(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0138992
(43) 공개일자 2014년12월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2014-7029199
(22) 출원일자(국제) 2013년03월20일
심사청구일자 없음
(85) 번역문제출일자 2014년10월17일
(86) 국제출원번호 PCT/US2013/033161
(87) 국제공개번호 WO 2013/142606
국제공개일자 2013년09월26일
(30) 우선권주장
13/843,395 2013년03월15일 미국(US)
(뒷면에 계속)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
베노이트, 올리비에 진
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)
팔라니고운더, 아난드
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)
(뒷면에 계속)
(74) 대리인
특허법인 남앤드남

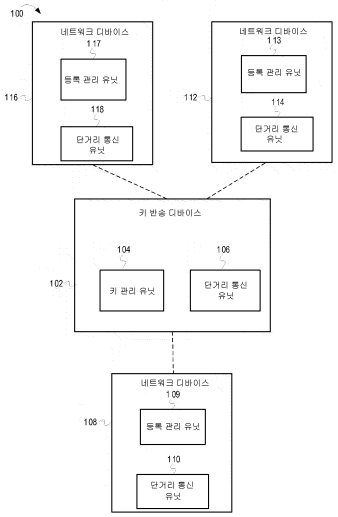
전체 청구항 수 : 총 68 항

(54) 발명의 명칭 **단거리 무선 통신을 사용하는 네트워크 보안성 구성**

(57) 요 약

구성 디바이스(102)는 통신 네트워크에서 네트워크 디바이스((109), (113), (117))를 구성하기 위하여 개시된다. 구성 디바이스는 단거리 통신 연결(302)을 통해 네트워크 디바이스와 페어링 동작들을 개시한다. 구성 디바이스는 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정한다(304). 만일 네트워크 디바이스가 등록해제 상태에 있음을 구성 디바이스가 결정하면, 구성 디바이스는 구성 디바이스와 네트워크 디바이스 사이에 보안 단거리 통신 채널을 설정한다(306). 구성 디바이스는 통신 네트워크에 통신가능하게 연결하기 위하여 네트워크 디바이스를 구성하기 위한 네트워크 키를 보안 단거리 통신 채널을 통해 네트워크 디바이스에 전송한다(308). 만일 네트워크 디바이스가 등록 상태에 있음을 구성 디바이스가 결정하면, 구성 디바이스는 네트워크 디바이스를 등록해제해야 하는지를 결정한다(314).

대 표 도 - 도1



(72) 발명자

호, 사이 이유 던칸

미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)

페레즈, 아람

미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)

모한티, 빕후 프라사드

미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)

코헨, 에탄 구르

미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775 퀄컴 인코포레이티드 (내)

(30) 우선권주장

61/613,438 2012년03월20일 미국(US)

61/637,234 2012년04월23일 미국(US)

특허청구의 범위

청구항 1

네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법으로서,

상기 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와의 페어링 동작들을 구성 디바이스에 의해 개시하는 단계;

상기 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 상기 구성 디바이스에 의해 결정하는 단계;

만일 상기 네트워크 디바이스가 상기 등록해제 상태에 있다고 결정되면,

상기 구성 디바이스와 상기 네트워크 디바이스 사이에 단거리 통신 채널을 설정하는 단계; 및

상기 통신 네트워크에 통신가능하게 연결하기 위하여 상기 네트워크 디바이스를 구성하기 위한 네트워크 키를 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스에 전송하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 2

제 1항에 있어서, 상기 네트워크 디바이스가 상기 등록 상태에 있다고 결정되면, 상기 네트워크 디바이스를 등록해제해야 하는지를 결정하는 단계를 더 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 3

제 2항에 있어서, 상기 네트워크 디바이스를 등록해제해야 하는지를 결정하는 상기 단계는,

상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지 또는 상기 상이한 구성 디바이스에 등록되어 있는지의 여부를 결정하는 단계; 및

상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정하고 상기 네트워크 디바이스를 등록해제할 것을 결정하는 것에 응답하여, 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 상기 네트워크 디바이스에 전송하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 4

제 3항에 있어서, 상기 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 전송하는 상기 단계는 상기 네트워크 디바이스에서의 페어링 동작들 동안 저장되는 데이터를 삭제할 적어도 하나의 명령을 전송하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 5

제 1항에 있어서, 상기 네트워크 디바이스와의 페어링 동작들을 개시하는 상기 단계는,

상기 네트워크 디바이스의 디바이스 식별자 및 복수의 키들을 교환하고 저장함으로써 상기 네트워크 디바이스와 페어링하는 단계; 및

비대칭 암호화 방식을 사용하여 상기 네트워크 디바이스와 페어링하는 단계 중 하나를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 6

