 단계를 포함한다.

[0033] [0033] 일부 실시예들에서, 신뢰 관계를 구축하는 단계는, 네트워크 디바이스와 관련된 네트워크 공개 키를 구성기 디바이스 또는 클라이언트 디바이스에 제공하는 단계를 포함하며, 네트워크 공개 키는 대응하는 네트워크 개인 키를 갖는다.

[0034] [0034] 일부 실시예들에서, 네트워크 디바이스와 관련된 네트워크 공개 키를 제공하는 단계는, 네트워크 디바이스의 디스플레이 또는 단거리 라디오 주파수 인터페이스를 이용하여 네트워크 공개 키를 제공하는 단계를 포함한다.

[0035] [0035] 일부 실시예들에서, 이 방법은, 디폴트 채널을 통해 제 1 메시지를 송신하는 단계를 더 포함하며, 제 1 메시지는 네트워크 디바이스와 관련된 네트워크 공개 키나 클라이언트 공개 키로부터 도출되는 정보를 포함한다.

[0036] [0036] 일부 실시예들에서, 이 방법은, 클라이언트 디바이스에 사용할 공유 키를 결정하는 단계를 더 포함하며, 공유 키는 클라이언트 공개 키 및 네트워크 개인 키에 적어도 부분적으로 기초한다.

[0037] [0037] 일부 실시예들에서, 이 방법은, 구성기 디바이스로부터 구성기 공개 키를 수신하는 단계; 및 네트워크 개인 키 및 구성기 공개 키에 적어도 부분적으로 기초하여 신뢰 관계와 관련된 신뢰 관계 키를 결정하는 단계를 더 포함한다.

[0038] [0038] 일부 실시예들에서, 클라이언트 공개 키를 수신하는 단계는, 신뢰 관계 키로 암호화된 클라이언트 공개

키를 수신하는 단계를 포함한다.

[0039] [0039] 일부 실시예들에서, 신뢰 관계를 구축하는 단계는, 네트워크 디바이스로부터 구성기 지원 서비스 통지를 송신하는 단계를 포함한다.

[0040] [0040] 일부 실시예들에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 수신하는 단계는, 구성기 디바이스로부터 요청 메시지를 수신하는 단계; 구성기 디바이스에 넌스를 전송하는 단계; 및 구성기 디바이스로부터 등록 메시지를 수신하는 단계를 포함하며, 등록 메시지는 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 클라이언트 공개 키를 포함한다.

[0041] [0041] 일부 실시예들에서, 이 방법은 구성기 공개 키 및 구성기 서명에 적어도 부분적으로 기초하여 등록 메시지를 인증하는 단계를 더 포함한다.

[0042] [0042] 일부 실시예들에서, 이 방법은, 네트워크 디바이스로부터 등록 키를 전송하는 단계; 및 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키와 함께 등록 키를 사용하는 단계를 더 포함한다.

[0043] [0043] 일부 실시예들에서, 이 방법은, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키를 사용한 후, 네트워크 디바이스로부터 클라이언트 디바이스로 구성 데이터를 전송하는 단계를 더 포함한다.

[0044] [0044] 일부 실시예들에서, 이 방법은, 네트워크 디바이스에서, 클라이언트 디바이스들의 리스트 및 클라이언트 디바이스들의 리스트 각각에 대한 대응하는 클라이언트 공개 키를 유지하는 단계를 더 포함한다.

[0045] [0045] 일부 실시예들에서, 이 방법은, 클라이언트 디바이스들의 리스트에 대한 변경을 결정 시, 변경의 통보를 다른 네트워크 디바이스로 전송하는 단계를 더 포함한다.

[0046] [0046] 일부 실시예들에서, 이 방법은, 네트워크 디바이스에서, 구성기 디바이스들의 리스트 및 구성기 디바이스들의 리스트 각각에 대한 대응하는 신뢰 관계 키를 유지하는 단계를 더 포함한다.

[0047] [0047] 일부 실시예들에서, 클라이언트 디바이스가 네트워크 디바이스에 인증하기 위한 방법은, 네트워크 디바이스와 관련된 네트워크 공개 키 및 제 1 넌스를 수신하는 단계; 제 2 넌스를 생성하는 단계; 제 1 넌스, 제 2 넌스, 네트워크 공개 키, 및 클라이언트 디바이스와 관련된 클라이언트 개인 키를 포함하는 계산에 적어도 부분적으로 기초하여 공유 키를 결정하는 단계 – 클라이언트 개인 키는 클라이언트 디바이스와 관련된 클라이언트 공개 키에 대응함–; 및 공유 키로부터 도출된 적어도 일부를 갖는 인증 응답을 전송하는 단계를 포함하며, 인증 응답은 제 2 넌스를 포함한다.

[0048] [0048] 일부 실시예들에서, 공유 키는 네트워크 디바이스에서 대응하는 공유 키와 매칭되며, 대응하는 공유 키는 제 1 넌스, 제 2 넌스, 네트워크 개인 키 및 클라이언트 공개 키를 포함하는, 네트워크 디바이스에서의 대응하는 계산에 적어도 부분적으로 기초한다.

[0049] [0049] 일부 실시예들에서, 이 방법은, 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 클라이언트 공개 키를 전송하는 단계를 더 포함한다.

[0050] [0050] 일부 실시예들에서, 인증 응답은, 클라이언트 디바이스가 네트워크 공개 키를 획득했다는 것을, 네트워크 디바이스에게 확인해 준다.

[0051] [0051] 일부 실시예들에서, 네트워크 공개 키는 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스로부터 수신된다.

[0052] [0052] 일부 실시예들에서, 이 방법은, 구성 데이터를 가진 제 1 메시지에 대해 디폴트 채널을 모니터링하는 단계; 및 디폴트 채널 상에서 제 1 메시지를 수신하는 단계를 더 포함하며, 구성 데이터는 네트워크 디바이스와 관련시키기 위해 클라이언트 디바이스에 대한 정보를 포함한다.

[0053] [0053] 일부 실시예들에서, 제 1 메시지는 클라이언트 공개 키나 네트워크 공개 키에 적어도 부분적으로 기초하는 아이덴티티 정보를 포함한다.

[0054] [0054] 일부 실시예들에서, 네트워크 디바이스에 클라이언트 디바이스를 인증하기 위한 방법은, 구성기 디바이스에서, 클라이언트 디바이스 또는 네트워크 디바이스 중 하나와 관련된 제 1 공개 키를 결정하는 단계; 구성기 디바이스에서, 제 1 공개 키 및 구성기 개인 키에 기초하여 제 1 증명서를 생성하는 단계; 및 클라이언트 디바

이스와 네트워크 디바이스 사이에서 인증 프로세스를 용이하게 하기 위해 클라이언트 디바이스 또는 네트워크 디바이스 중 하나에 제 1 증명서를 전송하는 단계를 포함한다.

[0055] [0055] 일부 실시예들에서, 이 방법은, 구성기 디바이스에서, 클라이언트 디바이스 또는 네트워크 디바이스 중 나머지 하나와 관련된 제 2 공개 키를 결정하는 단계; 구성기 디바이스에서, 제 2 공개 키 및 구성기 개인 키에 기초하여 제 2 증명서를 생성하는 단계; 및 클라이언트 디바이스와 네트워크 디바이스 사이의 인증 프로세스를 용이하게 하기 위해 클라이언트 디바이스 또는 네트워크 디바이스 중 나머지 하나에 제 2 증명서를 전송하는 단계를 더 포함한다.

[0056] [0056] 일부 실시예들에서, 제 1 증명서는 클라이언트 디바이스 또는 네트워크 디바이스 중 하나의 아이덴티티를 검증하고, 인증 프로세스는 제 1 증명서로부터 적어도 부분적으로 도출된 공유 키에 기초한다.

[0057] [0057] 일부 실시예들에서, 구성기 디바이스는, 프로세서; 및 명령들을 저장하기 위한 메모리를 포함하며, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 구성기 디바이스에서, 네트워크 디바이스와 신뢰 관계를 구축하게 하고; 구성기 디바이스에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하게 하고; 그리고 클라이언트 공개 키를 신뢰 관계에 따라 구성기 디바이스로부터 네트워크 디바이스로 전송하게 하며, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증은 클라이언트 공개 키에 적어도 부분적으로 기초한다.

[0058] [0058] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키를 구성기 디바이스 또는 네트워크 디바이스로부터 클라이언트 디바이스로 전송하게 하며, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증은 네트워크 공개 키에 적어도 부분적으로 추가로 기초한다.

[0059] [0059] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하게 하고; 구성기 공개 키 – 구성기 공개 키는 구성기 개인 키에 대응함–를 네트워크 디바이스에 전송하게 하고; 그리고 네트워크 공개 키 및 구성기 개인 키에 적어도 부분적으로 기초하여 신뢰 관계와 관련된 신뢰 관계 키를 결정하게 한다.

[0060] [0060] 일부 실시예들에서, 구성기 디바이스는 클라이언트 디바이스가 네트워크 디바이스와 구축할 연결과 상이한 네트워크 디바이스와의 대역 외 연결을 구축하기 위한 인터페이스를 더 포함하며, 네트워크 공개 키를 결정하기 위한 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와의 대역 외 연결을 통해 네트워크 공개 키를 결정하게 하는 명령들을 포함한다.

[0061] [0061] 일부 실시예들에서, 인터페이스는, 카메라, 마이크로폰, 광 검출기, 센서 및 단거리 라디오 주파수 인터페이스로 구성된 그룹의 멤버를 포함한다.

[0062] [0062] 일부 실시예들에서, 클라이언트 공개 키를 결정하기 위한 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 인터페이스를 이용하여 클라이언트 공개 키를 검출하게 하는 명령들을 포함한다.

[0063] [0063] 일부 실시예들에서, 클라이언트 공개 키를 전송하기 위한 명령들은, 프로세서에 의해 실행될 때 프로세서로 하여금, 요청 메시지를 네트워크 디바이스에 전송하게 하고; 네트워크 디바이스로부터 넌스를 수신하게 하고; 그리고 등록 메시지를 네트워크 디바이스에 전송하게 하는 명령들을 포함하며, 등록 메시지는 클라이언트 공개 키 및 구성기 서명을 포함하며, 구성기 서명은, 구성기 디바이스가 등록 메시지를 전송하도록 인가되었다는 인증을 네트워크 디바이스에 제공한다.

[0064] [0064] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때 프로세서로 하여금, 네트워크 디바이스로부터 등록 키를 수신하게 하고; 그리고 등록 키를 클라이언트 디바이스에 전송하게 하며, 등록 키는 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키와 함께 사용된다.

[0065] [0065] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때 프로세서로 하여금, 네트워크 디바이스와 관련하여 클라이언트 디바이스를 돕기 위해 구성 데이터를 구성기 디바이스로부터 클라이언트 디바이스로 전송하게 한다.

[0066] [0066] 일부 실시예들에서, 구성 데이터를 전송하기 위한 명령들은, 프로세서에 의해 실행될 때 프로세서로 하여금, 클라이언트 디바이스에 의해 액세스 가능한 디폴트 채널을 통해 제 1 메시지를 송신하게 하는 명령들을 포함한다.

[0067] [0067] 일부 실시예들에서, 제 1 메시지는, 네트워크 디바이스와 관련된 네트워크 공개 키나 클라이언트 공개

키에 적어도 부분적으로 기초한 아이덴티티 정보를 포함한다.

[0068] [0068] 일부 실시예들에서, 구성기 디바이스는, 네트워크 디바이스들의 리스트 및 네트워크 디바이스들의 리스트 각각에 대한 대응하는 네트워크 공개 키를 유지하기 위한 메모리를 더 포함한다.

[0069] [0069] 일부 실시예들에서, 네트워크 디바이스는, 프로세서; 및 명령들을 저장하기 위한 메모리를 포함하며, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스에서, 구성기 디바이스와 신뢰 관계를 구축하게 하고; 신뢰 관계에 따라 구성기 디바이스로부터, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 수신하게 하고; 그리고 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키를 사용하게 한다.

[0070] [0070] 일부 실시예들에서, 신뢰 관계를 구축하기 위한 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키를 구성기 디바이스 또는 클라이언트 디바이스에 제공하게 하는 명령들을 포함하며, 네트워크 공개 키는 대응하는 네트워크 개인 키를 갖는다.

[0071] [0071] 일부 실시예들에서, 네트워크 디바이스는 네트워크 인터페이스를 더 포함하며, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 인터페이스를 통해, 디폴트 채널 상에서 제 1 메시지를 송신하게 하며, 제 1 메시지는 네트워크 디바이스와 관련된 네트워크 공개 키나 클라이언트 공개 키로부터 도출되는 정보를 포함한다.

[0072] [0072] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 클라이언트 디바이스에 사용할 공유 키를 결정하게 하고, 공유 키는 클라이언트 공개 키 및 네트워크 개인 키에 적어도 부분적으로 기초한다.

[0073] [0073] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 구성기 디바이스로부터 요청 메시지를 수신하게 하고; 구성기 디바이스에 넌스를 전송하게 하고; 그리고 구성기 디바이스로부터 등록 메시지를 수신하게 하며, 등록 메시지는 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 클라이언트 공개 키를 포함한다.

[0074] [0074] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스로부터 등록 키를 전송하게 하고; 그리고 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키와 함께 등록 키를 사용하게 한다.

[0075] [0075] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키를 사용한 후, 네트워크 디바이스로부터 클라이언트 디바이스로 구성 데이터를 전송하게 한다.

[0076] [0076] 일부 실시예들에서, 네트워크 디바이스는, 네트워크 디바이스에서, 클라이언트 디바이스들의 리스트 및 클라이언트 디바이스들의 리스트 각각에 대한 대응하는 클라이언트 공개 키를 유지하기 위한 메모리를 더 포함한다.

[0077] [0077] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 클라이언트 디바이스들의 리스트에 대한 변경을 결정 시, 변경의 통보를 다른 네트워크 디바이스로 전송하게 한다.

[0078] [0078] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스에서, 구성기 디바이스들의 리스트 및 구성기 디바이스들의 리스트 각각에 대한 대응하는 신뢰 관계 키를 유지하도록 메모리하게 한다.

[0079] [0079] 일부 실시예들에서, 클라이언트 디바이스는, 프로세서; 및 명령들을 저장하기 위한 메모리를 포함하며, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키 및 제 1 넌스를 수신하게 하고; 제 2 넌스를 생성하게 하고; 제 1 넌스, 제 2 넌스, 네트워크 공개 키, 및 클라이언트 디바이스와 관련된 클라이언트 개인 키를 포함하는 계산에 적어도 부분적으로 기초하여 공유 키를 결정하게 하고 – 클라이언트 개인 키는 클라이언트 디바이스와 관련된 클라이언트 공개 키에 대응함–; 그리고 공유 키로부터 도출된 적어도 일부를 갖는 인증 응답을 전송하게 하며, 인증 응답은 제 2 넌스를 포함한다.

[0080] [0080] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 제 1 넌스를 수신하기 전에, 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 클라이언트 공개 키를 전송하게 한다.

[0081] [0081] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 구성 데이터를 가진 제 1

메시지에 대해 디폴트 채널을 모니터링하게 하고; 그리고 디폴트 채널 상에서 제 1 메시지를 수신하게 하며, 구성 데이터는 네트워크 디바이스와 관련시키기 위해 클라이언트 디바이스에 대한 정보를 포함한다.

[0082] [0082] 일부 실시예들에서, 제 1 메시지는 클라이언트 공개 키나 네트워크 공개 키에 적어도 부분적으로 기초하는 아이덴티티 정보를 포함한다.

[0083] [0083] 일부 실시예들에서, 컴퓨터 판독 가능 매체는 프로세서에 의해 실행될 때, 프로세서로 하여금 동작들을 수행하게 하는 명령들을 저장하며, 이 동작들은, 구성기 디바이스에서, 네트워크 디바이스와 신뢰 관계를 구축하는 것; 구성기 디바이스에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정하는 것; 및 클라이언트 공개 키를 신뢰 관계에 따라 구성기 디바이스로부터 네트워크 디바이스로 전송하는 것을 포함하며, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증은 클라이언트 공개 키에 적어도 부분적으로 기초한다.

[0084] [0084] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키를 구성기 디바이스 또는 네트워크 디바이스로부터 클라이언트 디바이스로 전송하는 것을 포함하는 동작들을 수행하게 하며, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증은 네트워크 공개 키에 적어도 부분적으로 추가로 기초한다.

[0085] [0085] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키를 결정하는 것; 구성기 공개 키 – 구성기 공개 키는 구성기 개인 키에 대응함–를 네트워크 디바이스에 전송하는 것; 및 네트워크 공개 키 및 구성기 개인 키에 적어도 부분적으로 기초하여 신뢰 관계와 관련된 신뢰 관계 키를 결정하는 것을 포함하는 동작들을 수행하게 한다.

[0086] [0086] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 카메라, 마이크로폰, 광 검출기, 센서 및 구성기 디바이스의 단거리 라디오 주파수 인터페이스로 구성된 그룹 중 적어도 하나의 멤버를 사용하여 클라이언트 공개 키 및 네트워크 공개 키 중 적어도 하나를 검출하는 것을 포함하는 동작들을 수행하게 한다.

[0087] [0087] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 요청 메시지를 네트워크 디바이스에 전송하는 것; 네트워크 디바이스로부터 넌스를 수신하는 것; 및 등록 메시지를 네트워크 디바이스에 전송하는 것을 포함하는 동작들을 수행하게 하고, 등록 메시지는 클라이언트 공개 키 및 구성기 서명을 포함하며, 구성기 서명은, 구성기 디바이스가 등록 메시지를 전송하도록 인가되었다는 인증을 네트워크 디바이스에 제공한다.

[0088] [0088] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스로부터 등록 키를 수신하는 것; 및 등록 키를 클라이언트 디바이스에 전송하는 것을 포함하는 동작들을 수행하게 하며, 등록 키는 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키와 함께 사용된다.

[0089] [0089] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 클라이언트 디바이스에 의해 액세스 가능한 디폴트 채널을 통해 제 1 메시지를 송신하는 것을 포함하는 동작들을 수행하게 하며, 제 1 메시지는 네트워크 디바이스와 관련하여 클라이언트 디바이스를 돕기 위한 구성 데이터를 포함한다.

[0090] [0090] 일부 실시예들에서, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스들의 리스트 및 네트워크 디바이스들의 리스트 각각에 대한 대응하는 네트워크 공개 키를 유지하는 것을 포함하는 동작들을 수행하게 한다.

[0091] [0091] 일부 실시예들에서, 컴퓨터 판독 가능 매체는 프로세서에 의해 실행될 때, 프로세서로 하여금 동작들을 수행하게 하는 명령들을 저장하며, 이 동작들은, 네트워크 디바이스에서, 구성기 디바이스와 신뢰 관계를 구축하는 것; 신뢰 관계에 따라 구성기 디바이스로부터, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 수신하는 것; 및 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키를 사용하는 것을 포함한다.

[0092] [0092] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 관련된 네트워크 공개 키를 구성기 디바이스 또는 클라이언트 디바이스에 제공하는 것을 포함하는 동작들을 수행하게 하며, 네트워크 공개 키는 대응하는 네트워크 개인 키를 갖는다.

[0093] [0093] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 클라이언트 디바이스에 사용할 공유 키를 결정하는 것을 포함하는 동작들을 수행하게 하며, 공유 키는 클라이언트 공개 키 및 네트워크

개인 키에 적어도 부분적으로 기초한다.

[0094] [0094] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 구성기 디바이스로부터 요청 메시지를 수신하는 것; 구성기 디바이스에 넌스를 전송하는 것; 및 구성기 디바이스로부터 등록 메시지를 수신하는 것을 포함하는 동작들을 수행하게 하며, 등록 메시지는 넌스 및 구성기 개인 키로부터 적어도 부분적으로 도출되는 구성기 서명 및 클라이언트 공개 키를 포함한다.

[0095] [0095] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스로부터 등록 키를 전송하는 것; 및 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키와 함께 등록 키를 사용하는 것을 포함하는 동작들을 수행하게 한다.

[0096] [0096] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 클라이언트 공개 키를 사용한 후, 네트워크 디바이스로부터 클라이언트 디바이스로 구성 데이터를 전송하는 것을 포함하는 동작들을 수행하게 한다.

[0097] [0097] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스에서, 클라이언트 디바이스들의 리스트 및 클라이언트 디바이스들의 리스트 각각에 대한 대응하는 클라이언트 공개 키를 유지하는 것을 포함하는 동작들을 수행하게 한다.

[0098] [0098] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 클라이언트 디바이스들의 리스트에 대한 변경을 결정 시, 변경의 통보를 다른 네트워크 디바이스로 전송하는 것을 포함하는 동작들을 수행하게 한다.

[0099] [0099] 일부 실시예들에서, 컴퓨터 판독 가능 매체는 프로세서에 의해 실행될 때, 프로세서로 하여금 동작들을 수행하게 하는 명령들을 저장하며, 이 동작들은, 네트워크 디바이스와 관련된 네트워크 공개 키 및 제 1 넌스를 클라이언트 디바이스에서 수신하는 것; 제 2 넌스를 생성하는 것; 제 1 넌스, 제 2 넌스, 네트워크 공개 키, 및 클라이언트 디바이스와 관련된 클라이언트 개인 키를 포함하는 계산에 적어도 부분적으로 기초하여 공유 키를 결정하는 것 – 클라이언트 개인 키는 클라이언트 디바이스와 관련된 클라이언트 공개 키에 대응함–; 및 공유 키로부터 도출된 적어도 일부를 갖는 인증 응답을 전송하는 것을 포함하며, 인증 응답은 제 2 넌스를 포함한다.