제 5항에 있어서, 상기 비대칭 암호화 방식을 사용하여 상기 네트워크 디바이스와 페어링하는 상기 단계는 상기 네트워크 디바이스에 상기 구성 디바이스의 공개 키를 저장하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 7

제 1항에 있어서, 상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하는 상기 단계는,

제 1 정보를 포함하는 제 1 메시지를 상기 구성 디바이스로부터 상기 네트워크 디바이스로 전송하는 단계; 및

상기 제 1 메시지에 응답하여 수신되는 제 2 메시지에 기초하여 상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 8

제 1항에 있어서, 상기 단거리 통신 연결은 근거리 무선 통신(NFC) 연결인, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 9

제 1항에 있어서, 상기 단거리 통신 연결은 Bluetooth 통신 연결, ZigBee 통신 연결 및 무선 근거리 통신망(WLAN) 통신 연결 중 하나인, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 10

제 1항에 있어서, 상기 단거리 통신 채널은 무결성, 암호화 및 리플레이 보호에 대한 지원을 가진 보안 단거리 통신 채널을 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 11

제 10항에 있어서, 상기 리플레이 보호는 시퀀스 번호들을 사용하여 구현되는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 12

제 10항에 있어서, 상기 리플레이 보호는 시간스탬프들을 사용하여 구현되는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 13

네트워크 디바이스를 구성하기 위한 방법으로서,

단거리 통신 연결을 통해 구성 디바이스에 등록할, 상기 구성 디바이스로부터의 요청을 통신 네트워크의 네트워크 디바이스에서 수신하는 단계;

상기 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 단계;

만일 상기 네트워크 디바이스가 등록해제 상태에 있다고 결정되면,

상기 네트워크 디바이스가 상기 등록해제 상태에 있음을 표시하기 위하여 상기 구성 디바이스에 응답을 전송하는 단계;

상기 네트워크 디바이스와 상기 구성 디바이스 사이에 단거리 통신 채널을 설정하는 단계; 및

상기 구성 디바이스에 등록하기 위하여 상기 단거리 통신 채널을 통해 상기 구성 디바이스로부터의 적어도 하나의 키를 수신하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 14

제 13항에 있어서, 상기 등록할 요청은 상기 구성 디바이스의 식별자를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 15

제 13항에 있어서, 상기 등록할 요청은 상기 구성 디바이스의 공개 키를 포함하는, 네트워크 디바이스를 구성하

기 위한 방법.

청구항 16

제 13항에 있어서, 상기 등록할 요청은,

난수에 대한 요청; 또는

난수를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 17

제 16항에 있어서, 상기 네트워크 디바이스에서 상기 난수를 수신하는 것에 응답하여, 상기 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 컴퓨팅하는 단계 및 상기 구성 디바이스에 상기 해싱된 값을 송신하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 18

제 16항에 있어서, 상기 네트워크 디바이스에서 상기 난수에 대한 요청을 수신하는 것에 응답하여, 상기 구성 디바이스에 난수를 송신하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 19

제 13항에 있어서, 상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하는 상기 단계는 상기 구성 디바이스로부터 수신되는 파라미터와 상기 네트워크 디바이스에 저장되는 적어도 하나의 파라미터를 비교하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 20

제 13항에 있어서, 상기 구성 디바이스에 상기 응답을 송신하는 상기 단계는 상기 네트워크 디바이스에 저장되는 상기 통신 네트워크의 네트워크 키를 상기 구성 디바이스에 송신하는 단계를 더 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 21

제 20항에 있어서, 상기 네트워크 디바이스에 저장되는 상기 통신 네트워크의 네트워크 키를 송신하는 상기 단계는 상기 구성 디바이스에 상기 네트워크 키의 해싱된 값을 송신하는 단계를 더 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 22

제 13항에 있어서, 상기 단거리 통신 채널을 설정하는 상기 단계는 보안 단거리 통신 채널을 설정하기 위하여 키 합의, 키 유도 및 키 확인 절차들을 수행하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 23

제 13항에 있어서, 상기 구성 디바이스로부터 등록해제할 요청을 상기 네트워크 디바이스에 수신하는 단계;

상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록 해제 상태에 있는지의 여부를 결정하는 단계;