[0100] [0100] 일부 실시예들에서, 공유 키는 네트워크 디바이스에서 대응하는 공유 키와 매칭되며, 대응하는 공유 키는 제 1 넌스, 제 2 넌스, 네트워크 개인 키 및 클라이언트 공개 키를 포함하는, 네트워크 디바이스에서의 대응하는 계산에 적어도 부분적으로 기초한다.

[0101] [0101] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 네트워크 디바이스와 신뢰 관계를 갖는 구성기 디바이스에 클라이언트 공개 키를 전송하는 것을 포함하는 동작들을 수행하게 한다.

[0102] [0102] 일부 실시예들에서, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금, 구성 데이터를 가진 제 1 메시지에 대해 디폴트 채널을 모니터링하는 것; 및 디폴트 채널 상에서 제 1 메시지를 수신하는 것을 포함하는 동작들을 수행하게 하며, 구성 데이터는 네트워크 디바이스와 관련시키기 위해 클라이언트 디바이스에 대한 정보를 포함한다.

[0103] [0103] 일부 실시예들에서, 제 1 메시지는 클라이언트 공개 키나 네트워크 공개 키에 적어도 부분적으로 기초하는 아이덴티티 정보를 포함한다.

도면의 간단한 설명

[0104] [00104] 본 개시는 첨부된 도면들을 참조함으로써 더 잘 이해될 수 있으며, 다양한 목적들, 특징들 및 장점들이 당업자에게 명확하게 될 수 있다.

[00105] 도 1은 본 개시의 실시예에 따라, 지원된 디바이스 프로비저닝(예를 들어, 등록, 구성, 및/또는 인증)의 개념을 도입하는 개념도이다.

[00106] 도 2는 본 개시의 실시예에 따라, 다양한 키 공유 특성들을 설명하는 예시적인 블록도이다.

[00107] 도 3은 본 개시의 실시예에 따라, 구성기 디바이스에 의해 수행된 동작들을 예시하는 흐름도이다.

[00108] 도 4는 본 개시의 실시예들에 따라, 클라이언트 공유 키를 네트워크 디바이스에 제공하기 위해 구성기

디바이스를 사용하는 지원된 디바이스 프로비져닝의 예를 예시하는 메시지 흐름도이다.

[00109] 도 5는 본 개시의 실시예들에 따라, 클라이언트 디바이스가 디폴트 채널을 모니터링하는 지원된 디바이스 프로비져닝의 예를 예시하는 메시지 흐름도이다.

[00110] 도 6은 본 개시의 실시예들에 따라, 구성기 디바이스가 등록 키를 클라이언트 디바이스에 제공하는 지원된 디바이스 프로비져닝의 예를 예시하는 메시지 흐름도이다.

[00111] 도 7은 본 개시의 실시예에 따라, 신뢰 관계를 구축하는 구성기 디바이스 및 네트워크 디바이스를 예시하는 메시지 프로세스 도면이다.

[00112] 도 8은 본 개시의 실시예에 따라, 연결을 구축하는 클라이언트 디바이스 및 네트워크 디바이스를 예시하는 메시지 프로세스 도면이다.

[00113] 도 9는 본 개시의 실시예에 따라, 지원된 디바이스 프로비져닝을 위한 클라우드 기반 신뢰 구성기 서비스를 예시하는 메시지 프로세스 도면이다.

[00114] 도 10은 본 개시의 실시예에 따라, 증명서들을 사용하여 클라우드 기반 신뢰 구성기 서비스를 예시하는 또 다른 메시지 프로세스 도면이다.

[00115] 도 11은 본 개시의 실시예에 따라, 피어-투-피어 무선 연결을 용이하게 하기 위해 구성기로서 역할을 하는 액세스 포인트를 예시하는 메시지 프로세스 도면이다.

[00116] 도 12는 본 개시의 실시예에 따라, 제 2 구성기 디바이스를 부가하는 것을 예시하는 메시지 프로세스 도면이다.

[00117] 도 13은 본 개시의 실시예에 따라, 공개 키 리스트들을 예시하는 개념도이다.

[00118] 도 14는 본 개시의 다양한 실시예들을 구현할 수 있는 디바이스를 설명하는 예시적인 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0105] [00119] 다음의 설명은 본 개시물의 기술들을 구현하는 예시적인 시스템들, 방법들, 기법들, 명령 시퀀스들 및 컴퓨터 프로그램 물건들을 포함한다. 그러나, 설명 실시예들은 이러한 특정한 세부사항들 없이도 실시될 수 있음을 이해한다. 예를 들어, 본 명세서에 개시된 예들이 무선 로컬 영역 네트워크(WLAN) 등록을 언급하지만, 실시예들은 그렇게 제한되지 않는다. 다른 실시예들에서, 디바이스 프로비져닝은, 다른 적절한 공유 매체 통신 네트워크들, 예컨대, PLC(powerline communications), 동축케이블 네트워크들 및/또는 전화회선 로컬 영역 네트워크들 등에서 클라이언트 디바이스들에 의해 구현될 수 있다. 일부 예들에서, 잘 알려진 명령 인스턴스들, 프로토콜들, 구조들 및 기술들은 설명을 모호하게 하지 않기 위해서 완전히 상세하게는 도시되지 않았다.

[0106] [00120] 본 개시의 실시예들은, 통신 네트워크의 네트워크 디바이스와의 클라이언트 디바이스의 디바이스 프로비져닝을 용이하게 할 수 있다. 디바이스 프로비져닝은, 클라이언트 디바이스가, 네트워크 디바이스를 통해 다른 디바이스 또는 네트워크 소스들, 예컨대, 데이터 저장소, 프린터들, 클라우드 기반 리소스들, 및/또는 인터넷 액세스 등에 액세스하게 할 수 있다. 이러한 개시에서, 등록, 등록하는 것 등의 용어들은 디바이스 프로비져닝을 지칭하기 위해 상호 교환가능하게 사용된다.

[0107] [00121] 일 실시예에서, 구성기 디바이스는 클라이언트 디바이스와 관련된 클라이언트 공개 키를 획득하고 클라이언트 공개 키를 네트워크 디바이스레 전송할 수 있다. 네트워크 디바이스는, 네트워크 디바이스와 클라이언트 디바이스 사이의 등록 프로세스에서 클라이언트 공개키를 사용할 수 있다. 등록 절차의 완료 이후, 클라이언트 디바이스는, 다른 네트워크 리소스들에 액세스하는 것과 같이, 네트워크 디바이스에 사용하기 위해 구성될 수 있다. 추가의 인증이 또한 성공적인 등록 프로세스의 결과로서 수행될 수 있다.

[0108] [00122] 일 실시예에서, 네트워크 디바이스는, 네트워크 디바이스와 클라이언트 디바이스 사이의 통신 채널을 통해 클라이언트 공개 키가 공유(예를 들어, 송신)되지 않고, 클라이언트 디바이스를 등록하기 위해 클라이언트 공개 키를 사용할 수 있다. 예를 들어, 네트워크 디바이스는 네트워크 디바이스와 클라이언트 디바이스 사이의 공유 키를 생성하기 위해 클라이언트 공개 키를 사용할 수 있다. 공유 키는, 공개 키들이 교환되는 등록 프로토콜을 사용하여 클라이언트 디바이스에 제공될 수 있고, 공유 키는 통신 매체를 통해 공유 키를 송신하지 않고, 클라이언트 디바이스와 네트워크 디바이스 각각에 의해 로컬하게 결정된다. 사용되고 있는 등록 프로토콜은, 적어도 부분적으로, Diffie-Hellman, SAE(Simultaneous Authentication of Equals), WPS(Wi-Fi

Protected Setup) 및/또는 클라이언트 공개/개인 키들 및 네트워크 공개/개인 키들을 사용하는 임의의 다른 기술적으로 적절한 키 구축 프로토콜에 기초한 동작들을 포함할 수 있다. 이러한 방식에서, 네트워크 디바이스에 액세스하기 위한 허가는, 예를 들어, 사용자가 코드들 또는 패스워드들을 입력하는 것과 같은 동작들을 취할 필요 없이, 클라이언트 디바이스의 사용자에게 투명할 수 있다.

[0109] [00123] 클라이언트 공개 키가 결정되고, 신뢰 디바이스, 예컨대, 구성기 디바이스를 통해 네트워크 디바이스로 제공될 수 있다. 구성기 디바이스는 네트워크 디바이스와 콜로케이팅될 수 있거나, 분리될 수 있다. 구성기 디바이스는 네트워크 디바이스, 예컨대, 액세스 포인트와 신뢰 관계를 구축하는 사용자 디바이스, 예컨대, 스마트폰일 수 있다. 일부 실시예들에서, 구성기 디바이스는 클라이언트 디바이스와 관련하여 접근성 또는 신뢰를 가질 수 있다. 예를 들어, 구성기 디바이스는, 클라이언트와 직접적으로 대역 외 통신을 사용하여 클라이언크 공개 키를 획득할 수 있다. 대역 외 통신의 사용은 잠재적 위장 또는 중간자 공격들을 방지함으로써 도움이 될 수 있다. 다른 어떠한 공개 키도 클라이언트 디바이스에 대해 공개 키로서 부적절하게 사용될 수 없도록, 구성기 디바이스는 클라이언트 디바이스로부터 클라이언트 공개 키를 획득하도록 구성될 수 있다.

[0110] [00124] 네트워크는, 몇몇 네트워크 디바이스들에서 디바이스의 등록을 조정하기 위해, 디바이스들의 리스트 및 관련된 공개 키들을 유지할 수 있다. 예를 들어, 제 1 네트워크 디바이스에 부가된 클라이언트 디바이스는, 제 1 네트워크 디바이스가 제 2 네트워크 디바이스에 대해 클라이언트 디바이스의 공개 키를 공유하는 것에 응답하여 제 2 네트워크 디바이스에서 등록될 수 있다. 부가적으로, 클라이언트 디바이스가 네트워크로부터 제거될 때, 디바이스들의 리스트로부터 디바이스 공개 키의 제거는 다른 네트워크 디바이스들 사이에서 클라이언트 디바이스의 제거를 캐스케이딩할 수 있다. 네트워크의 하나 이상의 네트워크 디바이스들은 네트어크와 관련되는 구성기 디바이스들의 리스트 및 클라이언트 디바이스의 리스트를 유지할 수 있다. 클라이언트 디바이스(들)의 공개 키들 및 구성기 디바이스(들)는 네트워크에서 신뢰된 디바이스들 사이에서 공유될 수 있다.

[0111] [00125] 일부 실시예들에서, 구성기 디바이스는 클라이언트 증명을 생성하기 위해 클라이언트 공개 키를 증명할 수 있고, 또한 네트워크 증명을 생성하기 위해 네트워크 공개 키를 증명할 수 있다. 클라이언트 증명 및 네트워크 증명은 구성기 개인 키를 사용하여 증명될 수 있다. 증명서들은 클라이언트 디바이스와 네트워크 디바이스 사이의 등록을 용이하게 하기 위해 사용될 수 있는데, 그 이유는 클라이언트 공개 키 및 네트워크 공개 키의 진정성이 이러한 두 디바이스들 각각에 의해 검증될 수 있기 때문이다.

[0112] [00126] 전술한 설명에서, 구성기 디바이스는 다수의 상이한 실시예들에서 사용될 수 있다. 예를 들어, 구성기 디바이스는 단일 공개 키(예를 들어, 클라이언트 디바이스로부터의 클라이언트 공개 키)를 네트워크 디바이스에 전달하기 위해 사용될 수 있다. 다른 예에서, 구성기 디바이스가 두 개의 공개 키들(예를 들어, 클라이언트 공개 키 및 네트워크 공개 키)을 네트워크 디바이스 및 클라이언트 디바이스에 각각 전달하기 위해 사용될 수 있다. 다른 예에서, 구성기 디바이스가 또한 클라이언트 디바이스 및 네트워크 디바이스 각각에 대해 인증 특성을 제공할 수 있다. 다양한 예들에서, 구성기 디바이스는, 공개 키들이 올바른 클라이언트 디바이스와 올바른 네트워크 디바이스 사이에서 공유되는 신뢰성을 제공하기 위해, 네트워크 디바이스와의 신뢰 관계를 그리고 클라이언트 디바이스와 대역 외 통신을 이용할 수 있다.

[0113] [00127] 도 1은 본 개시가 사용될 수 있는 예시적인 시스템(100)을 도시한다. 예시적인 시스템(100)에서, 클라이언트 디바이스(110)는 네트워크 디바이스(120)에 대한 통신의 범위 내에 있을 수 있다. 클라이언트 디바이스(110)는 랩탑, 스마트폰, 어플라이언스, 또는 네트워크 디바이스(120)에 의해 아직 인가되지 않은 임의의 다른 디바이스일 수 있다. 네트워크 디바이스(120)는 또한, 등록자 디바이스로 지칭될 수 있다. 예로서, 네트워크 디바이스(120)는 WLAN 액세스 포인트일 수 있다. 클라이언트 디바이스(110)가 네트워크 디바이스(120)에 대해 프로비저닝 된 후, 클라이언트의 디바이스(110)는 네트워크 디바이스(120)와 통신가능하게 커플링된 것으로 간주될 수 있다. 일부 실시예들에서, 클라이언트 디바이스(110)가 네트워크 디바이스(120)에 의해 적절하게 프로비져닝될 때까지, 클라이언트 디바이스(110)는 가입자 디바이스로 지칭될 수 있다.

[0114] [00128] 가상적인 시나리오에서, 집을 방문한 친구 또는 가족 멤버(즉, 클라이언트 디바이스의 사용자임)는 액세스 포인트를 통해 WLAN에 액세스하기를 원할 수 있다. 대안적으로, WLAN에 대한 액세스는, 호텔, 컨벤션 센터 또는 공공 공간에서 게스트들을 위해 제공될 수 있지만, 인증에 기초하여 제한된다. 전통적인 WLAN 배치들에서, 클라이언트 디바이스(110)의 사용자는, 클라이언트 디바이스(110)가 네트워크 디바이스(120)에 적절하게 인증할 수 하도록 패스코드 또는 다른 정보를 입력하도록 요구받을 수 있다. 본 개시에 따라, 클라이언트 디바이스(110)는, 일부 실시예들에서, 사용자가 패스코드 또는 네트워크 키를 수동으로 입력하는 것을 요구하지 않고, 프로비져닝될 수 있다. 더욱이, WLAN의 보안은, 오직 인가된 사용자들만이 WLAN에 액세스하게 허용되도록

유지될 수 있다.

[0115] [00129] 도 1에 도시된 바와 같이, 구성기 디바이스(130)는 클라이언트 디바이스(110)의 프로비져닝을 지원할 수 있다. 구성기 디바이스(130)는 컴퓨팅 디바이스(예컨대, 랩탑, 개인 컴퓨터, 태블릿, 스마트폰, 네트워킹된 어플라이언스 등)일 수 있다. 가정적인 예에서, 구성기 디바이스(130)는 카메라, 프로세서 및 네트워크 인터페이스를 가진 모바일 디바이스이다. 구성기 디바이스(130)는 네트워크 디바이스(120)에 통신가능하게 커플링된다. 클라이언트 디바이스(110)가 네트워크 디바이스(120)에 등록되게 하기 위해, 구성기 디바이스(130)는 클라이언트 디바이스(110)와 관련된 클라이언트 공개 키를 획득하고 이를 네트워크 디바이스(120)에 제공할 수 있다.

[0116] [00130] 본 개시에서, 공개 키들 및 개인 키들을 지칭할 때, 각각의 공개 키 및 개인 키가 쌍으로 관련될 수 있다. 쌍인 개인 키 및 공개 키는 수학적으로 링크되지만 서로 상이한 두 키를 형성할 수 있다. 공개 키는 정보를 암호화하거나 디지털 서명을 검증하기 위해 사용될 수 있다. 개인 키는 정보를 복호화하거나 디지털 서명을 생성하기 위해 사용될 수 있다. 당업자는 다른 명칭들, 예컨대 공개 키 암호문 또는 비대칭 암호문에 의해 이러한 개념을 인식할 수 있다. 다른 보안 메커니즘들이 공개 키 암호화에 부가하여, 또는 이를 대신하여 사용될 수 있음을 이해해야 한다. 예를 들어, 동적 키들, 키 로테이션, 해싱 알고리즘들 또는 다른 메커니즘들이 본 명세서에 설명된 공개 키 및 개인 키 메커니즘에 부가하여, 또는 대안적으로 사용될 수 있다. 간략화를 위해, 공개 키 암호문은 예시적인 실시예로서 본 명세서에 설명된다.

[0117] [00131] 도 1에 도시된 바와 같이, 클라이언트 공개 키(154)는, 클라이언트 공개 키(154)가 인코딩되어 있는 QR(Quick Response) 코딩된 이미지(160)의 픽쳐를 취함으로써 획득될 수 있다. 구성기 디바이스(130)는 클라이언트 공개 키(154)를 디코딩하고 등록 메시지(156)에서 클라이언트 공개 키(154)를 네트워크 디바이스(120)에 제공한다. 네트워크 디바이스(120)는 등록 프로세스에서 클라이언트 공개 키(154) 및/또는 추가의 인증(158로 도시됨)을 사용할 수 있어서, 클라이언트 디바이스(110)는 네트워크를 통한 센서티브 데이터를 전달하지 않고 네트워크에 통신가능하게 부가된다.

[0118] [00132] 구성기 디바이스(130)는 네트워크 디바이스(120)의 등록 성능들을 모바일 디바이스로 확장할 수 있다. 예를 들어, 네트워크 디바이스(120)에는 카메라, 스캐너, 단거리 라디오 인터페이스 또는 NFC(near field communications) 태그 판독기 성능들이 갖춰지지 않을 수 있다. 더욱이, 네트워크 디바이스(120)는 고정된 위치 또는 접속 곤란 위치에 장착될 수 있다. 그럼에도 불구하고, 구성기 디바이스(130)는 모바일 디바이스일 수 있고, 네트워크에 부가되는 클라이언트 디바이스(110)의 클라이언트 공개 키를 획득하기에 더 적절할 수 있다. 구성기 디바이스(130)는 클라이언트 디바이스(110)를 등록하는데 사용하기 위해 네트워크 디바이스(120)로 클라이언트 공개 키를 제공할 수 있다.

[0119] [00133] 상기 주어진 가정의 시나리오의 예를 참조하면, 가족 멤버 또는 친구는 자신들의 클라이언트 디바이스의 클라이언트 공개 키를 제공(예를 들어, 인코딩된 이미지를 디스플레이)하는 애플리케이션을 단순히 론칭할 수 있다. 가정의 주인은 구성기 디바이스(130)로서 역할을 하는 모바일 디바이스를 사용하여 클라이언트 공개 키를 검출함으로써 클라이언트 디바이스를 네트워크에 부가할 수 있다. 유사하게, 호텔 또는 컨벤션의 게스트들은, 패스코드들 또는 복잡한 수동 구성의 필요 없이, 지원된 등록을 사용하여 무선 네트워크 서비스들에 대한 액세스가 그랜트될 수 있다.

[0120] [00134] 일 실시예에서, 디바이스가 구성기 디바이스(130)로서 동작할 수 있는 한편, 다른 실시예에서는, 클라이언트 디바이스(110)로서 동작할 수 있다는 것이 이해되어야 한다. 예로서, 개인 A의 소유인 모바일 디바이스는 개인 A의 집에서 네트워크 디바이스(120)를 위한 구성기 디바이스(130)로서 개인 A의 집에서 사용될 수 있다. 개인 A의 소유인 동일한 모바일 디바이스는, 이 모바일 디바이스가 개인 B의 집에 있을 때 클라이언트 디바이스(110)로서 그리고 개인 B의 집에서 상이한 네트워크 디바이스(미도시)를 위해 사용될 수 있다. 끝으로, 모바일 디바이스는 또한, 모바일 디바이스가 핫스폿 또는 피어-투-피어(P2P) 그룹 오너로서 사용될 때와 같이, 네트워크 디바이스(120)로서 동작할 수 있다. 일부 실시예들에서, 네트워크 디바이스(120) 및 구성기 디바이스(130)는 동일한 물리적 장치에서 콜로케이트 또는 구현될 수 있다. 예를 들어, 모바일 디바이스는 모바일 핫스폿을 다른 디바이스들에 제공할 수 있다. 동시에, 모바일 디바이스는, 새로운 클라이언트 디바이스들의 등록을 지원하기 위해 구성기 디바이스(130)로서 동작할 수 있다.

[0121] [00135] 전술한 가정적인 시나리오들은 예시적인 목적들을 위해 제공된다. 이러한 개시의 많은 대안적인 사용들이 고려될 수 있다는 것이 주목된다. 전술한 설명들에서, 새로운 클라이언트 디바이스의 프로비져닝을 지원하기 위해 구성기 디바이스를 사용할 수 있는 몇몇 실시예들이 설명되었다.

[0122] [00136] 도 2는 추가의 세부사항을 갖는 예시적인 시스템(200)을 도시한다. 도 1과 유사하게, 클라이언트 디바이스(110)는 네트워크 디바이스(120)에 대한 통신의 범위 내에 있을 수 있다. 이러한 예에서, 구성기 디바이스(130)는 클라이언트 디바이스(110)를 프로비져닝하여 네트워크 디바이스(120)를 돕는다.