만일 상기 네트워크 디바이스가 상기 등록 상태에 있다고 결정되면,

상기 네트워크 디바이스가 등록해제할 상기 요청을 송신한 상기 구성 디바이스에 등록되어 있는지의 여부를 결정하는 단계; 및

만일 상기 네트워크 디바이스가 상기 등록해제할 요청을 송신한 상기 구성 디바이스에 등록되어 있으면, 상기 네트워크 디바이스에 저장되는 상기 적어도 하나의 키를 삭제하는 단계를 더 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 24

제 23항에 있어서, 상기 네트워크 디바이스가 상기 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하는 상기 단계는 등록 동작 동안 상기 네트워크 디바이스에 저장되는 파라미터와 상기 등록해제 요청에서 수신되는 적어도 하나의 파라미터를 비교하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 25

제 23항에 있어서, 상기 네트워크 디바이스가 상기 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하는 상기 단계는 상기 구성 디바이스로부터 수신되는 메시지에 포함된 무결성 필드가 유효한지 또는 무효한지의 여부를 결정하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위한 방법.

청구항 26

네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법으로서,

상기 네트워크 디바이스를 등록하기 위하여 구성 디바이스에서 상기 네트워크 디바이스와의 메시지 교환을 개시하는 단계;

상기 네트워크 디바이스로부터 수신되는 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 상기 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 단계;

만일 상기 네트워크 디바이스가 상기 등록해제 상태에 있다고 결정되면, 상기 구성 디바이스에 상기 네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신하는 단계;

상기 통신 네트워크의 네트워크 키가 상기 네트워크 디바이스에 저장되어 있는지의 여부를 결정하는 단계;

만일 상기 네트워크 키가 상기 네트워크 디바이스에 저장되어 있다고 결정되면, 상기 네트워크 키로부터 상기 네트워크 키를 수신하는 단계; 및

만일 상기 네트워크 키가 상기 네트워크 디바이스에 저장되어 있지 않다고 결정되면, 상기 네트워크 디바이스에 네트워크 키를 송신하는 단계를 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 27

제 26항에 있어서, 상기 네트워크 디바이스로부터의 응답은 상기 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 28

제 26항에 있어서, 상기 네트워크 디바이스가 상기 등록상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하는 상기 단계는,

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널일 때 상기 네트워크 디바이스가 상기 등록해제 상태에 있음을 결정하는 단계;

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널이 아닐 때 상기 네트워크 디바이스가 상기 등록 상태에 있음을 결정하는 단계; 및

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 상기 구성 디바이스에 저장되는 적어도 하나의 키의 해싱된 값과 매칭될 때 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정하는 단계 중 하나 이상을 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 29

제 26항에 있어서, 보안 단거리 통신 채널을 통해 상기 네트워크 디바이스를 등록하기 위하여 상기 네트워크 디바이스와 상기 메시지 교환을 개시하는 단계를 더 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 30

제 26항에 있어서, 상기 네트워크 디바이스를 등록해제하기 위하여 상기 구성 디바이스에서 상기 네트워크 디바이스와의 제 2 메시지 교환을 개시하는 단계;

상기 네트워크 디바이스로부터의 제 2 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지의 여부를 결정하는 단계; 및

만일 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정되면, 상기 네트워크 디바이스를 등록해제할 적어도 하나의 명령을 송신하는 단계를 더 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 31

제 30항에 있어서, 상기 네트워크 디바이스로부터의 상기 제 2 응답은 상기 네트워크 디바이스에 저장되는 적어도 하나의 파라미터의 해싱된 값을 포함하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 32

제 30항에 있어서, 상기 네트워크 디바이스로부터의 제 2 응답은 상기 네트워크 디바이스의 상태를 포함하며, 상기 상태는 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지의 여부를 표시하는, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법.

청구항 33

네트워크 디바이스를 구성하기 위한 구성 디바이스로서,

네트워크 인터페이스,

키 관리 유닛을 포함하며;

상기 키 관리 유닛은,

상기 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와의 페어링 동작들을 개시하고,

상기 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며,

만일 상기 네트워크 디바이스가 상기 등록해제 상태에 있다고 결정되면,

상기 구성 디바이스와 상기 네트워크 디바이스 간의 단거리 통신 채널을 설정하며, 그리고

상기 통신 네트워크에 통신가능하게 연결하기 위하여 상기 네트워크 디바이스를 구성하기 위한 네트워크 키를 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스에 전송하도록 구성되는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 34

제 33항에 있어서, 상기 키 관리 유닛은 상기 네트워크 디바이스가 상기 등록 상태에 있다고 결정되는 경우 상기 네트워크 디바이스를 등록해제해야 하는지를 결정하도록 추가로 구성되는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 35