[0123] [00137] 구성기 디바이스(130)는 구성기 디바이스(130)와 네트워크 디바이스(120) 사이에서 신뢰 관계(225)를 구축할 수 있다. 신뢰 관계(225)의 예들은 도 7을 참조하여 추가로 설명된다. 신뢰 관계(225)는 구성기 디바이스(130)와 네트워크 디바이스(120) 사이의 통신들을 인증 및/또는 암호화하기 위한 보안 키들의 사용을 포함한다. 또한, 신뢰 관계(225)는 구성기 디바이스(130)가 새로운 디바이스들, 예컨대, 클라이언트 디바이스(110)의 프로비져닝을 돕도록 인가되는 관계를 나타낸다.

[0124] [00138] 신뢰 관계를 구축하는 것은, 구성기 디바이스(130)가 신뢰 관계(225)를 위한 신뢰 관계 키를 셋업하기 위한 단계들을 포함할 수 있다. 예를 들어, 구성기 디바이스(130)는 네트워크 디바이스(120)와 관련된 네트워크 공개 키를 결정할 수 있다. 구성기 디바이스(130)는 구성기 공개 키 및 대응하는 구성기 개인 키를 가질 수 있다. 구성기 디바이스(130)는 네트워크 공개 키와 구성기 개인 키에 적어도 부분적으로 기초하여 신뢰 관계 키를 결정할 수 있다. 유사하게, 네트워크 디바이스(120)는 네트워크 개인 키와 구성기 공개 키에 적어도 부분적으로 기초하여 신뢰 관계 키를 결정할 수 있다.

[0125] [00139] 도 2에서, 구성기 디바이스(130)는 클라이언트 디바이스(110)와 관련된 클라이언트 공개 키를 획득(라인 254로 도시됨)한다. 클라이언트 디바이스(110)는 클라이언트 공개 키(254) 및 대응하는 클라이언트 개인 키를 가질 수 있다. 구성기 디바이스(130)는, 예를 들어, 대역 외 통신 채널 또는 검출을 이용함으로써, 클라이언트 공개 키(254)를 획득할 수 있다. 예를 들어, 구성기 디바이스(130)는 클라이언트 디바이스(110)와 관련된 이미지를 스캔하기 위해 카메라를 사용할 수 있다. 이미지는 2D 또는 3D 이미지일 수 있다. 예를 들어, 이미지는 QR(Quick Response) 코드 또는 바코드일 수 있다. 이미지는 클라이언트 디바이스(110) 또는 클라이언트 디바이스(110)와 관련된 패킹에 첨부(affix)될 수 있다. 다른 타입들의 시각적, 오디오, 또는 전기적 대역 외 통신 채널은 클라이언트 공개 키(254)를 획득하기 위해 구성기 디바이스(130)에 의해 사용될 수 있다. 간략화를 위해, 본 명세서의 예들은 클라이언트 공개 키가 인코딩되어 있는 이미지에 관하여 설명된다.

[0126] [00140] 일부 실시예들에서, 이미지는 정적이거나 일시적일 수 있다. 예를 들어, 클라이언트 디바이스(110)에는 디스플레이가 장착될 수 있고 등록의 상이한 인스턴스들을 위한 또는 상이한 네트워크들을 위한 상이한 이미지를 생성할 수 있다. 클라이언트 공개 키(254)는, 카메라, 스마트폰, 스캐너 또는 구성기 디바이스(130)의 다른 머신 판독 가능 코드 판독기로 머신 판독 가능 이미지(예를 들어, QR 코드)를 스캐닝 및 디코딩함으로써 결정될 수 있다. 머신 판독 가능 이미지, 예컨대 QR 코드를 이용하는 것은 클라이언트 키를 비교적 빠르게 결정하는 것을 돕고, 클라이언트 공개 키의 획득 또는 판독과 관련된 인간 에러를 감소시킬 수 있다. 또 다른 실시예에서, 클라이언트 공개 키(254)를 포함하는 NFC(near field communication) 태그(미도시)가 제조자에 의해 제공될 수 있고 클라이언트 디바이스(110)에 부착 또는 이에 근접하게 위치될 수 있다. NFC 태그는 클라이언트 공개 키(254)를 결정하기 위해 NFC 태그 판독기에 의해 판독될 수 있다. NFC 태그를 사용하는 것은 클라이언트 디바이스(110)의 클라이언트 공개 키(254)를 결정하는데 있어서 에러들을 또한 감소시킬 수 있다.

[0127] [00141] 일단 구성기 디바이스(130)가 클라이언트 공개 키(254)를 획득하면, 구성기 디바이스(130)는 등록 메시지(256)에서 클라이언트 공개 키(254)를 네트워크 디바이스(120)에 전송할 수 있다. 일 실시예에서, 등록 메시지(256)를 전송하기 전에, 구성기 디바이스(130)는 네트워크 디바이스(120)에 요청 메시지를 전송함으로써 등록을 개시할 수 있다. 요청 메시지(미도시)는 네트워크 디바이스(120)가 등록을 위한 넌스를 제공하게 할 수 있다. 넌스는 네트워크 디바이스(120)에 의해 제공될 수 있는 랜덤 또는 의사랜덤 수일 수 있다. 구성기 디바이스(130)는 넌스를 사용하여 클라이언트 공개 키(254)를 수반하기 위한 서명을 준비할 수 있다. 서명은 또한 구성기 디바이스(130)가 등록 메시지(256)를 전송하도록 인가된 것을 증명하는 암호화 및/또는 서명 프로세스에 기초할 수 있다. 등록 메시지(256)는 클라이언트 공개 키(254) 및 서명은 물론 다른 정보를 포함할 수 있다. 예를 들어, 등록 메시지(256)는 클라이언트 공개 키(254)가 어떻게 획득되었는지에 대한 정보, 타임 스탬프, 네트워크 디바이스(120)의 식별자, 등록 요청 식별자 및/또는 다른 정보를 포함할 수 있다. 일 실시예에서, 서명, 넌스 또는 이 둘 모두는 신뢰 관계 키를 사용하여 암호화될 수 있다.

[0128] [00142] 네트워크 디바이스(120)가 등록 메시지(256)를 수신할 때, 네트워크 디바이스(120)는, 네트워크 디바이스(120)와 신뢰 관계(225)를 갖는 적절하게 인가된 구성기 디바이스(130)로부터 유래한 것으로 서명을 검증할 수 있다. 서명이 검증되면, 네트워크 디바이스(120)는 클라이언트 디바이스(110)와 직접 등록을 완료하기 위해 등록 메시지(256)로부터 클라이언트 공개 키(254)를 사용할 수 있다. 예를 들어, 일 실시예에서, 네트워크 디

바이스(120)는, 조사 요청 메시지에 응답하여 조사 응답 메시지(미도시)를 송신함으로써 등록을 개시할 수 있다. 조사 응답 메시지는 클라이언트 공개 키의 해시 또는 다른 파생물을 포함할 수 있다. 다른 실시예에서, 클라이언트 디바이스(110)와 통신 세션을 구축하기 위해 네트워크 디바이스(120)는 등록을 개시하고 초기 무선 연계를 수행할 수 있으며, 이를 통해 추가의 인증 및 구성이 교환될 수 있다.

[0129] [00143] 클라이언트 디바이스(110)의 등록 및 인증은 네트워크 디바이스(120)와 클라이언트 디바이스(110) 사이의 인증 절차를 개시할 수 있다. 예를 들어, 네트워크 디바이스(120)는 인증 요청 메시지(258)를 클라이언트 디바이스(110)에 전송할 수 있다. 인증 요청 메시지(258)는 네트워크 공개 키는 물론 네트워크 디바이스에 의해 제공된 넌스("네트워크 제공된 넌스")를 포함할 수 있다. 클라이언트 디바이스(110)는 제 2 넌스(또는 "클라이언트 제공 넌스")를 생성하고, 그 다음 네트워크 제공 넌스, 클라이언트 제공 넌스, 네트워크 공개 키, 및 클라이언트 개인 키를 사용하여 공유 키를 생성할 수 있다. 다음으로, 클라이언트 디바이스(110)는 인증 응답 메시지(260)를 네트워크 디바이스(120)로 되전송할 수 있다. 인증 응답 메시지(260)는 클라이언트 제공 넌스 및 클라이언트 제공 넌스의 메시지 인증 코드(MAC)를 포함할 수 있다. 클라이언트 제공 넌스의 MAC는 (예를 들어, 공유 키를 사용하여 준비되는) 클라이언트 제공 넌스의 암호화 해시 함수일 수 있다.

[0130] [00144] 네트워크 디바이스(120)는 유사하게 공유 키를 준비할 수 있다. 공유 키는 네트워크 제공 넌스, 클라이언트 제공 넌스, 클라이언트 공개 키, 및 네트워크 개인 키로부터 생성될 수 있다. 네트워크 디바이스(120)는, 네트워크 디바이스(120)가 클라이언트 제공 넌스 및 공유 키로부터 인증 응답 메시지(260)에 포함된 MAC와 동일한 MAC를 생성하면, 네트워크 디바이스(120)는 클라이언트 디바이스(110)에 의해 생성되는 것과 동일한 공유 키를 갖는 것을 검증할 수 있다.

[0131] [00145] 일단 공유 키의 존재가 검증되면, 네트워크 디바이스(120)는 클라이언트 디바이스(110)가 등록된 것으로 간주할 수 있다. 네트워크 디바이스(120)는, 구성, 네트워크 연계 또는 추가의 인증과 같은, 네트워크 디바이스(120)와 클라이언트 디바이스(110) 사이의 추가의 통신(도 2에 도시되지 않음)을 위해 공유 키를 사용할 수 있다. 예를 들어, 네트워크 디바이스(120)는 구성 데이터를 클라이언트 디바이스(110)에 전송할 수 있다. 구성 데이터는 무선 액세스를 위한 세팅들, 예컨대, 무선 액세스 포인트의 SSID, 채널 또는 전력 세팅들을 포함할 수 있다. 구성 데이터는 또한, 보안, 애플리케이션 층, 또는 네트워크 디바이스(120)를 통해 통신하기 위해 클라이언트 디바이스(110)에 의해 사용되는 다른 세팅들에 대한 추가의 정보를 포함할 수 있다.

[0132] [00146] 등록 이후에, 일 실시예에서, 클라이언트 디바이스(110) 및 네트워크 디바이스(120)는 추가의 인증(도 2에 미도시)을 수행할 수 있다. 예를 들어, 4 방향 핸드쉐이크 절차가 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이에서 수행되어 클라이언트 디바이스(110)의 인증 및/또는 연계를 완료할 수 있다. 쌍 마스터 키(PMK:pairwise master key)는 후속 WPA(Wi-FiTM Protected Access) 핸드쉐이크 및 구성 메시지들에 대해 사용될 수 있다. 일 실시예에서, 네트워크 제공 넌스, 클라이언트 제공 넌스, 네트워크 공개 키, 및 클라이언트 개인 키에 기초하여 생성된 공유 키(SK)는 PMK로 사용될 수 있다. 대안적으로, PMK는 SK로부터 도출될 수 있다. 클라이언트 디바이스는 입력 변수로서 적어도 SK를 갖는 미리 정해진 함수 또는 알고리즘을 사용하여 PMK를 도출할 수 있다. 유사하게, 네트워크 디바이스는 미리 정해진 함수 또는 알고리즘 및 동일한 SK를 사용하여 PMK를 도출할 수 있다. 예를 들어, PKM는 SK의 해시일 수 있다. 이어, PMK는 클라이언트 디바이스와 네트워크 디바이스 사이의 4 방향 핸드쉐이크 또는 추가의 연계/구성 단계들을 위해 사용될 수 있다.

[0133] [00147] 도 3은, 일부 실시예들에 따라, 구성기 디바이스(예컨대, 구성기 디바이스(130))에 의해 수행될 수 있는 동작들의 예시적은 흐름(300)을 도시한다. 블록(302)에서, 구성기 디바이스는 네트워크의 네트워크 디바이스와 신뢰 관계를 구축할 수 있다. 신뢰 관계를 구축하는 예들은 도 2 및 7에 제공된다.

[0134] [00148] 블록(304)에서, 구성기 디바이스는 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정할 수 있다. 예를 들어, 클라이언트 공개 키를 결정하는 것은, 대역 외 매체를 사용하여 클라이언트 공개 키를 검출하기 위해, 카메라, 마이크로폰, 광 검출기, 스캐너, 단거리 라디오 주파수 인터페이스(예컨대, 블루투스 TM 또는 NFC) 또는 구성기 디바이스의 다른 센서를 사용하는 것을 포함할 수 있다. 일부 실시예들에서, 클라이언트 공개 키를 결정하기 위해 사용되는 방법은, 의도되지 않은 원격 액세스 또는 보안 위반을 방지하기 위해, 구성기 디바이스와 클라이언트 디바이스 사이의 근접성을 요구할 수 있다.

[0135] [00149] 블록(308)에서, 구성기 디바이스는 신뢰 관계에 따라 클라이언트 디바이스와 관련된 클라이언트 공개 키를 전송할 수 있고, 클라언트 공개 키는 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 사용된다.

[0136] [00150] 도 4는 본 개시의 실시예들에 따라, 클라이언트 공유 키를 네트워크 디바이스에 제공하기 위해 구성기 디바이스를 사용하는 지원된 디바이스 프로비져닝의 예를 예시하는 메시지 흐름도이다. 도 4의 예시적인 메시지 흐름(400)에서, 구성기 디바이스(130)는 단방향 대역 외 통신 매체를 사용하여 클라이언트 공개 키(414)를 획득할 수 있다. 구성기 디바이스(130)는 네트워크 디바이스(120)와 신뢰 관계(402)를 구축하였다. 일부 실시예들에서, 구성기 디바이스가 클라이언트 디바이스(110)의 클라이언트 공개 키를 획득하기 이전에, 신뢰 관계(402)가 사전 구성될 수 있다. 대안적으로, 신뢰 관계(402)는, 구성기 디바이스가 클라이언트 디바이스(110)와 관련된 클라이언트 공개 키를 획득한 이후 또는 이에 응답하여 구축될 수 있다.

[0137] [00151] 신뢰 관계(402)를 구축할 때, 네트워크 디바이스(120)는 구성기 디바이스(130)에 관한 정보(404), 예컨대 구성기 공개 키, 식별자, 인가 기간 등을 저장할 수 있다. 저장된 정보(404)는, 예컨대, 구성기 디바이스(130)의 인가를 검증하기 위해, 그리고/또는 클라이언트 디바이스(110)의 등록 및 인증을 돕기 위해, 추후에 사용될 수 있다. 예를들어, 저장된 정보(404)는 등록 메시지에서 구성기 디바이스(130)에 의해 제공된 서명을 복호화 또는 검증하기 위해 사용될 수 있다.

[0138] [00152] 구성기 디바이스(130)는 클라이언트 디바이스(110)의 클라이언트 공개 키(414)를 획득하기 위해 대역 외 매체를 사용할 수 있다. 예를 들어, 클라이언트 공개 키는 카메라 및 이미지, 단거리 라디오 주파수 신호들(예컨대, 블루투스 또는 NFC) 또는 다른 대역 외 매체를 통해 획득될 수 있다. 일부 실시예들에서, 구성기 디바이스(130)는 클라이언트 공개 키(414)를 획득하기 위해 클라이언트 디바이스(110)에 선택적으로 질의(412)할 수 있다. 일부 실시예들에서, 구성기 디바이스(130)는, 예컨대, 클라이언트 공개 키(414)가 코딩된 이미지를 스캐팅함으로서 획득될 때, 클라이언트 디바이스(110)에 질의(412)하지 않을 수 있다. 클라이언트 공개 키는 정적이거나 일시적일 수 있다. 클라이언트 공개 키가 일시적이면, 클라이언트 디바이스(110)는 클라이언트 공개 키를 생성하고 질의(412)에 응답하여 클라이언트 공개 키를 구성기 디바이스(130)에 제공할 수 있다. 다른 예들에서, 클라이언트 공개 키는 정적일 수 있다. 대역 외 매체가 양방향 통신을 지원하지 않는다면, 구성기 디바이스(130)는 센서, 마이크로폰, 광 검출기, 카메라 또는 구성기 디바이스의 다른 성능들을 이용하여 클라이언트 공개 키를 간단히 검출할 수 있다.

[0139] [00153] 구성기 디바이스(130)는 네트워크 디바이스(120)에 등록 요청(420)을 전송함으로써 등록 세션을 개시할 수 있다. 네트워크 디바이스(120)는 넌스를 갖는 응답(422)(이는 또한 등록 넌스 또는 등록 세션 식별자로 지칭될 수 있음)을 전송할 수 있다. 넌스는 네트워크 디바이스(120)에 의해 제공될 수 있는 랜덤 또는 의사랜덤 수일 수 있다. 일부 실시예들에서, 넌스는 구성기 디바이스(130)에 의해 생성되어 등록 요청(420)에 제공되며 응답(422)에 의해 확인응답될 수 있다. 넌스의 사용은, 비인가된 데이터를 도입하기 위해 이전에 사용된 메시지 교환을 사용하는 보안 위반인 소위 응답 어택들을 방지할 수 있다.

[0140] [00154] 구성기 디바이스(130)는 등록 메시지(424)에서 클라이언트 디바이스(110)의 클라이언트 공개 키를 네트워크 디바이스(120)에 제공할 수 있다. 전술한 바와 같이, 등록 메시지(424)는 다른 정보, 예컨대 등록 넌스로부터 도출되는 서명을 포함할 수 있다. 서명은 클라이언트 디바이스(110)의 등록을 진행하기 전에, 구성기 디바이스(130)의 권한을 검증(검증 절차(426)로 도시됨)하기 위해 사용될 수 있다. 검증된다면, 클라이언트 공개 키는 인증 프로세스에서 사용하기 위해 저장될 수 있다.

[0141] [00155] 등록 메시지(424) 및 서명의 검증에 응답하여, 네트워크 디바이스(120)는 등록 절차(430)를 수행할 수 있다. 등록 절차는 비컨 메시지, 요청 메시지, 조사 응답 메시지, 인증 시작 메시지, 인증 개시 메시지, 연계 요청 및 연계 응답 중 하나 이상을 포함할 수 있다. 이러한 메시지들은 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 초기 통신을 구축하기 위해 사용되는 발견 단계들로 지칭될 수 있고, 이를 통해 추가의 인증 및 구성이 발생할 수 있다. 일례에서, 등록 절차(430)는 인증 프로토콜, 예컨대 확장 가능한 인증 프로토콜(EAP)에 의해 사용될 수 있는 인증 채널의 구축을 포함한다.

[0142] [00156] 예시적인 인증 프로스세는, 인증 요청 메시지(432)(인증 요청 메시지(258)와 유사함)와 인증 응답 메시지(434)(인증 응답 메시지(260)와 유사함)를 포함할 수 있다. 도 2에 도시된 바와 같이, 인증 프로세스는, 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 공유 키를 결정하기 위해, (인증 요청 메시지(432)에서) 네트워크 제공 넌스 및 (인증 응답 메시지(434)에서) 클라이언트 제공 넌스의 사용을 포함할 수 있다.

[0143] [00157] 인증 요청 메시지(432)와 인증 응답 메시지(434) 이후에, 구성 프로세스가 발생할 수 있다. 예를 들어, 네트워크 디바이스(120)는 구성 데이터(436)를 클라이언트 디바이스(110)에 송신할 수 있다. 구성 데이터(436)는 정보, 예컨대 액세스 포인트의 SSID, 무선 채널 정보(이를테면, 채널 식별자), 애플리케이션 층 키 등을 포함할 수 있다. 일례에서, 구성 데이터(436)는 공유 키에 적어도 부분적으로 기초하여 보호될 수 있다.

예를 들어, 구성 데이터(436)는 공유 키 또는 공유 키의 파생물을 사용하여 암호화될 수 있다.

[0144] [00158] 공유 키는 또한, 네트워크 액세스에 대해 사용되는 후속 인증 프로세스에서 사용될 수 있다. 예를 들어, 추가의 인증(도 1에 미도시)은 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이에서 수행되는 4 방향 핸드쉐이크 절차를 포함할 수 있다. 4 방향 핸드쉐이크 절차는, 공유 키로부터 도출되는 쌍 마스터 키에 기초할 수 있다.

[0145] [00159] 네트워크 디바이스(120)는, 클라이언트 디바이스(110)가 네트워크에 대해 성공적으로 등록되었고 그리고/또는 네트워크에 인증되었음을 확인해 주기 위해 확인 메시지(440)를 구성기 디바이스(130)에 전송할 수 있다. 확인 메시지(440)에 응답하여, 구성기 디바이스(130)는, 네트워크 등록 및/또는 인증이 성공적으로 완료되었음을 사용자에게 알리기 위해 시각적, 청각적 및/또는 다른 신호를 제공할 수 있다.