제 34항에 있어서, 상기 네트워크 디바이스를 등록해제해야 하는지를 결정하도록 구성된 상기 키 관리 유닛은,

상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지 또는 상기 상이한 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고

상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정하고 상기 네트워크 디바이스를 등록해제할 것을 결정하는 것에 응답하여, 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 상기 네트워크 디바이스에 전송하도록 구성된 키 관리 유닛을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 36

제 35항에 있어서, 상기 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 전송하도록 구성된 상기 키 관리 유닛은 상기 네트워크 디바이스에서의 페어링 동작들 동안 저장되는 데이터를 삭제할 적어도 하나의 명령들을 전송하도록 구성된 키 관리 유닛을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 37

제 33항에 있어서, 상기 네트워크 디바이스와의 페어링 동작들을 개시하도록 구성되는 상기 키 관리 유닛은,

상기 네트워크 디바이스의 디바이스 식별자 및 복수의 키들을 교환하고 저장함으로써 상기 네트워크 디바이스와 페어링하고, 그리고

비대칭 암호화 방식을 사용하여 상기 네트워크 디바이스와 페어링하는 것 중 하나를 수행하도록 구성되는 키 관리 유닛을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 38

제 37항에 있어서, 상기 비대칭 암호화 방식을 사용하여 상기 네트워크 디바이스와 페어링하도록 구성된 상기 키 관리 유닛은 상기 네트워크 디바이스에 상기 구성 디바이스의 공개 키를 저장하도록 구성되는 키 관리 유닛을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 39

제 33항에 있어서, 상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하도록 구성된 상기 키 관리 유닛은,

제 1 정보를 포함하는 제 1 메시지를 상기 구성 디바이스로부터 상기 네트워크 디바이스로 전송하며; 그리고

상기 제 1 메시지에 응답하여 수신되는 제 2 메시지에 기초하여 상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하도록 구성되는 키 관리 유닛을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 40

제 33항에 있어서, 상기 단거리 통신 채널은 무결성, 암호화 및 릴레이 보호에 대한 지원을 가진 단거리 통신 채널을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

청구항 41

통신 디바이스의 네트워크 디바이스로서,

네트워크 디바이스;

등록 관리 유닛을 포함하며;

상기 등록 관리 유닛은,

단거리 통신 연결을 통해 구성 디바이스에 등록할 요청을 수신하며;

상기 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며;

만일 상기 네트워크 디바이스가 등록해제 상태에 있다고 결정되면,

상기 네트워크 디바이스가 상기 등록해제 상태에 있음을 표시하기 위하여 상기 구성 디바이스에 응답을 전송하며;

상기 네트워크 디바이스와 상기 구성 디바이스 사이에 단거리 통신 채널을 설정하며; 그리고

상기 구성 디바이스에 등록하기 위하여 상기 단거리 통신 채널을 통해 상기 구성 디바이스로부터의 적어도 하나의 키를 수신하도록 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 42

제 41항에 있어서, 상기 등록할 요청은 상기 구성 디바이스의 식별자를 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 43

제 41항에 있어서, 상기 등록할 요청은 상기 구성 디바이스의 공개 키를 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 44

제 41항에 있어서, 상기 등록할 요청은,

난수에 대한 요청; 또는

난수를 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 45

제 44항에 있어서, 상기 네트워크 디바이스에서 상기 난수를 수신하는 것에 응답하여, 상기 등록 관리 유닛은 상기 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 컴퓨팅하며 상기 구성 디바이스에 상기 해싱된 값을 송신하도록 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 46

제 44항에 있어서, 상기 네트워크 디바이스에서 상기 난수에 대한 요청을 수신하는 것에 응답하여, 상기 등록 관리 유닛은 상기 구성 디바이스에 난수를 송신하도록 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 47

제 41항에 있어서, 상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하도록 구성된 상기 등록 관리 유닛은 상기 구성 디바이스로부터 수신되는 파라미터와 상기 네트워크 디바이스에 저장되는 적어도 하나의 파라미터를 비교하도록 구성된 등록 관리 유닛을 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 48

제 41항에 있어서, 상기 구성 디바이스에 상기 응답을 송신하도록 구성된 상기 등록 관리 유닛은 상기 네트워크 디바이스에 저장되는 상기 통신 네트워크의 네트워크 키를 상기 구성 디바이스에 송신하도록 구성된 등록 관리 유닛을 더 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 49

제 48항에 있어서, 상기 네트워크 디바이스에 저장되는 상기 통신 네트워크의 네트워크 키를 송신하도록 구성된 상기 등록 관리 유닛은 상기 구성 디바이스에 상기 네트워크 키의 해싱된 값을 송신하도록 구성된 등록 관리 유닛을 더 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 50

제 41항에 있어서, 상기 단거리 통신 채널을 설정하도록 구성된 상기 등록 관리 유닛은 보안 단거리 통신 채널을 설정하기 위하여 키 합의, 키 유도 및 키 확인 절차들을 수행하도록 구성된 등록 관리 유닛을 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 51

제 41항에 있어서, 상기 등록 관리 유닛은,

상기 구성 디바이스로부터 등록해제할 요청을 상기 네트워크 디바이스에 수신하며;

상기 네트워크 디바이스가 상기 등록 상태에 있는지 또는 상기 등록 해제 상태에 있는지의 여부를 결정하며;

만일 상기 네트워크 디바이스가 상기 등록 상태에 있다고 결정되면,

상기 네트워크 디바이스가 등록해제할 상기 요청을 송신한 상기 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고

만일 상기 네트워크 디바이스가 상기 등록해제할 요청을 송신한 상기 구성 디바이스에 등록되어 있다고 결정되면, 상기 네트워크 디바이스에 저장되는 상기 적어도 하나의 키를 삭제하도록 추가로 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 52

제 51항에 있어서, 상기 네트워크 디바이스가 상기 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하도록 구성되는 상기 등록 관리 유닛은 등록 동작 동안 상기 네트워크 디바이스에 저장되는 파라미터와 상기 등록해제 요청에서 수신되는 적어도 하나의 파라미터를 비교하도록 구성된 등록 관리 유닛을 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 53

제 51항에 있어서, 상기 네트워크 디바이스가 상기 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하도록 구성된 상기 등록 관리 유닛은 상기 구성 디바이스로부터 수신되는 메시지에 포함된 무결성 필드가 유효한지 또는 무효한지의 여부를 결정하도록 구성되는 등록 관리 유닛을 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 54

네트워크 디바이스를 구성하기 위한 구성 디바이스로서,

네트워크 인터페이스;

키 관리 유닛을 포함하며;

상기 키 관리 유닛은,

상기 네트워크 디바이스를 등록하기 위하여 상기 네트워크 디바이스와의 메시지 교환을 개시하며;

상기 네트워크 디바이스로부터 수신되는 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 상기 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며;

만일 상기 네트워크 디바이스가 상기 등록해제 상태에 있다고 결정되면, 상기 구성 디바이스에 상기 네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신하며;

상기 통신 네트워크의 네트워크 키가 상기 네트워크 디바이스에 저장되어 있는지의 여부를 결정하며;

만일 상기 네트워크 키가 상기 네트워크 디바이스에 저장되어 있다고 결정되면, 상기 네트워크 키로부터 상기 네트워크 키를 수신하며; 그리고

만일 상기 네트워크 키가 상기 네트워크 디바이스에 저장되어 있지 않다고 결정되면, 상기 네트워크 디바이스에 네트워크 키를 송신하도록 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 55

제 54항에 있어서, 상기 네트워크 디바이스로부터의 응답은 상기 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 56

제 54항에 있어서, 상기 네트워크 디바이스가 상기 등록상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하도록 구성되는 상기 키 관리 유닛은,

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널일 때 상기 네트워크 디바이스가 상기 등록해제 상태에 있음을 결정하는 것,

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널이 아닐 때 상기 네트워크 디바이스가 상기 등록 상태에 있음을 결정하는 것; 및

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 상기 구성 디바이스에 저장되는 적어도 하나의 키의 해싱된 값과 매칭될 때 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정하는 것 중 하나 이상을 수행하도록 구성된 키 관리 유닛을 포함하는, 통신 디바이스의 네트워크 디바이스.

청구항 57

제 54항에 있어서, 상기 키 관리 유닛은 보안 단거리 통신 채널을 통해 상기 네트워크 디바이스를 등록하기 위하여 상기 네트워크 디바이스와 상기 메시지 교환을 개시하도록 추가로 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 58

제 54항에 있어서, 상기 키 관리 유닛은,

네트워크 디바이스를 등록해제하기 위하여 상기 구성 디바이스에서 상기 네트워크 디바이스와의 제 2 메시지 교환을 개시하며;

상기 네트워크 디바이스로부터의 제 2 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고

만일 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정되면, 상기 네트워크 디바이스를 등록해제할 적어도 하나의 명령을 송신하도록 추가로 구성되는, 통신 디바이스의 네트워크 디바이스.