[0146] [00160] 도 5는 본 개시의 실시예들에 따라, 클라이언트 디바이스가 디폴트 채널을 모니터링하는 지원된 디바이스 프로비져닝의 예를 예시하는 메시지 흐름도이다. 도 5의 예시적인 메시지 흐름(500)에서, 클라이언트 디바이스(110)는 일시적인 디폴트 채널을 통해 구성기 디바이스(130) 또는 네트워크 디바이스(120)에 의해 프로비져닝된다. 구성기 디바이스(130)는 네트워크 디바이스(120)와 신뢰 관계(402)를 구축하였다. 신뢰 관계(402)를 구축한 후, 구성기 디바이스(130)는 클라이언트 디바이스(110)의 클라이언트 공개 키를 획득(414로 도시됨)하기 위해 대역 외 매체를 사용할 수 있다. 예를 들어, 구성기 디바이스(130)는 클라이언트 디바이스(110)와 관련된 QR 코드를 스캐닝할 수 있다. 구성기 디바이스(130)는 클라이언트 공개 키를 갖는 등록 메시지(424)를 네트워크 디바이스(120)에 전송할 수 있다. 이 예에서, 클라이언트 디바이스(110)는 디폴트 채널을 사용하여 프로비져닝된다. 예를 들어, 클라이언트 디바이스(110)는 디바이스 프로비져닝을 개시하는 비컨 메시지에 대해 디폴트 채널을 모니터링(521)할 수 있다. 일 실시예에서, 클라이언트 디바이스(110)는 자신이 아직 네트워크 연결을 갖지 않는다면 디폴트 채널을 모니터링할 수 있다. 대안적으로, 클라이언트 디바이스(110)는 클라이언트 디바이스(110)를 프로비젼하려고 하는 임의의 네트워크 디바이스로부터 비컨 메시지에 대해 디폴트 채널을 주기적으로 모니터링할 수 있다.

[0147] [00161] 네트워크 디바이스(120) 또는 구성기 디바이스(130) 중 하나는, 비컨 메시지를 전송하기 위해 디폴트 채널을 일시적으로 액세스할 수 있다. 예를 들어, 네트워크 디바이스(120)는 디폴트 채널을 통해 비컨 메시지(526)를 전송할 수 있다. 다른 예에서, 구성기 디바이스(130)는 디폴트 채널을 통해 비컨 메시지(528)를 전송할 수 있다. 비컨 메시지에 추가하여 또는 이를 대신하여, 발견 메시지들의 다른 타입들이 사용될 수 있다. 디바이스 프로비져닝(예를 들어, 등록 및/또는 인증)은 앞서 설명한 대로 계속될 수 있다(도 4의 메시지들의 대응하는 설명들(430-440)을 참조).

[0148] [00162] 도 6은 본 개시의 실시예들에 따라, 구성기 디바이스가 등록 키를 클라이언트 디바이스에 제공하는 지원된 디바이스 프로비져닝의 예를 예시하는 메시지 흐름도이다. 도 6의 예시적인 메시지 흐름(600)에서, 구성기 디바이스(130)는 양방향 대역 외 통신 매체를 사용하여 클라이언트 공개 키(614)를 획득할 수 있다. 이 예에서, 구성기 디바이스(130)는 또한, 네트워크 공개 키(630)(이는 또한 등록 공개 키로 지칭될 수 있음)를 제공할 수 있다.

[0149] [00163] 구성기 디바이스(130)는 네트워크 디바이스(120)와 신뢰 관계(602)를 구축하였다. 신뢰 관계(602)를 구축한 후, 네트워크 디바이스(120)는 구성기 디바이스(130)에 관한 정보(604), 예컨대 구성기 공개 키, 식별자, 인가 기간 등을 저장할 수 있다.

[0150] [00164] 구성기 디바이스(130)는 대역 외 매체 및 대역 외 인터페이스(605)를 통해 클라이언트 디바이스(110)의 클라이언트 공개 키를 획득하기 위해 대역 외 인터페이스(606)를 사용할 수 있다. 도 6의 예에서, 대역 외 매체는 양방향 통신을 지원한다. 대역 외 매체는 통신 매체 -이 매체에 대해 네트워크 디바이스(120)가 액세스를 제어함-와 상이하다. 따라서, 클라이언트 디바이스(110) 및 구성기 디바이스(130)는 대안적인 통신 인터페이스, 예컨대 단거리 라디오 주파수 인터페이스, 피어-투-피어 무선 네트워킹, 직접 와이어링된 매체, 또는 양방향 통신을 지원하는 다른 통신 매체로 구성될 수 있다. 구성기 디바이스(130)는, 클라이언트 디바이스(110)의 클라이언트 공개 키를 획득하기 위해 질의 메시지(612)를 클라이언트 디바이스(110)에 전송할 수 있다. 질의 메시지(612)에 응답하여, 클라이언트 디바이스(110)는 클라이언트 공개 키를 포함하는 응답 메시지(614)로 응답한다.

[0151] [00165] 도 4의 메시지들(420-424)에 유사하게, 구성기 디바이스(130)는 등록 요청(620)을 네트워크 디바이스(120)에 전송하고, 넌스(이는 또한 등록 넌스 또는 등록 세션 식별자로 지칭됨)를 갖는 응답(622)을 수신하고,

등록 넌스에 적어도 부분적으로 기초하여 클라이언트 공개 키 및 서명을 갖는 등록 메시지(624)를 전송할 수 있다. 클라이언트 디바이스(110)의 등록을 진행하기 전에, 서명이, 구성기 디바이스(130)의 권한을 검증하기 위한 검증 절차(625)에서 사용될 수 있다. 검증된다면, 클라이언트 공개 키는 인증 프로세스에서 사용하기 위해 저장될 수 있다.

[0152] [00166] 도 6의 예에서, 네트워크 디바이스(120)는 구성기 디바이스(130)에 등록 키(626)를 제공할 수 있다. 등록 키(626)는 또한, 네트워크 디바이스(120)와 관련된 네트워크 공개 키로 지칭될 수 있다. 그러나 도 6의 예에서, 등록 키(626)는, 양방향 2단계 통신 매체를 사용하여 클라이언트 디바이스(110)에 전송하기 위해 구성기 디바이스(130)에 제공되는 1회 사용 등록 키이다. 구성기 디바이스(130)는 등록 키(630)를 클라이언트 디바이스(110)에 제공한다. 등록 키는 네트워크 디바이스(120)에 저장된 대응하는 개인 키를 갖는 공개 키일 수 있다. 일부 예들에서, 구성 디바이스(130)는 구성 디바이스(130)에 의해 앞서 인지된 네트워크 공개 키 또는 등록 키를 전송할 수 있다. 예로서, 네트워크 디바이스(120)는 신뢰 관계(602)를 구축한 후, 구성기 디바이스(130)에 등록 키를 제공할 수 있다. 등록 키는 만료 기간을 가질 수 있고 그리고/또는 특정 구성기 디바이스(130)에 고유할 수 있다. 대안적으로, 메시지(626)에 제공되면, 등록 키는 클라이언트 디바이스(110)에 한정적일 수 있다.

[0153] [00167] 631에서, 네트워크 디바이스(120)는 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 초기 통신을 구축하기 위해 발견 단계들을 수행할 수 있다. 발견 단계들은 등록 키를 이용하기 위해 변경될 수 있다. 예를 들어, 등록 키(또는 그 파생물)는 클라이언트 디바이스(110) 및/또는 네트워크 디바이스(120)의 식별을 검증하기 위한 방식으로서 조사 요청 메시지 또는 조사 응답 메시지에 사용될 수 있다. 대안적으로, 등록 키(또는 그 파생물)는 네트워크 디바이스(120)로부터의 비컨 메시지에 포함될 수 있다. 클라이언트 디바이스(110) 또는 네트워크 디바이스(120)의 아이덴티티가 검증될 수 없으면, 등록 프로세스는 종료될 수 있어서, 추가의 비필수적 통신 또는 인증이 프로세서 또는 네트워크 리소스들을 소비하는 것을 방지한다.

[0154] [00168] 도 2 및 4와 유사하게, 예시적인 인증 프로세스는 인증 요청 메시지(632) 및 인증 응답 메시지(634)를 포함할 수 있다. 도 4와는 상이하게, 도 6에서, 인증 요청 메시지(632)는 네트워크 공개 키를 포함하지 않을 수 있다. 구성기 디바이스(130)가 양방향 대역 외 통신 매체를 사용하여 클라이언트 디바이스(110)에 등록 키를 이미 제공했기 때문이다. 대신에, 인증 요청 메시지(632)는 네트워크 제공 넌스를 포함하지만, 네트워크 공개 키를 포함하지 않을 수 있다. 다음으로, 도 2 및 4에 도시된 바와 같이, 인증 프로세스는, 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 공유 키를 결정하기 위해, (인증 요청 메시지(632)에서) 네트워크 제공 넌스, (인증 응답 메시지(634)에서) 클라이언트 제공 넌스, 및 이들 각각의 개인 키들 및 다른 공개 키의 사용을 포함할 수 있다. 636에서, 구성 프로세스는 네트워크 디바이스(120)로부터 클라이언트 디바이스(110)로의 구성 데이터의 전송을 포함할 수 있다.

[0155] [00169] 네트워크 디바이스(120)는, 클라이언트 디바이스(110)가 네트워크에 대해 성공적으로 등록되고 인증되었음을 확인해 주기 위해 확인 메시지(640)를 구성기 디바이스(130)에 전송할 수 있다. 확인 메시지(640)에 응답하여, 구성기 디바이스(130)는, 네트워크 등록 및 인증이 성공적으로 완료되었음을 사용자에게 알리기 위해 시각적, 청각적 및/또는 다른 신호를 제공할 수 있다.

[0156] [00170] 도 7은 구성기 디바이스(130)와 네트워크 디바이스(120) 사이의 신뢰 관계를 구축하기 위한 예시적인 메시지 흐름(700)을 도시한다. 네트워크 디바이스(120)는 구성기 지원 서비스 통지 메시지(702)를 송신할 수 있다. 구성기 지원 서비스 통지 메시지는 비컨 메시지 또는 오버헤드 메시지의 일부일 수 있다. 예를 들어, 구성기 지원 서비스 통지 메시지는 네트워크 디바이스(120)의 성능들을 나타내는 메시지에 포함될 수 있다. 구성기 지원 서비스 통지 메시지(702)는, 본 개시에 설명된 바와 같이, 네트워크 디바이스(120)가 지원된 등록 및 인증의 사용을 지원한다는 것을 구성기 디바이스(130)에 나타낼 수 있다.

[0157] [00171] 구성기 디바이스(130)는 네트워크 디바이스(120)와 관련된 네트워크 공개 키를 획득하기 위해 대역 외 매체를 사용할 수 있다. 예를 들어, 구성기 디바이스(130)는, 네트워크 공개 키를 요청하기 위해 질의 메시지(708)를 네트워크 디바이스(120)에 전송할 수 있다. 네트워크 디바이스(120)는 메시지(709)에 응답하여 네트워크 공개 키를 제공할 수 있다. 대안적으로, 구성기 디바이스(130)는, 네트워크 공개 키를 검출하기 위해, 카메라, 바코드 스캐너, 단거리 라디오 주파수 인터페이스, 또는 NFC 태그 판독기를 간단하게 사용할 수 있다. 일례에서, 구성기 디바이스(130)는 머신 인코딩된 데이터를 갖는 이미지를 디코딩함으로써 네트워크 공개 키를 획득한다. 구성기 디바이스(130)는 또한, 다른 정보, 예컨대, 네트워크 디바이스의 식별자(ID) 또는 구성 정보를 포함할 수 있다. 일 실시예에서, 식별자는 네트워크 공개 키로부터 도출될 수 있다. 구성 정보는 디폴트 채널

정보를 포함할 수 있다.

[0158] [00172] 구성기 디바이스(130) 및 네트워크 디바이스(120)는 구성기 디바이스(130)와 네트워크 디바이스(120) 사이의 초기 통신을 구축하기 위해 발견 단계들(712, 714)을 수행할 수 있다. 발견 단계들(712, 714)은 도 4-6에 설명된 것들과 유사할 수 있다. 발견 단계들은 또한, 구성기 디바이스(130) 및 네트워크 디바이스(120)가 신뢰 관계의 구축을 계속해야 하는 지를 검증하기 위해 사용될 수 있다. 예를 들어, 구성기 디바이스(130)는 네트워크 디바이스의 ID를 포함하는 조사 요청 메시지를 송신할 수 있다. 네트워크 디바이스(120)는 ID가 네트워크 디바이스의 올바른 ID와 매치되는 지를 검증할 수 있고, 그 다음 조사 요청 메시지로 응답할 수 있다. 네트워크 디바이스(120)의 ID가 검증될 수 없다면, 네트워크 디바이스(120)는 구성기 디바이스(130)와의 통신을 중단하고, 그리고/또는 신뢰 관계가 구축되는 것을 방지할 수 있다.

[0159] [00173] 구성기 디바이스(130)는, 구성기 디바이스(130)가 네트워크 디바이스(120)에 대해 구성기 디바이스로서 역할을 하기 위해 권한을 원한다는 표시와 함께 인증 요청 메시지(716)를 네트워크 디바이스(120)에 전송할 수 있다. 인증 요청 메시지(716)는 구성기 공개 키 및 구성기 제공 넌스를 포함할 수 있다. 추가적으로, 인증 요청 메시지(716)는 다른 정보, 예컨대, 네트워크 공개 키를 획득하기 위해 사용되는 방법, 구성기 디바이스(130)의 식별자, 또는 다른 정보를 나타낼 수 있다.

[0160] [00174] 네트워크 디바이스(120)는, 신뢰 관계 키(625)를 결정하기 위해, 구성기 제공 넌스, 구성기 공개 키, 네트워크 제공 넌스, 및 네트워크 개인 키를 사용할 수 있다. 네트워크 디바이스(120)는 네트워크 제공 넌스를 암호화하기 위해 공유 키를 사용할 수 있다. 선택적으로, WLAN의 서비스 세트 식별자(SSID), 또는 다른 네트워크 구성 정보와 같은 다른 정보가 또한 네트워크 제공 넌스와 함께 암호화될 수 있다. 예를 들어, 네트워크 디바이스(120)는 SSID 및 네트워크 제공 넌스에 적어도 부분적으로 기초하여 MAC를 생성할 수 있다.

[0161] [00175] 인증 응답 메시지(718)에서, 네트워크 디바이스(120)는 네트워크 제공 넌스 및 MAC를 구성기 디바이스(130)에 제공한다. SSID가 MAC를 생성하기 위해 사용되면, SSID는 인증 응답 메시지(718)에 선택적으로 포함될 수 있다.

[0162] [00176] 구성기 디바이스(130)는, 신뢰 관계 키(722)를 결정하기 위해, 네트워크 제공 넌스, 구성기 제공 넌스, 구성기 개인 키, 및 네트워크 공개 키를 사용할 수 있다. 구성기 디바이스(130)는, 인증 응답 메시지(718)에서 구성기 생성 MAC가 네트워크 제공 MAC와 매칭되는 것을 검증하도록 MAC를 계산하기 위해 신뢰 관계 키를 사용할 수 있다.

[0163] [00177] 네트워크 디바이스(120)는 구성기 공개 키, 및 선택적으로 추후 사용을 위한 신뢰 관계 키를 저장(732)할 수 있다. 예를 들어, 구성기 공개 키는 인가된 구성기 디바이스들의 리스트에 저장될 수 있다. 구성기 공개 키는 제한된 시간 동안 저장될 수 있고 시간 기간의 만료 시 제거될 수 있다. 대안적으로, 구성기 디바이스는 자신이 더 이상 네트워크에 대해 구성기 디바이스로서 역할을 하지 않는다고 나타내는 메시지(미도시)를 전송할 수 있다. 그 다음 네트워크 디바이스는 구성기 공개 키 및 신뢰 관계 키를 제거할 수 있다. 네트워크 디바이스는 재부팅 또는 리셋 시, 모든 구성기 공개 키들을 제거하도록 구성될 수 있다. 또한, 네트워크 디바이스는 동시 승인된 구성기 디바이스들의 수를 제한할 수 있다.

[0164] [00178] 일 실시예에서, 신뢰 관계는 또한 구성 데이터를 교환하기 위해 사용될 수 있다. 예를 들어, 하나 이상의 구성 메시지들(742, 744)은 구성 데이터를 전달하기 위해 송신될 수 있다. 일례에서, 네트워크 디바이스(120)는 현재 구성 데이터(742)를 구성기 디바이스(130)에 송신할 수 있다. 다른 예에서, 구성기 디바이스(130)는 새로운 구성 데이터(744)를 네트워크 디바이스(120)에 송신할 수 있다.

[0165] [00179] 일례에서, 유사한 메시지들 및 절차들이 두 디바이스들 사이에서 피어-투-피어 환경에서 수행될 수 있다. 다시 말해서, 일 실시예에서, 도 7의 구성기 디바이스(130) 및 네트워크 디바이스(120)는, 위에서 설명된 신뢰 관계를 구축하기 위해 사용될 유사한 메시지들을 사용하여 피어-투-피어 관계를 구축하는 피어 디바이스들일 수 있다. 피어-투-피어 환경에서, 공개 키들을 교환하기 전에, 디바이스들은 피어-투-피어 발견 절차 및 그룹 협상을 수행할 수 있다. 종종, 피어-투-피어 환경들에서, 디바이스들 중 하나는, 설명된 네트워크 디바이스(120)와 유사한 기능을 갖는 그룹 관리자로서 역할을 할 수 있다.

[0166] [00180] 다른 실시예에서, 유사한 메시지들 및 절차들이, 직접 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 디바이스 프로비져닝을 위해 수행될 수 있다. 다시 말해서, 도 7의 구성기 디바이스(130)는, 네트워크 디바이스(120)와 관련된 네트워크에 대해 아직 프로비져닝되지 않은 클라이언트 디바이스로서 거동할 수 있다. 클라이언트 디바이스는 위에서 설명된 신뢰 관계를 구축하기 위해 사용될 유사한 메시지들을 사용하여

네트워크 연결을 구축하고 있을 수 있다.

[0167] [00181] 도 8은 디바이스 프로비져닝의 다른 예를 도시하며, 여기서, 클라이언트 디바이스(110) 및 네트워크 디바이스(120)가 예시된다. 클라이언트 디바이스(110)는 네트워크 디바이스(120)의 네트워크 공개 키를 획득(709)할 수 있다. 도 8에서, 네트워크 공개 키가 대역 외 매체를 통해 획득된다. 예를 들어, 클라이언트 디바이스(110)는 네트워크 디바이스(120)와 관련된 QR 코드를 스캔할 수 있고, 여기서 QR 코드는 이미지로 인코딩된 네트워크 공개 키를 포함한다. 네트워크 디바이스(120)는 네트워크 디바이스(120)로부터의 제 1 메시지(811)에 네트워크 공개 키(또는 그 파생물)를 포함시킬 수 있다. 예를 들어, 제 1 메시지(811)는 서비스 통지 메시지, 조사 응답, 오버헤드 메시지 또는 비컨 메시지일 수 있다. 일 실시예에서, 네트워크 공개 키의 파생물(예컨대, 해시)은 제 1 메시지(811)에 포함될 수 있다. 클라이언트 디바이스(110)는, 네트워크 공개 키(또는 파생물)를 갖는 제 1 메시지(811)를 갖는 채널을 식별할 때까지 복수의 채널들을 수동적으로 스캔할 수 있다. 이러한 방식에서, 클라이언트 디바이스(110)는 프로비져닝 프로세스를 계속하기 위해 적절한 채널을 식별할 수 있다. 프로비져닝 프로세스(712-744로 도시됨)는 도 7에 도시된 프로세스와 유사할 수 있다.

[0168] [00182] 도 8의 다른 실시예에서, 클라이언트 디바이스(110)는 네트워크 디바이스(120)에 의해 관리되는 채널을 식별하기 위해 복수의 채널들에서 능동 스캔을 사용할 수 있다. 클라이언트 디바이스(110)는 조사 요청 메시지(810)를 전송하고 (제 1 메시지(811)로서) 조사 응답을 수신할 수 있다. 조사 응답이 네트워크 공개 키(또는 네트워크 공개 키의 파생물)를 포함하면, 클라이언트 디바이스(110)는 이 채널을 디바이스 프로비져닝을 계속하기 위해 적절한 채널로서 식별할 수 있다.

[0169] [00183] 전술한 바와 같이, 도 7-8에 설명된 메시지들은, 구성기 디바이스에 대한 신뢰 관계의 구축, 피어-투-피어 네트워크의 생성, 또는 네트워크로의 새로운 클라이언트 디바이스의 연결을 포함하여, 다양한 시나리오들에 대해 사용될 수 있다. 도 7에서, 초기 발견 프로세스 이후, 두 디바이스들은 공개 키들을 교환한다. 공개 키들은, 일 디바이스를 다른 디바이스에 대해 프로비져닝하기 위해 사용되는 파생 키를 결정하기 위해 각각의 디바이스에 대해 개인 키들과 함께 사용된다. 앞선 도면들에서 주지되듯이, 제 3 디바이스(예를 들어, 구성기 디바이스(130))는 제 1 디바이스와 제 2 디바이스(예를 들어, 클라이언트 디바이스(110)와 네트워크 디바이스(120)) 사이에서 중개자로서 사용될 수 있다. 이하의 도면들은 구성기 디바이스(130)에 관해 앞서 설명된 것과 유사한 특성들을 수행하는 중개자 디바이스의 추가의 예들을 제공한다.

[0170] [00184] 도 9는 예시적인 시스템(900)을 도시하며, 여기서 구성기 디바이스의 기능은 네트워크 기반(예를 들어, "클라우드") 서비스와 같은 신뢰된 구성기 서비스(131)에서 구현될 수 있다. 도 9는 클라이언트 디바이스(110) 및 네트워크 디바이스(120)를 포함한다. 초기에, 클라이언트 디바이스(110)는 네트워크 디바이스(120)에 등록되지 않은 것으로 간주된다.

[0171] [00185] 대역 외 통신 매체를 사용하여, 클라이언트 디바이스(110)는 (제 1 메시지(914)에서) 클라이언트 공개 키를 신뢰된 구성기 서비스(131)에 제공한다. 신뢰된 구성기 서비스(131)는 (제 2 메시지(924)에서) 클라이언트 공개 키를 네트워크 디바이스(120)에 제공할 수 있다. 유사하게, 네트워크 디바이스(120)는 (제 3 메시지(916)에서) 네트워크 공개 키를 신뢰된 구성기 서비스(131)에 제공할 수 있다. 신뢰된 구성기 서비스(131)는 (제 4 메시지(926)에서) 네트워크 공개 키를 클라이언트 디바이스(110)에 제공할 수 있다.

[0172] [00186] 신뢰된 구성기 디바이스(131)는 공개 키 클리어링하우스 또는 키 인증기관으로서 서빙할 수 있다. 일 실시예에서, 클라이언트 디바이스(110) 및 네트워크 디바이스(120)는, 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 임의의 잠재적 연계에 앞서, 클라이언트 공개 키 및 네트워크 공개 키를 각각 제공할 수 있다. 예를 들어, 신뢰된 구성기 디바이스(131)는 다수의 클라이언트 디바이스들 및 네트워크 디바이스들의 공개 키를 저장하는 클라우드 기반 저장소일 수 있어서, 공개 키들의 분포를 간단히 관리함으로써 특정 클라이언트 디바이스와 특정 네트워크 디바이스 사이에 관계가 구축될 수 있다.

[0173] [00187] 일 실시예에서, 신뢰된 구성기 디바이스(131)는 클라이언트 디바이스(110) 및 네트워크 디바이스(120) 중 하나 또는 둘 모두와 신뢰 관계를 구축할 수 있다. 클라이언트 공개 키 및 네트워크 공개 키는 신뢰 관계에 따라 보안 통신 링크를 사용하여 제공될 수 있다.

[0174] [00188] 클라이언트 디바이스(110) 또는 네트워크 디바이스(120)는 신뢰된 구성기 서비스(131)로부터 수신된 공개 키를 기초로 등록 프로세스(931)를 개시할 수 있다. 도 4-8에 도시된 바와 같이, 등록 프로세스(931)는 발견 단계들을 포함할 수 있다. 발견 단계들 이후, 클라이언트 디바이스(110)는, 인증 요청 메시지(934)를 네트워크 디바이스(120)에 전송함으로써 인증 프로세스를 개시할 수 있다. 인증 요청 메시지(934)는 클라이언트 제

공 넌스를 포함할 수 있고, 선택적으로 클라이언트 디바이스(110)에 관한 추가 정보를 포함할 수 있다. 네트워크 디바이스(120)는 네트워크 제공 넌스를 생성할 수 있고, 공유된 키를 결정하기 위해 네트워크 제공 넌스, 클라언트 제공 넌스, 네트워크 개인 키, 및 (신뢰된 구성기 디바이스(131)로부터의) 클라이언트 공유 키를 사용할 수 있다. 인증 응답 메시지(932)에서, 네트워크 디바이스(120)는 공유 키에 적어도 부분적으로 기초하여 네트워크 제공 넌스는 물론 MAC를 포함할 수 있다.

[0175] [00189] 클라이언트 디바이스(110)는, 동일한 공유 키를 결정하기 위해, 네트워크 제공 넌스, 클라이언트 제공 넌스, 클라이언트 개인 키, 및 네트워크 공개 키를 사용할 수 있다. 공유 키는 MAC를 생성하고 클라이언트 생성 MAC를 수신된 MAC와 비교함으로써 검증될 수 있다.

[0176] [00190] 등록 및 인증 이후, 네트워크 디바이스(120)는 구성 데이터(952)를 클라이언트 디바이스(110)에 제공할 수 있다. 부가적으로, 추가 인증(예컨대, 4 방향 핸드쉐이크 또는 PMK의 구축)이 수행될 수 있다(미도시).

[0177] [00191] 도 10은 또 다른 예시적인 시스템(1000)을 도시하며, 여기서 구성기 서비스(131)는 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 인증을 도울 수 있다. 일례에서, 구성기 서비스(131)는 (예를 들어, 클라우드에서) 신뢰된 서비스일 수 있다. 일 실시예에서, 신뢰된 구성기 서비스(131)는 클라이언트 공개 키 및 네트워크 공개 키의 추가의 신뢰 증명을 제공할 수 있다. 증명은 개인 키를 사용하여 정보의 일부를 암호화함으로 인한 정보의 일부의 증명 또는 "서명"을 포함한다. 증명 프로세스의 결과로서, "증명서"가 생성될 수 있다.

[0178] [00192] 대역 외 통신 매체를 사용하여, 클라이언트 디바이스(110)는 (제 1 메시지(1014)에서) 클라이언트 공개 키를 신뢰된 구성기 서비스(131)에 제공한다. 신뢰된 구성기 서비스(131)는 클라이언트 증명서를 생성하기 위해 구성기 개인 키를 사용하여 클라이언트 공개 키를 서명할 수 있다. 클라이언트 증명서는 클라이언트 디바이스와 네트워크 디바이스에 인지될 있는 구성기 공개 키를 사용하여 검증될 수 있다.

[0179] [00193] 유사하게, 네트워크 디바이스(120)는 (제 2 메시지(1016)에서) 네트워크 공개 키를 신뢰된 구성기 서비스(131)에 제공할 수 있다. 신뢰된 구성기 디바이스(131)는 또한 구성기 개인 키로 네트워크 공개 키를 서명함으로써 네트워크 증명서를 생성할 수 있다.

[0180] [00194] 신뢰된 구성기 디바이스(131)는 구성기 공개 키 및 네트워크 증명서를 제 3 메시지(1024)로 네트워크 디바이스(120)에 전송할 수 있다. 구성기 공개 키는 또한, 증명서 인가(CA) 공개 키로 지칭될 수 있다. 신뢰된 구성기 디바이스(131)는 구성기 공개 키 및 클라이언트 증명서를 제 4 메시지(1026)에서 클라이언트 디바이스(110)에 전송할 수 있다. 따라서, 클라이언트 디바이스 및 네트워크 디바이스 각각은 구성기 공개 키는 물론 이들 자신의 공개 키의 구성기 증명된 사본을 가질 것이다. 클라이언트 증명서 및 네트워크 증명서 각각은 신뢰된 구성기 서비스(131)에 의해 제공된 서명을 포함할 수 있다. 서명은 구성기 개인 키 및 증명서의 일부에 기초하여 컴퓨팅될 수 있다. 예를 들어, 증명서의 데이터 부분은 메시지 다이제스트 또는 해시를 생성하기 위해 사용될 수 있다. 그 다음, 메시지 다이제스트 또는 해시는 서명을 생성하기 위해 구성기 개인 키를 사용하여 암호화될 수 있다. 서명은 증명서의 제 2 부분으로서 부가될 수 있다.

[0181] [00195] 클라이언트 디바이스(110) 또는 네트워크 디바이스(120) 중 하나는 이들 자신의 공개 키의 구성기 증명된 사본을 수신하고 서명의 진정성을 검증한 것에 응답하여 등록을 개시할 수 있다. 등록은, 인증 프로토콜이 사용될 수 있는, 클라이언트 디바이스(110)와 네트워크 디바이스(120) 사이의 초기 통신 채널을 구축하기 위해 발견 단계들(1031)에서 시작할 수 있다. 인증 프로토콜은 인증 요청 메시지(1034) 및 인증 응답 메시지(1032)를 포함할 수 있다.

[0182] [00196] 클라이언트 디바이스(110)는 인증 요청 메시지(1034)에 클라이언트 증명서 및 클라이언트 제공 넌스를 포함할 수 있다. 클라이언트 증명서를 수신 시, 네트워크 디바이스(120)는 검증 절차(1046)에서 클라이언트 증명서를 검증할 수 있다. 예를 들어, 네트워크 디바이스(120)는 클라이언트 증명서를 검증하기 위해 구성기 공개 키를 사용할 수 있다. 증명서가 신뢰된 구성기 서비스(131)에 의해 발행된 것을 검증하기 위해, 수신기 디바이스는 서명 메시지 다이제스트 또는 해시를 획득하도록 서명을 암호화하기 위해 구성기 공개 키를 사용할 수 있다. 그 다음, 수신기 디바이스는 데이터 부분으로부터 수신된 메시지 다이제스트 또는 해시를 컴퓨팅하고 수신된 메시지 다이제스트/해시를 서명 메시지 다이제스트/해시와 비교할 수 있다. 네트워크 디바이스(120)는 공유된 키를 결정할 수 있다. 예를 들어, 네트워크 디바이스(120)는 네트워크 제공 넌스를 생성하고, 클라이언트 제공 넌스, 클라이언트 증명서로부터 추출된 클라이언트 공개 키, 네트워크 개인 키, 및 네트워크 제공 넌스를 사용하여 공유된 키를 결정할 수 있다.

[0183] [00197] 인증 응답 메시지(1032)에서, 네트워크 디바이스(120)는 네트워크 제공 넌스, 네트워크 증명서 및 클라이언트 제공 넌스의 MAC를 포함할 수 있다. 클라이언트 제공 넌스의 MAC는 공유 키를 사용하여 준비된 클라이언트 제공 넌스의 암호화 해시 함수일 수 있다.

[0184] [00198] 검증 절차(1042)에서, 클라이언트 디바이스는 구성기 공개 키를 사용하여 네트워크 증명서를 검증할 수 있다. 검증되면, 클라이언트 디바이스(110)는 네트워크 증명서에 저장된 네트워크 공개 키를 사용하고, 네트워크 디바이스(120)에 의해 사용된 유사한 프로세스를 이용하여, 네트워크 제공 넌스, 클라이언트 제공 넌스, 네트워크 공개 키 및 클라이언트 공개 키를 사용하여 동일한 공유 키를 생성할 수 있다.

[0185] [00199] 공유 키가 일단 획득되면, 클라이언트 디바이스(110) 및 네트워크 디바이스(120)는 추후의 4 방향 핸드쉐이크 인증 및/또는 구성 단계들(1052)을 위해 공유 키를 사용할 수 있다.

[0186] [00200] 도 11은 다른 예시적인 시스템(1100)을 도시하며, 여기서 구성기 디바이스는 제 1 클라이언트 디바이스(1110)와 제 2 클라이언트 디바이스(1120) 사이의 직접 피어-투-피어 무선 연결을 가능하게 하도록 액세스 포인트(1130)로서 구현될 수 있다. 처음에, 제 1 클라이언트 디바이스(1110) 및 제 2 클라이언트 디바이스(1120)는 액세스 포인트(1130)와 무선 연계를 가질 수 있지만, 서로 직접 피어-투-피어 무선 연계를 갖지 않을 수 있다.

[0187] [00201] 액세스 포인트(1130)는 제 1 및 제 2 클라이언트 디바이스들(1110, 1120)에 공개 키들을 제공하도록 구성될 수 있다. 일 실시예에서, 액세스 포인트(1130)는 제 1 클라이언트 디바이스(1110)로부터 (제 1 메시지(1114)에서) 제 1 클라이언트 공개 키를 획득할 수 있고 (제 2 메시지(1124)에서) 제 1 클라이언트 공개 키를 제 2 클라이언트 디바이스(1120)로 제공할 수 있다. 액세스 포인트(1130)는 제 2 클라이언트 디바이스(1120)로부터 (제 3 메시지(1116)에서) 제 2 클라이언트 공개 키를 획득할 수 있고 (제 4 메시지(1126)에서) 제 2 클라이언트 공개 키를 제 1 클라이언트 디바이스(1110)로 제공할 수 있다. 다른 실시예에서, 액세스 포인트(1130)는 하나 이상의 일시적 클라이언트 공개 키들을 생성하고 이들을 제 1 및 제 2 클라이언트 디바이스들(1110, 1120)에 제공하도록 구성될 수 있다. 예를 들어, 액세스 포인트(1130)는 제 1 클라이언트 공개 키를 생성하고 제 1 클라이언트 공개 키를 제 2 클라이언트 디바이스(1120)에 전송할 수 있다. 액세스 포인트(1130)는 제 2 클라이언트 공개 키를 생성하고 제 2 클라이언트 공개 키를 제 1 클라이언트 디바이스(1110)에 전송할 수 있다. 제 1 클라이언트 공개 키 및 제 2 클라이언트 공개 키 중 하나 또는 둘 모두는 액세스 포인트(1130)에 의해 생성된 일시적 클라이언트 공개 키들일 수 있다.

[0188] [00202] 제 1 클라이언트 디바이스(1110) 또는 제 2 클라이언트 디바이스(1120)는 액세스 포인트(1130)로부터 수신된 클라이언트 공개 키들에 기초하여 등록 프로세스(1131)를 개시할 수 있다. 일례에서, 제 1 클라이언트 디바이스(1110)는 인증 요청 메시지(1134)를 제 2 클라이언트 디바이스(1120)에 전송함으로써 인증 프로세스를 개시할 수 있다. 인증 요청 메시지(1134)는 제 1 넌스를 포함할 수 있고, 선택적으로 제 1 클라이언트 디바이스(1110)에 관한 추가 정보를 포함할 수 있다. 제 2 클라이언트 디바이스(1120)는 제 2 넌스를 생성하고, 공개 키를 결정하기 위해 제 2 넌스, 제 1 넌스 및 제 1 클라이언트 공개 키를 사용할 수 있다. 인증 응답 메시지(1132)에서, 제 2 클라이언트 디바이스(1120)는 공유 키에 적어도 부분적으로 기초하여 제 2 넌스는 물론 MAC를 포함할 수 있다.

[0189] [00203] 제 1 클라이언트 디바이스(1110)는 동일한 공유 키를 결정하기 위해, 제 1 넌스, 제 2 넌스 및 2 클라이언트 공개 키(1126)를 사용할 수 있다. 공유 키는 검증 MAC를 생성하고 검증 MAC를 수신된 MAC와 비교함으로써 검증될 수 있다.

[0190] [00204] 등록 및 인증 이후, 제 2 클라이언트 디바이스(1120) 또는 제 1 클라이언트 디바이스(1110)는 피어-투-피어 무선 연결을 위해 구성 데이터(1152)를 제공할 수 있다. 부가적으로, 추가 인증(예컨대, 4 방향 핸드쉐이크 또는 PMK의 구축)이 수행될 수 있다(미도시).

[0191] [00205] 도 12는 네트워크에 새로운 구성기 디바이스(1210)를 부가하는 것을 도시하는 메시지 프로세스 다이어그램(1200)이며, 여기서 기존 구성기 디바이스(1230)가 이미 존재한다. 네트워크는 네트워크 디바이스(1220)를 포함하며, 이는 대역 외 매체를 통해 새로운 구성기 디바이스(1210)로 네트워크 공개 키(1213)를 제공할 수 있다. 예를 들어, 새로운 구성기 디바이스(1210)는 네트워크 디바이스(1220)와 관련된 QR 코드를 스캐닝할 수 있다. 새로운 구성기 디바이스(1210)는 네트워크 디바이스(1220)에 대한 등록 메시지(1225)에서 네트워크 공개 키를 포함할 수 있다. 네트워크 디바이스(1220)는 기존 구성기 디바이스가 이미 존재한다고 결정할 수 있고 기존 구성기 디바이스(1230)가 이미 프로비저닝되었다고 나타내는 응답 메시지(1227)를 전송할 수 있다. 일 실시

예에서, 응답 메시지(1227)는 기존 구성기 디바이스(1230)의 표시자(예를 들어, 명칭 또는 위치)를 제공할 수 있다. 새로운 구성기 디바이스(1210)는 응답 메시지(1227)에 대답하여 확인 응답(1229)을 선택적으로 전송할 수 있다.

[0192] [00206] 새로운 구성기 디바이스(1210)는 QR 코드(1231)를 제공할 수 있고, 사용자에게 기존 구성기 디바이스(1230)에 의해 QR 코드가 스캐닝되도록 명령할 수 있다. QR 코드는 새로운 구성기 디바이스(1210)와 관련된 디바이스 공개 키를 가질 수 있다. 디바이스 공개 키는 기존 구성기 디바이스(1230)에 제공된다(예를 들어, 기존 구성기 디바이스(1230)는 새로운 구성기 디바이스(1210)에 의해 제공된 QR 코드를 스캔(1233)한다). 기존 구성기 디바이스(1230)는 (신뢰된 메시지(1235)에서) 디바이스 공개 키를, 기존 구성기 디바이스(1230)와 네트워크 디바이스(1220) 사이의 기존 신뢰 관계를 사용하여 네트워크 디바이스(1220)에 제공할 수 있다. 디바이스 공개 키를 수신하는 것에 응답하여, 네트워크 디바이스(1220)는 새로운 구성기 디바이스(1210)를 등록하고, 이를 구성기 디바이스들의 리스트에 부가할 수 있다.

[0193] [00207] 도 13은 본 개시의 실시예에 따라, 다양한 디바이스들에 의해 유지될 수 있는 공개 키 리스트들을 예시하는 개념도이다. 도 13에서, 클라이언트 디바이스(110)는 적어도 하나의 네트워크 디바이스와 관련된 공개 키들을 저장하기 위한 메모리(1310)를 가질 수 있다. 메모리(1310)는 또한 구성기 디바이스의 공개 키를 저장할 수 있다. 일 실시예에서, 클라이언트 디바이스(110)가 커버리지 또는 사용자 선택에 기초하여 상이한 네트워크들을 액세스하기 위해 프로비져닝되는 때와 같이, 메모리(1310)는 둘 이상의 네트워크 디바이스에 대한 공개 키들을 저장할 수 있다.

[0194] [00208] 구성기 디바이스(130)는 네트워크에 대해 프로비져닝된 클라이언트 디바이스들의 리스트에 대한 공개 키들을 저장하기 위한 메모리(1330)를 가질 수 있다. 클라이언트 디바이스들의 리스트는, 새로운 네트워크 디바이스가 네트워크에 부가될 때, 새로운 네트워크 디바이스(미도시)와 공유될 수 있다. 메모리(1330)는 또한, 네트워크와 관련된 네트워크 디바이스들의 리스트를 위한 공개 키들을 저장할 수 있다. 네트워크 디바이스들의 리스트에 대한 공개 키들은 네트워크 디바이스로부터의 요청들을 검증하기 위해 사용될 수 있다.

[0195] [00209] 네트워크 디바이스(120)는 구성기 디바이스들의 리스트에 대한 공개 키들 및 클라이언트 디바이스들의 리스트와 관련된 공개 키들을 저장하기 위한 메모리(1320)를 가질 수 있다. 새로운 네트워크 디바이스가 네트워크에 부가된 경우, 클라이언트 디바이스들의 리스트에 대한 공개 키들은 새로운 네트워크 디바이스가 클라이언트 디바이스들을 자동으로 등록할 수 있도록 새로운 네트워크 디바이스에 공유될 수 있다. 구성기 디바이스들의 리스트에 대한 공개 키들은 또한, 새로운 네트워크 디바이스가 네트워크의 구성기 디바이스들에 의해 수신된 등록 요청들을 검증할 수 있도록 새로운 네트워크 디바이스와 공유될 수 있다.

[0196] [00210] 도 13의 예들을 사용하면, 리스트들(및 관련된 공개 키들)은 네트워크에서 액세스를 관리하기 위해 사용될 수 있다는 것이 이해될 수 있다. 예를 들어, 사용자가 클라이언트 디바이스로 하여금 구성기 디바이스의 클라이언트 디바이스들의 리스트로부터 제거되게 하는 경우, 변경들은 다른 구성기 디바이스들 및 네트워크 디바이스들에 전파될 수 있다. 예로서 도 13을 사용하면, 구성기 디바이스(130)는 네트워크 디바이스(120)로 메시지를 전송하여, 네트워크 디바이스(120)로 하여금 메모리(1320)의 클라이언트 디바이스들의 리스트로부터 클라이언트 디바이스(110)에 대한 공개 키를 제거하게 할 수 있다. 그 이후, 클라이언트 디바이스(110)는 네트워크에 대해 프로비져닝되지 않을 것이다.

[0197] [00211] 도 1-13 및 본 명세서에 설명된 동작들은 다양한 실시예들의 이해를 돕기위해 의도된 예들이며, 청구항들의 범위를 제한하기 위해 사용되지 않아야 한다. 실시예들은 추가의 동작들을, 몇몇 동작들을, 동시에 또는 상이한 순서로 동작들을 그리고 상이하게 몇몇 동작들을 수행할 수 있다. 본 개시가 몇몇 실시예들을 열거하지만, 추가 실시예들이 본 개시의 범위 내에서 고려된다. 예를 들어, 일 실시예에서, 네트워크 디바이스로 클라이언드 디바이스를 인증하기 위한 방법은, 구성기 디바이스를 통해, 클라이언트 디바이스와 네트워크 디바이스 사이의 인증을 용이하게 하는 것을 포함하며, 이 인증은 구성기 디바이스를 통해 클라이언트 디바이스로부터 네트워크 디바이스로 공유되는 클라이언트 디바이스의 클라이언트 공개 키에 적어도 부분적으로 기초하며, 구성기 디바이스는 클라이언트 공개 키를 획득하기 위해 대역 외 통신들을 사용한다.

[0198] [00212] 당업자에 의해 인식되는 바와 같이, 본 개시의 양상들은 시스템, 방법, 또는 컴퓨터 프로그램 물건으로서 구현될 수 있다. 따라서, 본 개시의 양상들은, 전체적으로 하드웨어 실시예, 소프트웨어 실시예(펌웨어, 상주 소프트웨어, 마이크로-코드 등을 포함함), 또는 소프트웨어와 하드웨어 양상들을 결합한 실시예의 형태를 가질 수 있고, 이들 모두는 일반적으로 본 명세서에서 "회로", “유닛” 또는 "시스템"으로 지칭될 수 있다. 게다가, 본 개시의 양상들은, 컴퓨터 판독가능 프로그램 코드가 구현된 하나 이상의 컴퓨터 판독가능 매체(들)로

구현되는 컴퓨터 프로그램 물건의 형태를 가질 수 있다.

[0199] [00213] 하나 이상의 컴퓨터 판독 가능 매체(들)의 임의의 결합이 사용될 수 있으며, 유일한 예외는 일시적, 전파 신호이다. 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체일 수 있다. 컴퓨터 판독가능 저장 매체는, 예를 들어, 전자, 자기, 광학, 전자기, 적외선 또는 반도체 시스템, 장치 또는 디바이스 또는 상기한 것들의 임의의 적절한 조합일 수 있지만 이에 한정되는 것은 아니다. 컴퓨터 판독가능 저장 매체의 더 특정한 예들(비포괄적 리스트)은 다음의 것들, 즉, 하나 이상의 와이어들을 갖는 전기 접속, 휴대용 컴퓨터 디스켓, 하드 디스크, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 소거가능한 프로그래머블 판독 전용 메모리(EPROM 또는 플래쉬 메모리), 광 섬유, 휴대용 컴팩트 디스크 판독 전용 메모리(CD-ROM), 광학 저장 디바이스, 자기 저장 디바이스 또는 상기한 것들의 임의의 적절한 조합을 포함할 것이다. 본 문헌의 문맥에서, 컴퓨터 판독가능 저장 매체는, 명령 실행 시스템, 장치 또는 디바이스에 의해 또는 이와 관련하여 이용하기 위한 프로그램을 포함 또는 저장할 수 있는 임의의 유형의(tangible) 매체일 수 있다.

[0200] [00214] 본 개시의 양상들에 대한 동작들을 수행하기 위한 컴퓨터 판독가능 매체 상에 구현되는 컴퓨터 프로그램 코드는, Java, Smalltalk, C++ 등과 같은 객체 지향적 프로그래밍 언어, 및 "C" 프로그래밍 언어 또는 유사한 프로그래밍 언어들과 같은 종래의 절차 지향적 프로그래밍 언어들을 포함하는 하나 이상의 프로그래밍 언어들의 임의의 조합으로 기록될 수 있다. 프로그램 코드는, 전체적으로 사용자의 컴퓨터 상에서, 부분적으로 사용자의 컴퓨터 상에서, 독립형 소프트웨어 패키지로서, 부분적으로는 사용자의 컴퓨터 상에서 그리고 부분적으로는 원격 컴퓨터 상에서, 또는 전체적으로 원격 컴퓨터 또는 서버 상에서 실행될 수 있다. 후자의 시나리오에서, 원격 컴퓨터는, 로컬 영역 네트워크(LAN) 또는 광역 네트워크(WAN)를 포함하는 임의의 타입의 네트워크를 통해 사용자의 컴퓨터에 접속될 수 있거나, 외부 컴퓨터에 대해 (예를 들어, 인터넷 서비스 제공자를 이용한 인터넷을 통해) 접속이 행해질 수 있다.

[0201] [00215] 본 개시의 양상들은, 본 개시의 실시예들에 따라, 흐름도 예시들, 및/또는 방법, 장치(시스템) 및 컴퓨터 프로그램 물건들의 블록 다이어그램들을 참조하여 설명된다. 흐름도 예시들 및/또는 블록도들의 각각의 블록, 및 흐름도 예시들 및/또는 블록도들의 블록들의 조합들은 컴퓨터 프로그램 명령들에 의해 구현될 수 있음이 이해될 것이다. 이 컴퓨터 프로그램 명령들은, 머신을 생성하기 위한 범용 컴퓨터, 특수 목적 컴퓨터, 또는 다른 프로그래머블 데이터 프로세싱 장치의 프로세서에 제공될 수 있어서, 컴퓨터 또는 다른 프로그래머블 데이터 프로세싱 장치의 프로세서를 통해 실행되는 명령들은, 흐름도 및/또는 블록도의 블록 또는 블록들에서 특정되는 기능들/동작들을 구현하기 위한 수단을 생성한다.

[0202] [00216] 컴퓨터 프로그램 명령들은 또한, 컴퓨터, 다른 프로그래머블 데이터 프로세싱 장치 또는 다른 디바이스들이 특정한 방식으로 기능하도록 지시할 수 있는 컴퓨터 판독가능 매체에 저장될 수 있어서, 컴퓨터 판독가능 매체에 저장된 명령들은, 흐름도 및/또는 블록도의 블록 또는 블록들에서 특정된 기능/동작을 구현하는 명령들을 포함하는 제조 물품을 생성한다. 컴퓨터 프로그램 명령들은 또한, 컴퓨터, 다른 프로그래머블 데이터 프로세싱 장치, 또는 다른 디바이스들 상으로 로딩되어, 컴퓨터 구현된 프로세스를 생성하도록 일련의 동작 단계들이 컴퓨터, 다른 프로그래머블 장치 또는 다른 디바이스들 상에서 수행되게 할 수 있어서, 컴퓨터 또는 다른 프로그래머블 장치 상에서 실행되는 명령들은 흐름도 및/또는 블록도의 블록 또는 블록들에서 특정된 기능들/동작들을 구현하기 위한 프로세스들을 제공한다.

[0203] [00217] 도 14는 본 개시의 다양한 실시예들을 구현할 수 있는 전자 디바이스(1400)의 일 실시예의 예시적인 블록도이다. 일부 구현들에서, 전자 디바이스(1400)는 전자 디바이스, 예컨대, 랩탑 컴퓨터, 태블릿 컴퓨터, 모바일 폰, 게임 콘솔 또는 다른 전자 시스템일 수 있다. 전자 디바이스(1400)는, (가능하게는, 다수의 프로세서들, 다수의 코어들, 다수의 노드들을 포함하고 그리고/또는 멀티-스레딩을 구현하는 등의) 프로세서(1402)를 포함한다. 전자 디바이스(1400)는 메모리(1406)를 포함한다. 메모리(1406)는, 시스템 메모리(예를 들어, 캐시, SRAM, DRAM, 제로 커패시터 RAM, 트윈 트랜지스터 RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM 등 중 하나 이상), 또는 기계 판독가능 매체의 앞서 이미 설명된 가능한 실현들 중 임의의 하나 이상일 수 있다. 전자 디바이스(1400)는 또한 버스(1401)(예를 들어, PCI, ISA, PCI-Express, HyperTransport®, InfiniBand®, NuBus, AHB, AXI 등) 를 포함한다. 전자적인 하나 이상의 네트워크 인터페이스들은 무선 네트워크 인터페이스(예를 들어, WLAN 인터페이스, Bluetooth® 인터페이스, WiMAX 인터페이스, ZigBee® 인터페이스, 무선 USB 인터페이스 등) 또는 유선 네트워크 인터페이스(예를 들어, 파워라인 통신 인터페이스, 이더넷 인터페이스 등)를 포함할 수 있다. 일부 실시예들에서, 전자 디바이스(1400)는 다수의 네트워크 인터페이스들(1404)을 지원할 수 있고, 이들 각각은 전자 디바이스(1400)를 상이한 통신 네트워크에 커플링하도록 구성될 수 있다.

[0204] [00218] 메모리(1406)는 전술한 실시예들을 실현하기 위한 기능을 구현한다. 메모리(1406)는 지원된 등록 및 인증을 가능하게 하는 하나 이상의 기능들을 포함할 수 있다. 예를 들어, 메모리(1406)는 전술한 바와 같이, 클라이언트 디바이스(110), 네트워크 디바이스(120) 또는 구성기 디바이스(130)의 하나 이상의 양상들을 실현할 수 있다. 메모리(1406)는 앞서 도 1-13에 설명된 실시예들을 실현하기 위한 기능을 구현할 수 있다. 일 실시예에서, 메모리(1406)는 키들, 인증 메시지들 등을 전송 및 수신하게 할 수 있는 하나 이상이 기능들을 포함할 수 있다.

[0205] [00219] 전자 디바이스(1400)는 또한, 센서 인터페이스(1420), 액추에이터 인터페이스(1430) 또는 다른 입력/출력 컴포넌트를 포함할 수 있다. 다른 실시예들에서 전자 디바이스(1400)는 네트워크 공개 키 및/또는 클라이언트 공개 키를 결정하기 위해 사용되는 다른 적절한 센서들(예를 들어, 카메라, 마이크로폰, NFC 검출기, 바코드 스캐너 등)을 가질 수 있다.

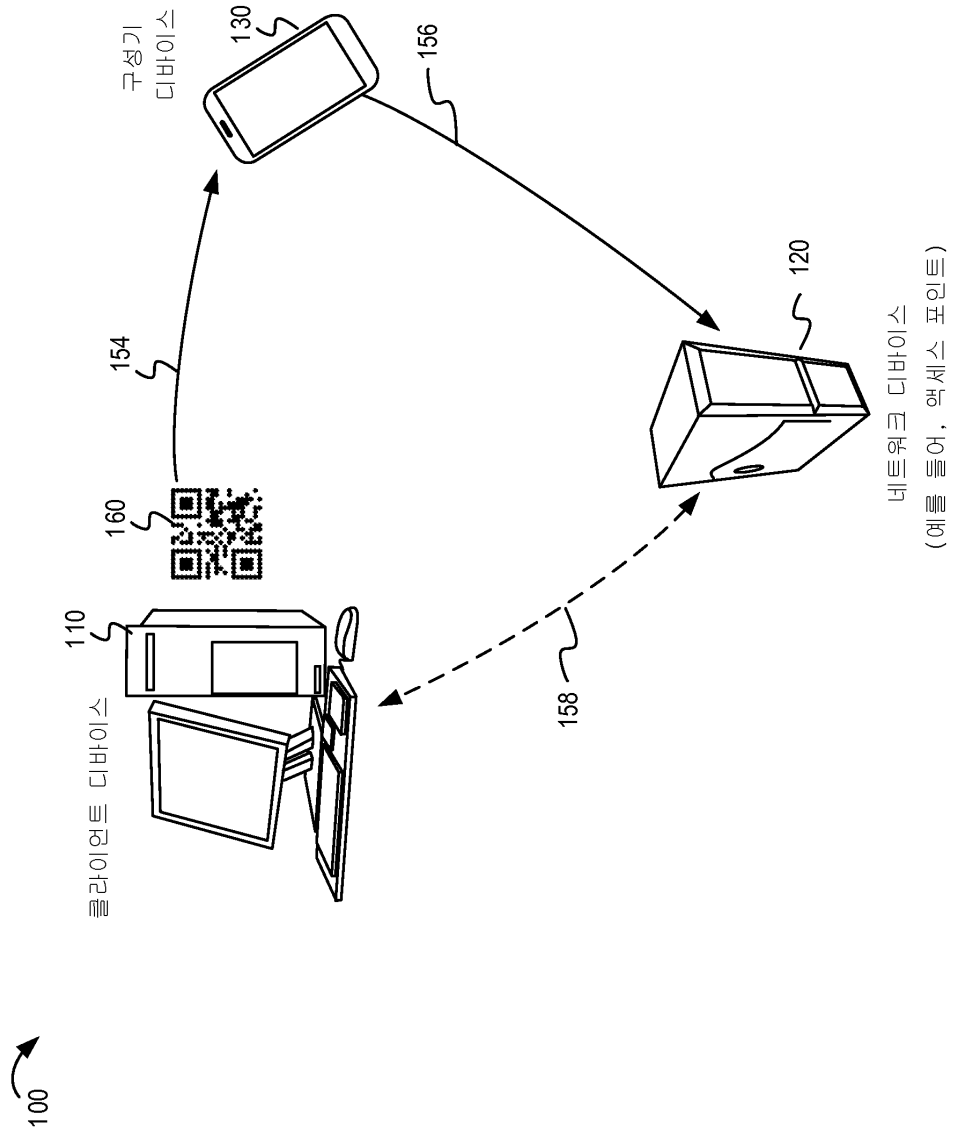
[0206] [00220] 이러한 기능들 중 임의의 하나는 하드웨어에서 그리고/또는 프로세서(1402) 상에서 부분적으로(또는 전적으로) 실현될 수 있다. 예를 들어, 기능은 주문형 집적 회로로, 프로세서(1402)에서 구현된 로직에서, 주변 디바이스 또는 카드 상의 코-프로세서 등에서 구현될 수 있다. 추가로, 실현들은, 더 적은 컴포넌트들 또는 도 14에 예시되지 않은 더 적거나 추가적인 컴포넌트들(예를 들어, 비디오 카드들, 오디오 카드들, 추가적인 네트워크 인터페이스들, 주변 디바이스들 등)을 포함할 수 있다. 프로세서(1402) 및 메모리(1406)는 버스(1401)에 커플링된다. 버스(1401)에 커플링되는 것으로 도시되지만, 메모리(1406)는 프로세서(1402)에 직접 커플링될 수 있다.

[0207] [00221] 실시예들이 다양한 실현들 및 개발을 참조하여 설명되었지만, 이러한 실시예들이 예시적이며 본 개시의 범위가 이들에 제한되지 않는다는 것이 이해될 것이다. 일반적으로, 본 명세서에서 설명되는 바와 같이 디바이스 프로비저닝을 위한 기술들은 임의의 하드웨어 시스템 또는 하드웨어 시스템들과 일치하는 설비들로 구현될 수 있다. 많은 변화들, 변형들, 추가들 및 개선들이 가능하다.

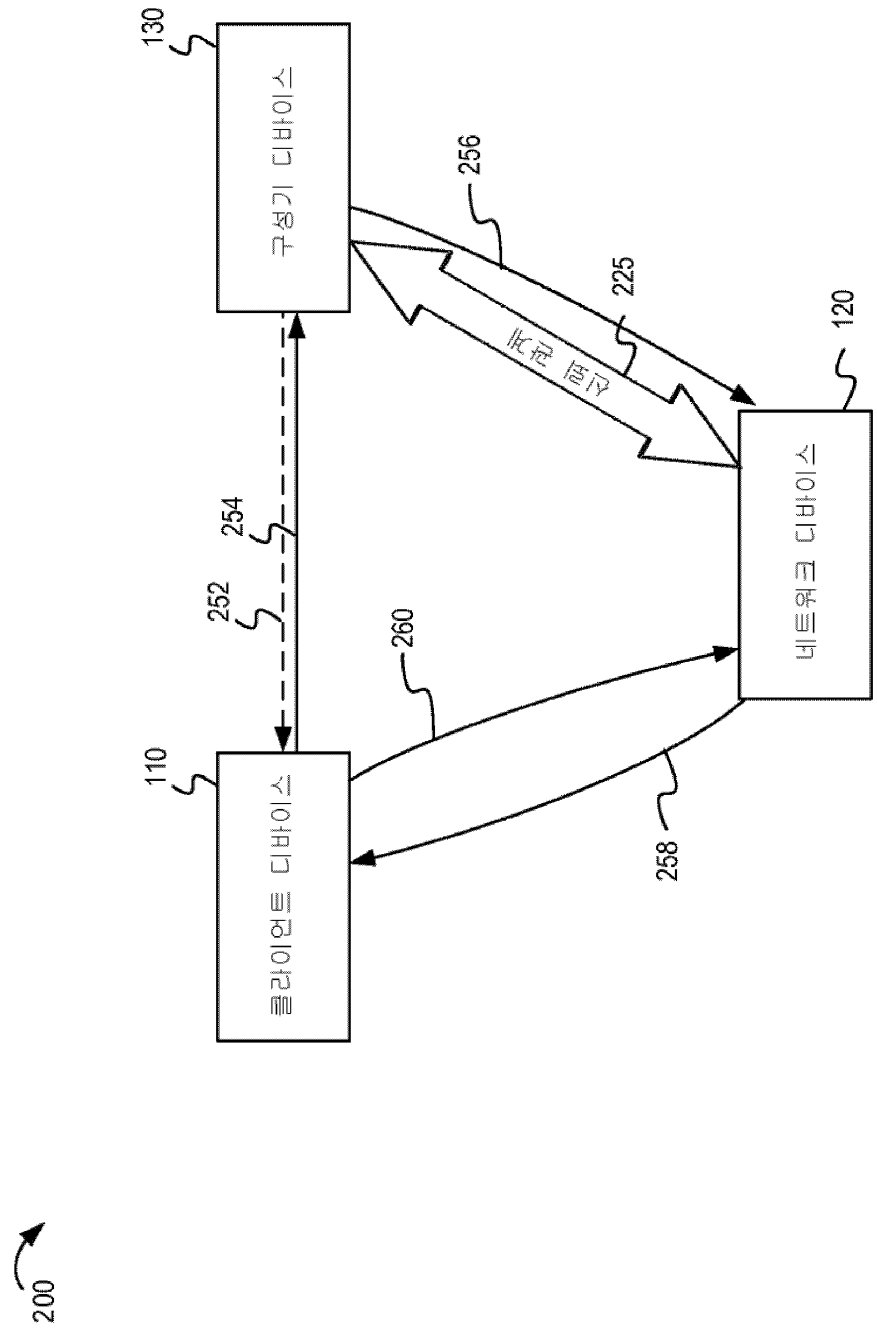
[0208] [00222] 복수의 인스턴스들이 컴포넌트들, 단일 인스턴스로서 본 명세서에 설명된 동작들 또는 구조들에 대해 제공될 수 있다. 마지막으로, 다양한 컴포넌트들, 동작들 및 데이터 저장소들 사이의 경계들은 다소 임의적이고, 특정한 동작들은 특정한 예시적인 구성들의 상황에서 예시된다. 기능의 다른 할당들이 고려되고, 이는 본 개시의 범위 내에 속할 수 있다. 일반적으로, 예시적인 구성들에서 별개의 컴포넌트들로서 제시된 구조들 및 기능은 결합된 구조 또는 컴포넌트로서 구현될 수 있다. 유사하게, 단일 컴포넌트로서 제시된 구조들 및 기능은 별개의 컴포넌트들로 구현될 수 있다. 이러한 변화들, 변형들, 추가들 및 개선들 및 다른 변화들, 변형들, 추가들 및 개선들은 본 개시의 범위 내에 속할 수 있다.

도면

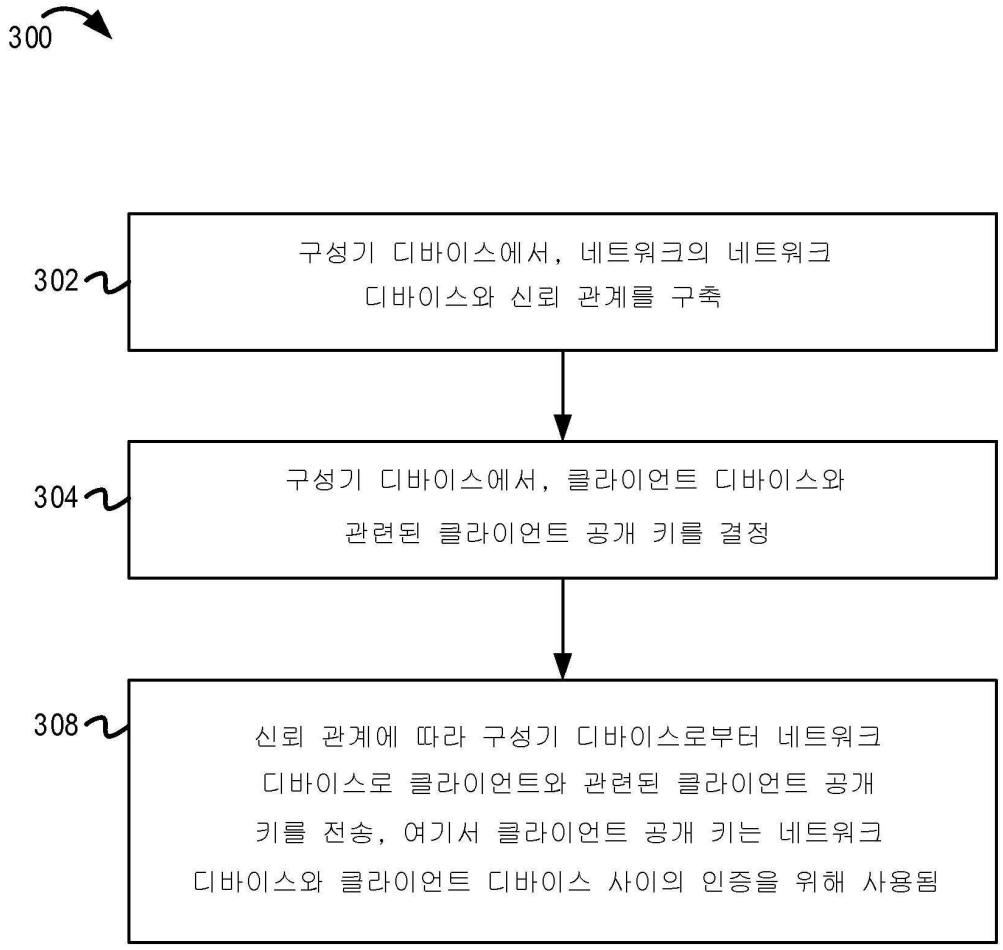
도면1


구성기 디바이스
130
156
120
네트워크 디바이스
(예를 들어, 액세스 포인트)
154
160
110
클라이언트 디바이스
158
100

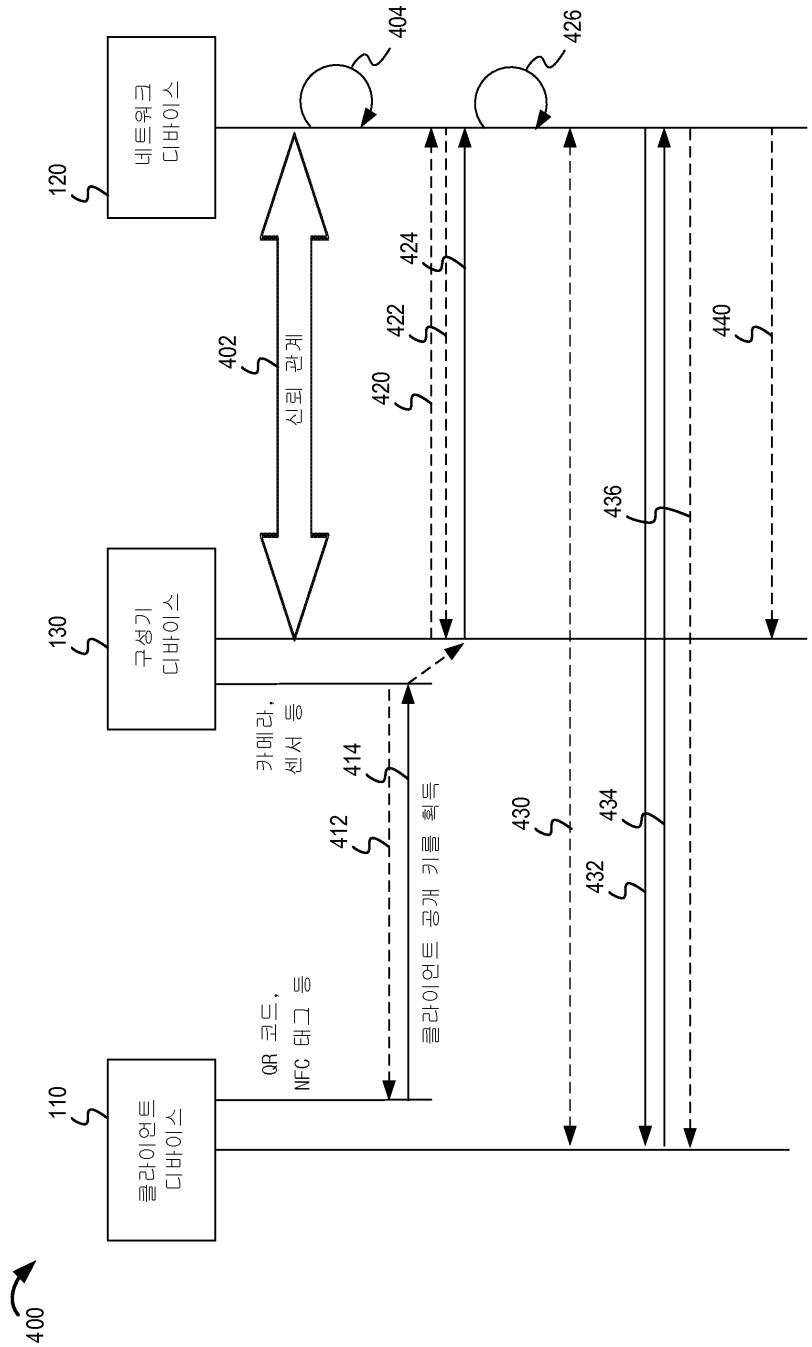
도면2


130
구성기 디바이스
256
225
120
254
252
260
110
클라이언트 디바이스
네트워크 디바이스
258
200

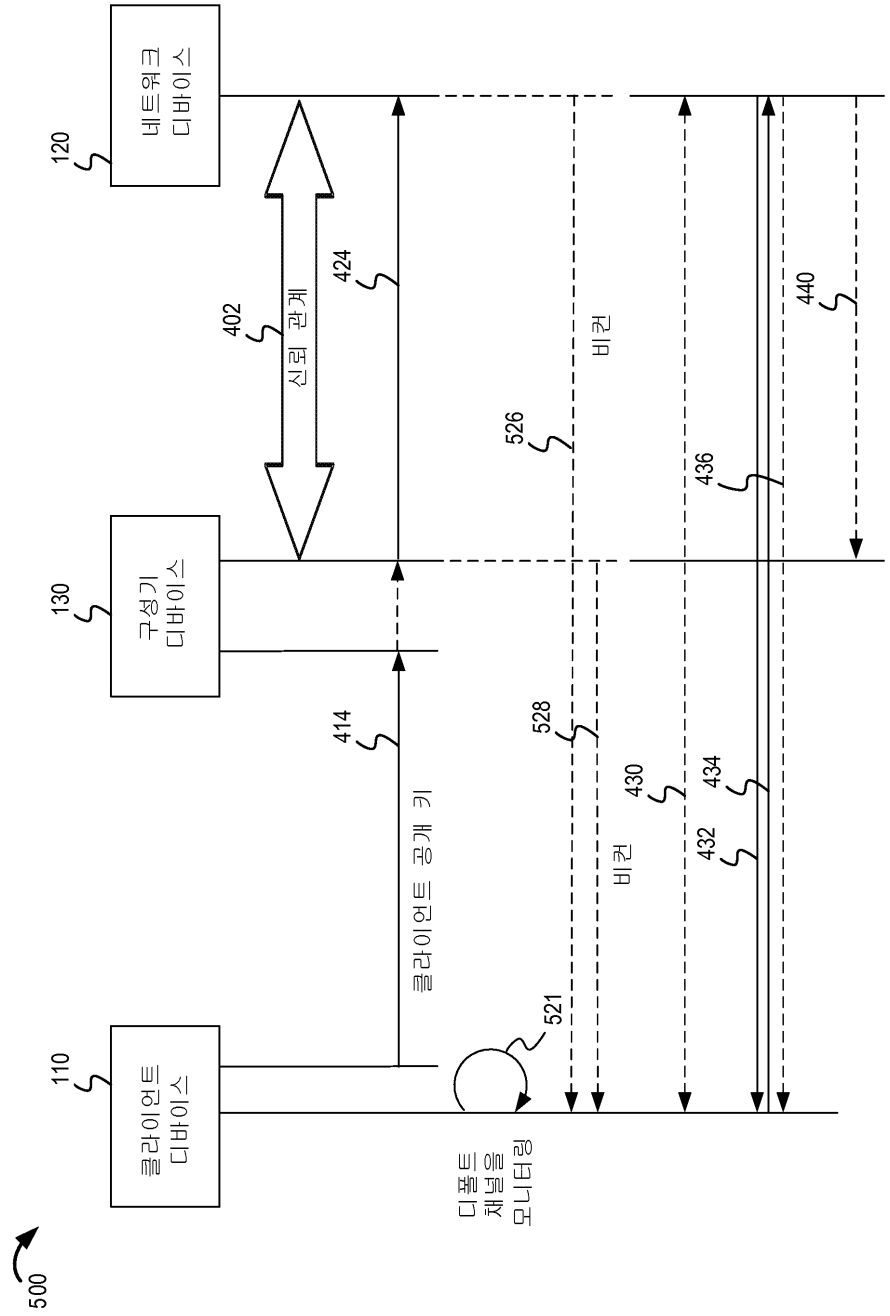
도면3


300
302
구성기 디바이스에서, 네트워크의 네트워크 디바이스와 신뢰 관계를 구축
304
구성기 디바이스에서, 클라이언트 디바이스와 관련된 클라이언트 공개 키를 결정
308
신뢰 관계에 따라 구성기 디바이스로부터 네트워크 디바이스로 클라이언트와 관련된 클라이언트 공개 키를 전송, 여기서 클라이언트 공개 키는 네트워크 디바이스와 클라이언트 디바이스 사이의 인증을 위해 사용됨

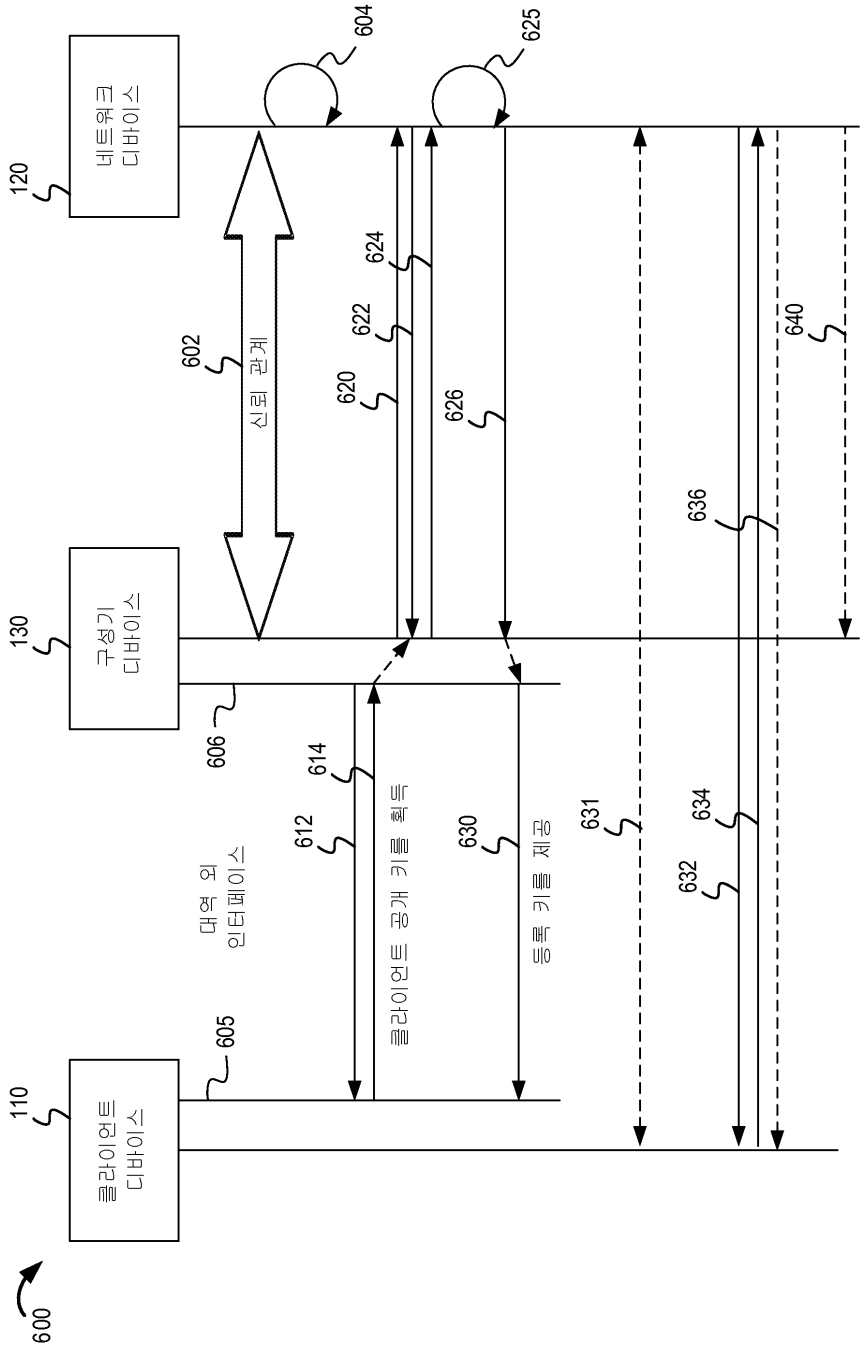
도면4


400
110
클라이언트 디바이스
120
네트워크 디바이스
130
구성기 디바이스
402
신뢰 관계
404
426
420
422
424
440
436
430
434
432
412
414
QR 코드, NFC 태그 등
카메라, 센서 등
클라이언트 공개 키를 획득

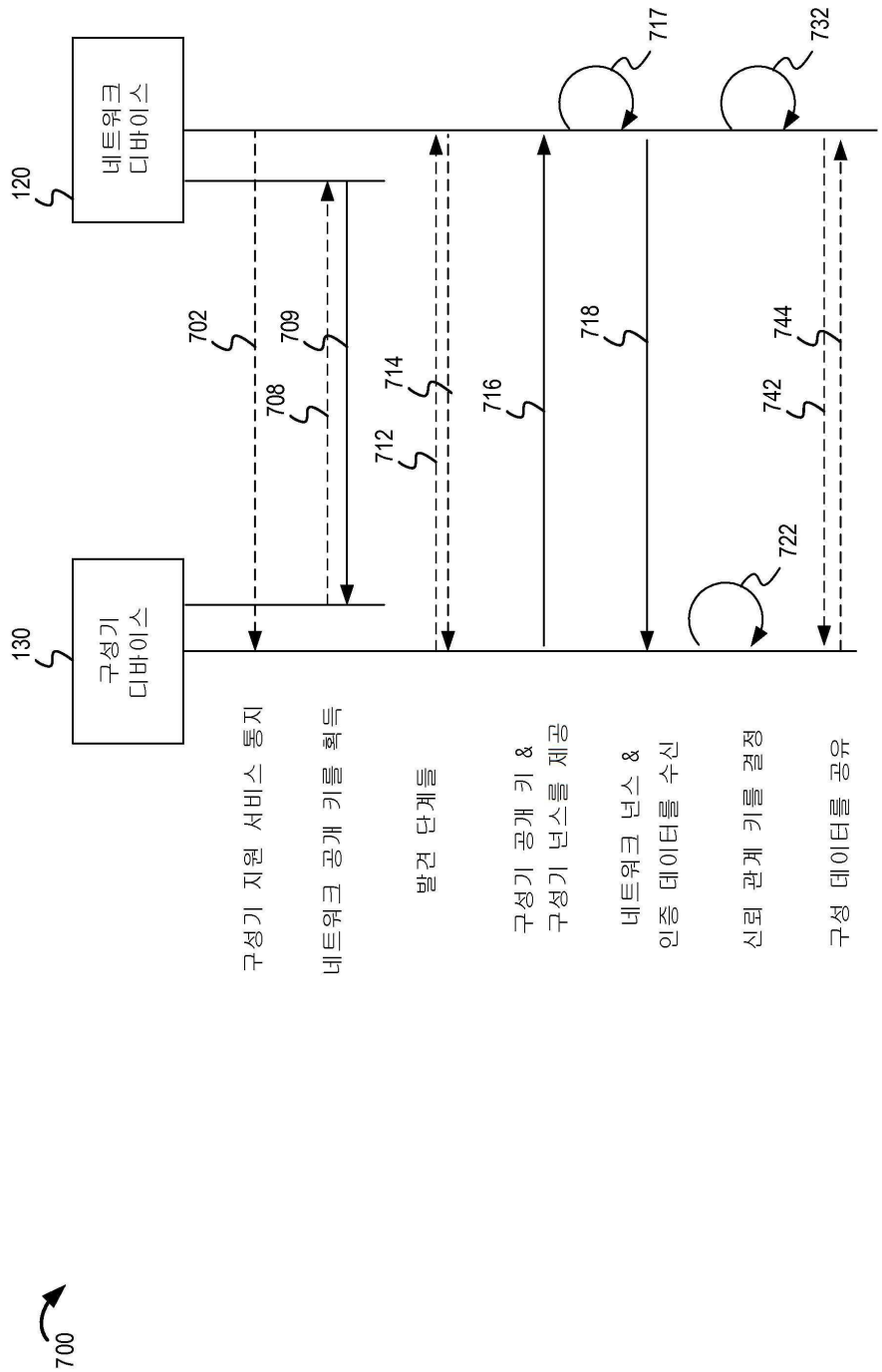
도면5


500
110
클라이언트 디바이스
120
네트워크 디바이스
130
구성기 디바이스
402
신뢰 관계
414
클라이언트 공개 키
424
521
디폴트 채널을 모니터링
526
528
비컨
430
432
434
436
비컨
440

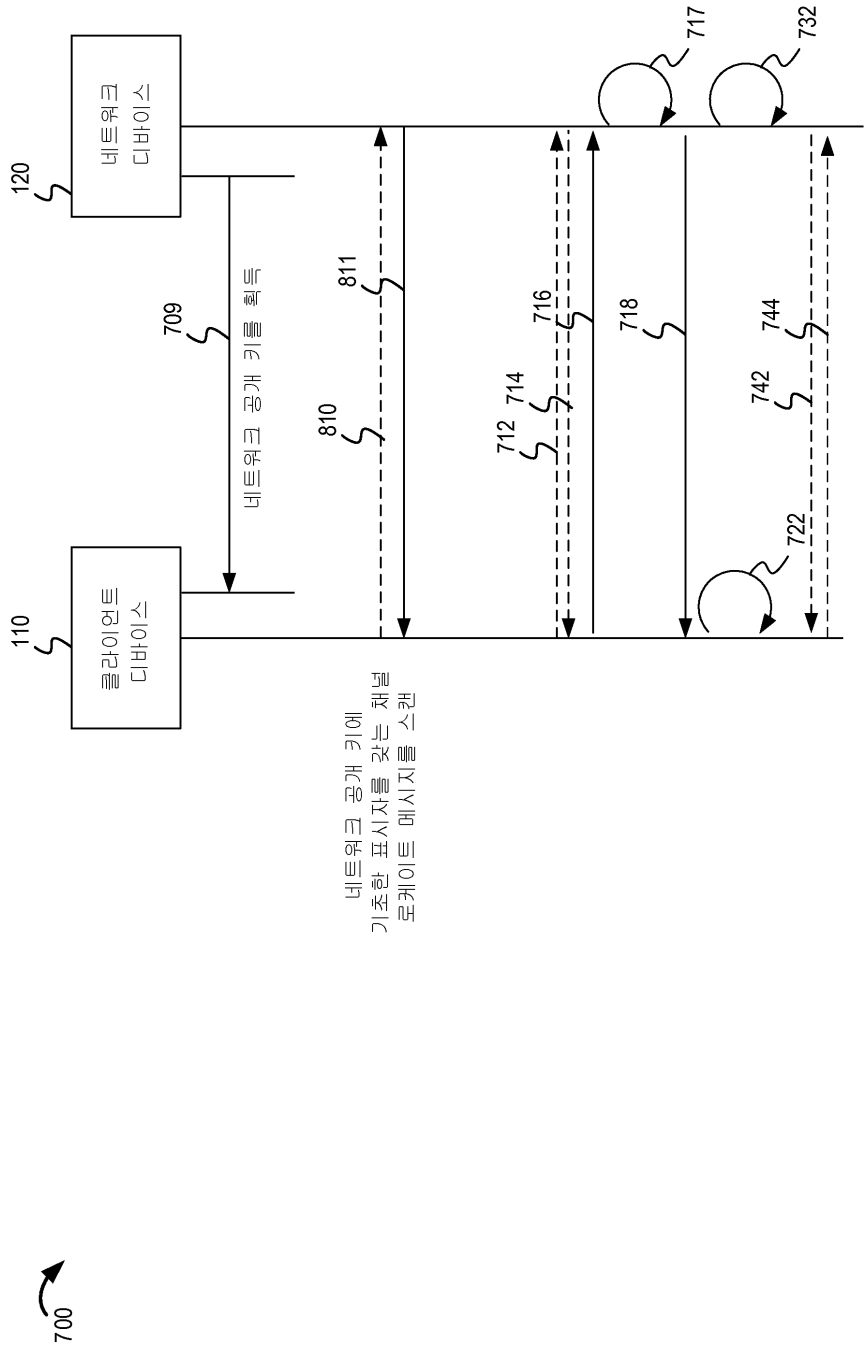
도면6


600
110
클라이언트 디바이스
120
네트워크 디바이스
130
구성기 디바이스
602
신뢰 관계
604
625
606
605
대역 외 인터페이스
614
612
클라이언트 공개 키를 획득
630
등록 키를 제공
620
622
624
626
631
632
634
636
640

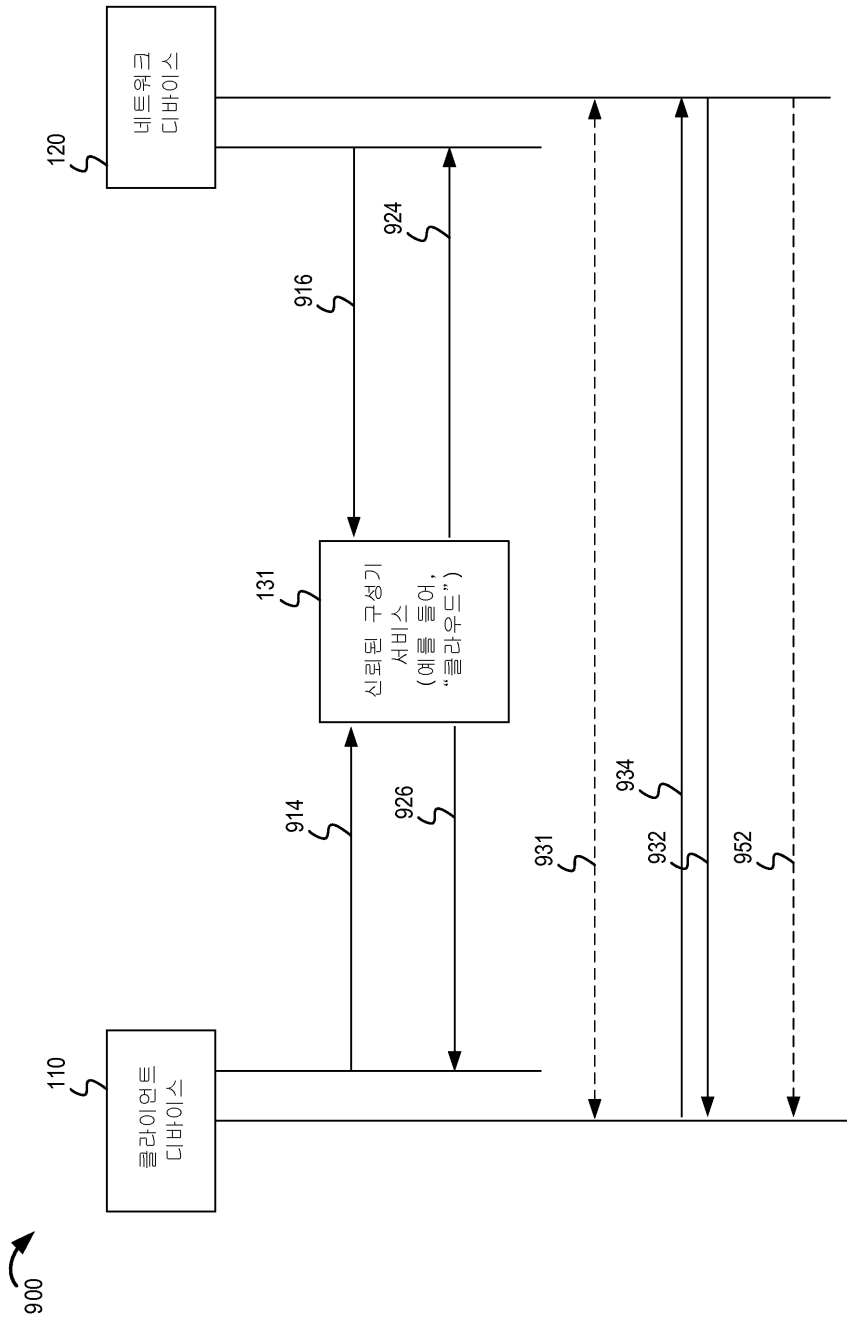
도면7


700
120
네트워크 디바이스
130
구성기 디바이스
702
708
709
712
714
716
717
718
722
732
742
744
구성기 지원 서비스 통지
네트워크 공개 키를 획득
발견 단계들
구성기 공개 키 &
구성기 넌스를 제공
네트워크 넌스 &
인증 데이터를 수신
신뢰 관계 키를 결정
구성 데이터를 공유

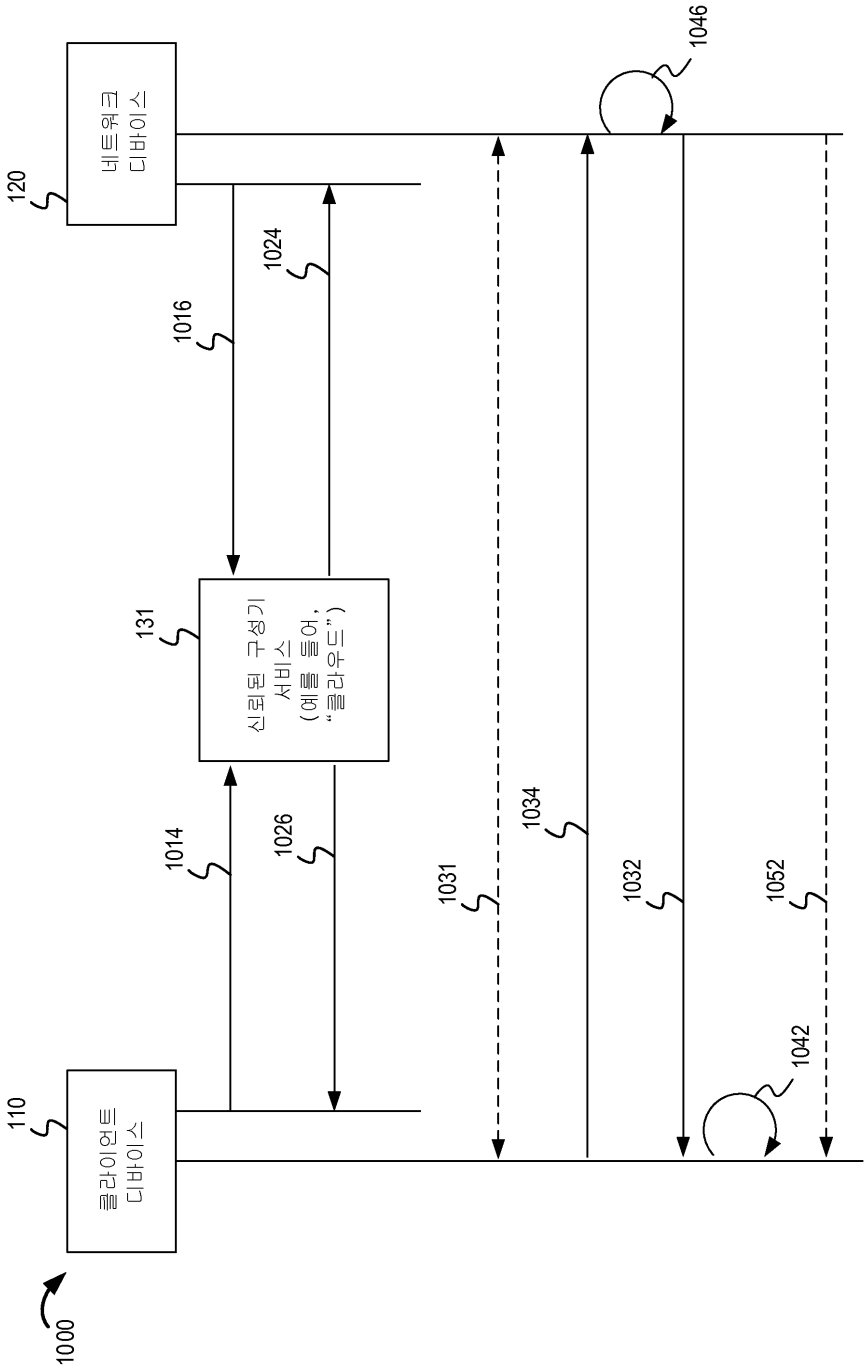
도면8


700
110
클라이언트 디바이스
120
네트워크 디바이스
709
네트워크 공개 키를 획득
810
811
712
714
716
718
717
722
742
744
732
네트워크 공개 키에 기초한 표시자를 갖는 채널 로케이트 메시지를 스캔

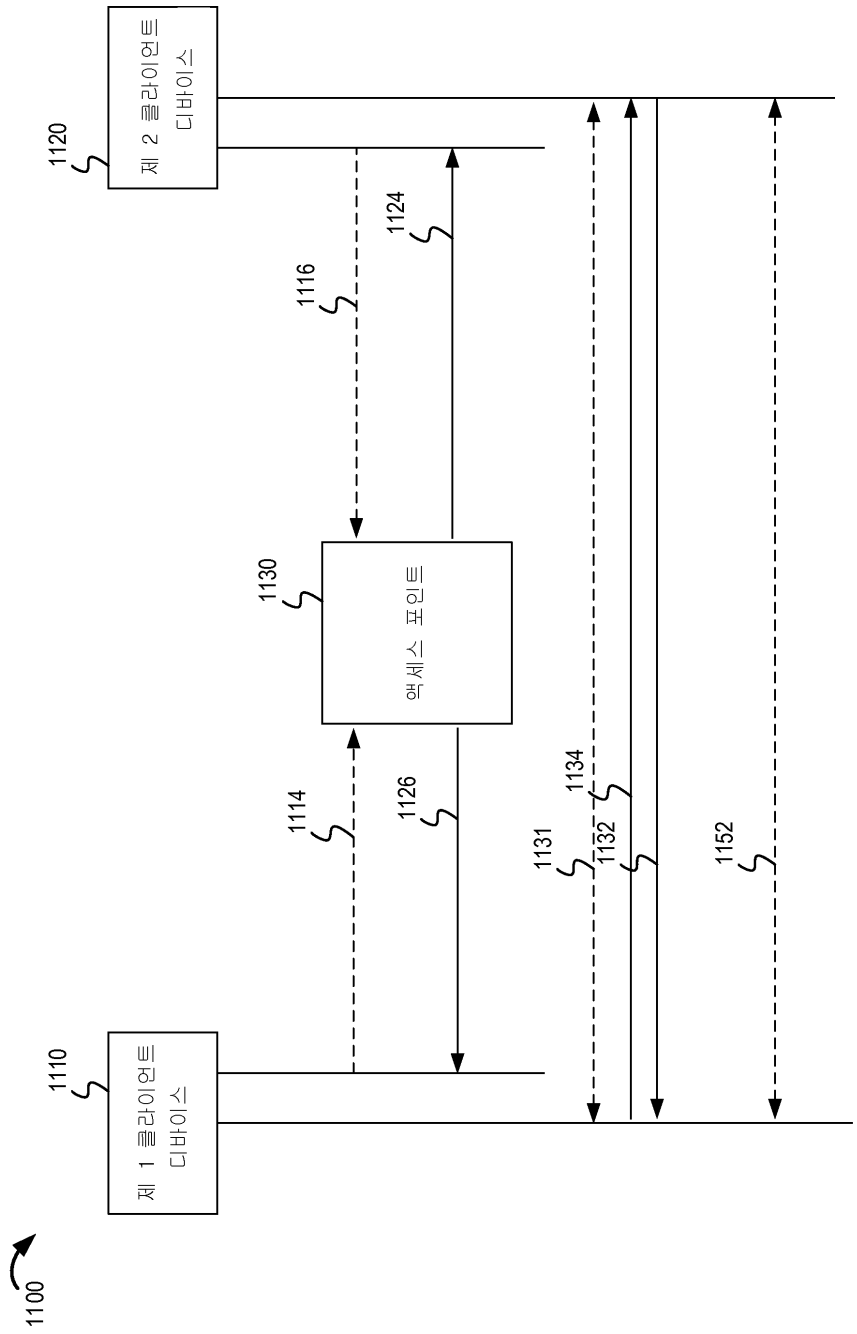
도면9


900
110
클라이언트 디바이스
120
네트워크 디바이스
131
신뢰된 구성기 서비스 (예를 들어, "클라우드")
914
916
924
926
931
932
934
952

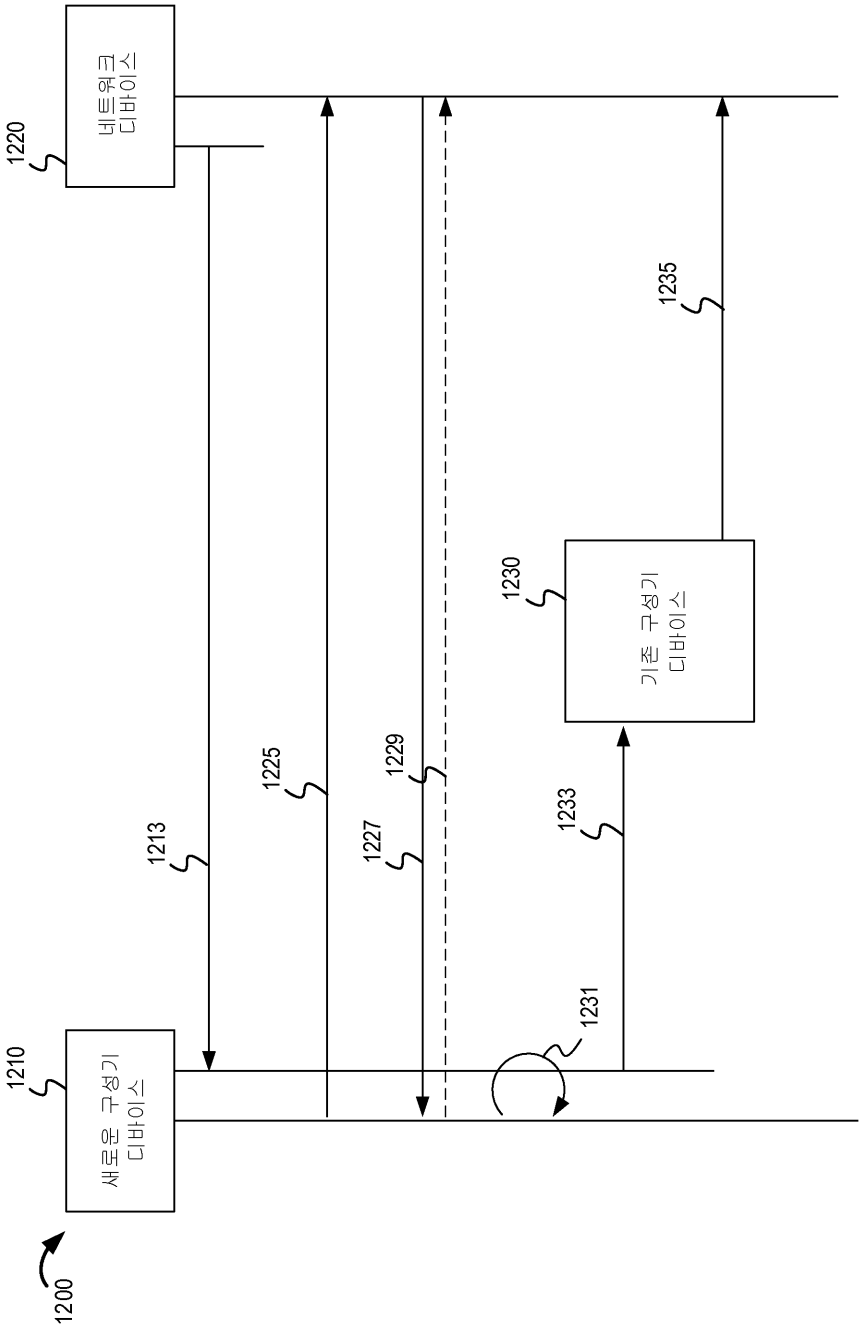
도면10


1000
110
클라이언트 디바이스
120
네트워크 디바이스
131
신뢰된 구성기 서비스 (예를 들어, "클라우드")
1014
1016
1024
1026
1031
1032
1034
1042
1046
1052

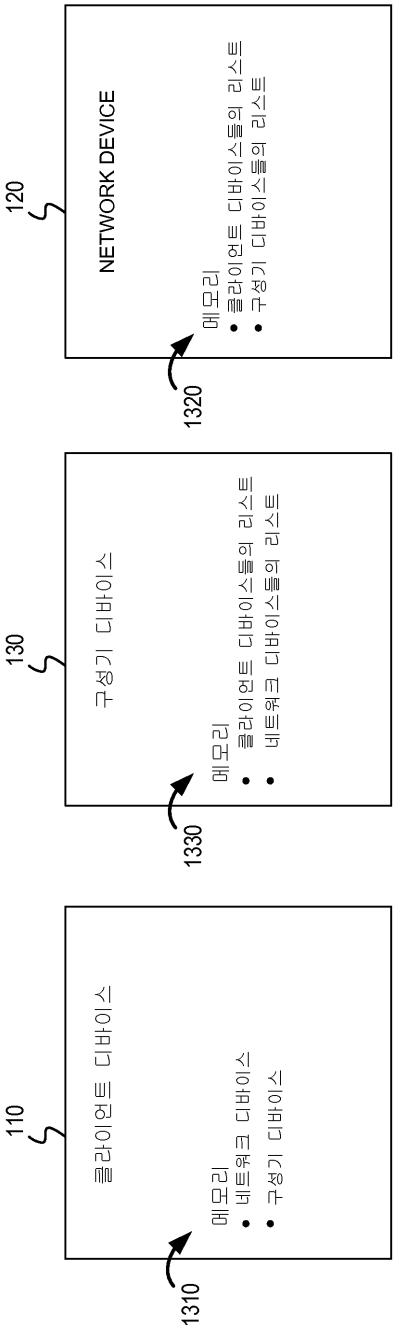
도면11


1100
1110
제 1 클라이언트 디바이스
1120
제 2 클라이언트 디바이스
1130
액세스 포인트
1114
1116
1124
1126
1131
1132
1134
1152

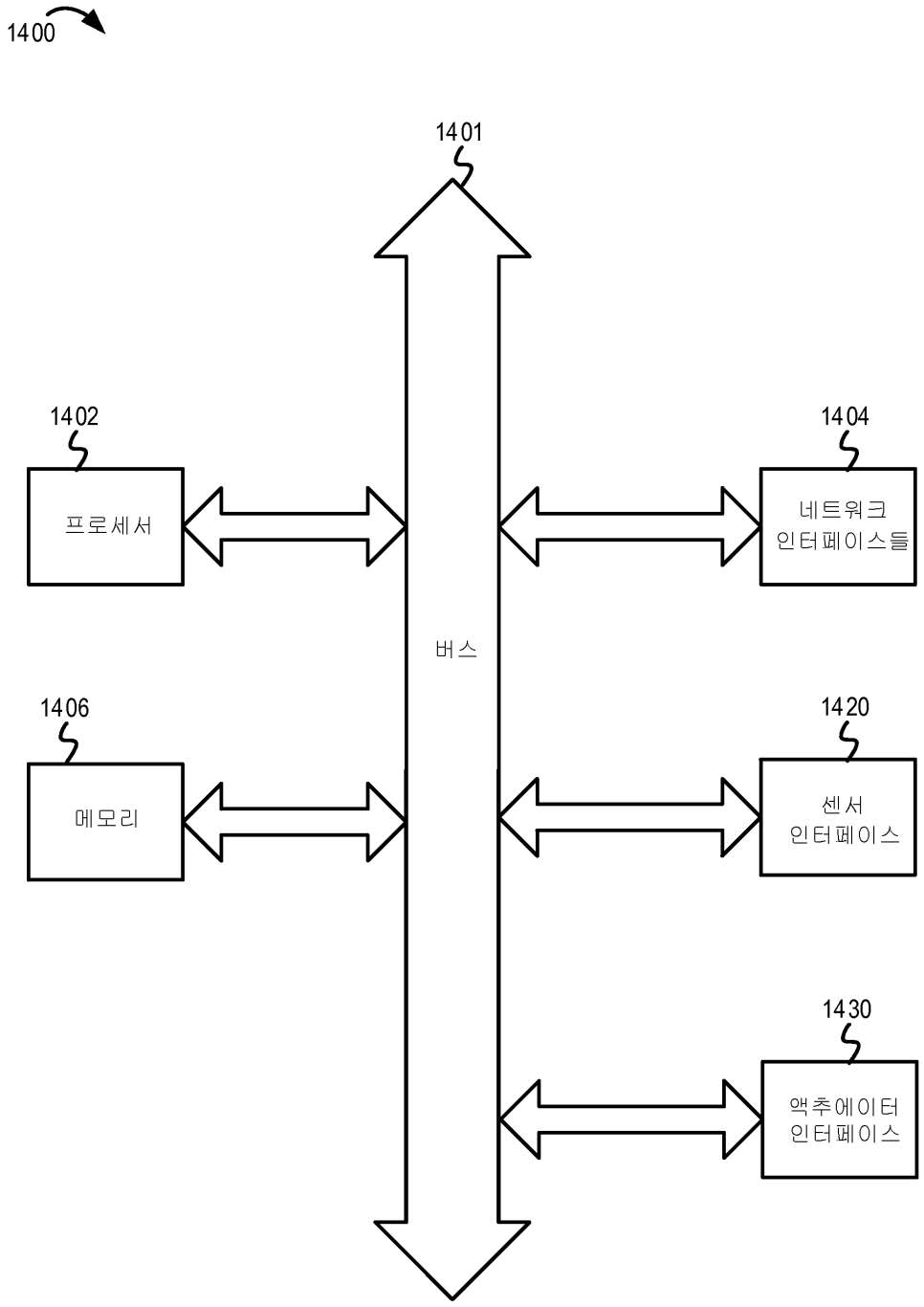
도면12


네트워크
디바이스
1220
1235
1230
기존 구성기
디바이스
1225
1229
1213
1227
1233
1231
1210
새로운 구성기
디바이스
1200

도면13


110
클라이언트 디바이스
메모리
• 네트워크 디바이스
• 구성기 디바이스
1310
130
구성기 디바이스
메모리
• 클라이언트 디바이스들의 리스트
• 네트워크 디바이스들의 리스트
1330
120
NETWORK DEVICE
메모리
• 클라이언트 디바이스들의 리스트
• 구성기 디바이스들의 리스트
1320

도면14


1400
1401
1402
프로세서
1404
네트워크
인터페이스들
버스
1406
메모리
1420
센서
인터페이스
1430
액추에이터
인터페이스