청구항 59

머신 실행가능 명령들이 저장되는 비-일시적 머신 판독가능 저장 매체로서,

상기 머신 실행가능 명령들은,

상기 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와의 페어링 동작들을 구성 디바이스에 의해 개시하며;

상기 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 상기 구성 디바이스에 의해 결정하며;

만일 상기 네트워크 디바이스가 상기 등록해제 상태에 있다고 결정되면,

상기 구성 디바이스와 상기 네트워크 디바이스 사이에 단거리 통신 채널을 설정하며; 그리고

상기 통신 네트워크에 통신가능하게 연결하기 위하여 상기 네트워크 디바이스를 구성하기 위한 네트워크 키를 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스에 전송하기 위한 명령들을 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 60

제 59항에 있어서, 상기 명령들은 상기 네트워크 디바이스가 등록 상태에 있다고 결정되면, 상기 네트워크 디바이스를 등록해제해야 하는지를 결정하기 위한 명령들을 더 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 61

제 60항에 있어서, 상기 네트워크 디바이스를 등록해제해야 하는지를 결정하는 상기 명령들은,

상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지 또는 상기 상이한 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고

상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정하고 상기 네트워크 디바이스를 등록해제할 것을 결정하는 것에 응답하여, 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 상기 네트워크 디바이스에 전송하기 위한 명령들을 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 62

제 61항에 있어서, 상기 네트워크 디바이스를 등록해제할 적어도 하나의 명령들을 전송하기 위한 상기 명령들은 상기 네트워크 디바이스에서의 페어링 동작들 동안 저장되는 데이터를 삭제하기 위한 적어도 하나의 명령을 전송하기 위한 명령들을 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 63

머신 실행가능 명령들이 저장되는 비-일시적 머신-판독가능 저장 매체로서,

상기 머신 실행가능 명령들은,

상기 네트워크 디바이스를 등록하기 위하여 구성 디바이스에서 상기 네트워크 디바이스와의 메시지 교환을 개시하며;

상기 네트워크 디바이스로부터 수신되는 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 상기 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며;

만일 상기 네트워크 디바이스가 상기 등록해제 상태에 있다고 결정되면, 상기 구성 디바이스에 상기 네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신하며;

상기 통신 네트워크의 네트워크 키가 상기 네트워크 디바이스에 저장되어 있는지의 여부를 결정하며;

만일 상기 네트워크 키가 상기 네트워크 디바이스에 저장되어 있다고 결정되면, 상기 네트워크 디바이스로부터 상기 네트워크 키를 수신하며; 그리고

만일 상기 네트워크 키가 상기 네트워크 디바이스에 저장되어 있지 않다고 결정되면, 상기 네트워크 디바이스에 네트워크 키를 송신하기 위한 명령들을 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 64

제 63항에 있어서, 상기 네트워크 디바이스로부터의 응답은 상기 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 65

제 63항에 있어서, 상기 네트워크 디바이스가 상기 등록상태에 있는지 또는 상기 등록해제 상태에 있는지의 여부를 결정하기 위한 명령들은,

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널일 때 상기 네트워크 디바이스가 상기 등록해제 상태에 있음을 결정하기 위한 명령들,

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널이 아닐 때 상기 네트워크 디바이스가 상기 등록 상태에 있음을 결정하기 위한 명령들; 및

상기 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 상기 구성 디바이스에 저장되는 적어도 하나의 키의 해싱된 값과 매칭될 때 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정하기 위한 명령들 중 적어도 하나를 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 66

제 63항에 있어서, 상기 명령들은 보안 단거리 통신 채널을 통해 상기 네트워크 디바이스를 등록하기 위하여 상기 네트워크 디바이스와 상기 메시지 교환을 개시하기 위한 명령들을 더 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 67

제 63항에 있어서, 상기 명령들은,

네트워크 디바이스를 등록해제하기 위하여 상기 구성 디바이스에서 상기 네트워크 디바이스와의 제 2 메시지 교환을 개시하며;

상기 네트워크 디바이스로부터의 제 2 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고

만일 상기 네트워크 디바이스가 상기 구성 디바이스에 등록되어 있다고 결정되면, 상기 네트워크 디바이스를 등록해제할 적어도 하나의 명령을 송신하기 위한 명령들을 더 포함하는, 비-일시적 머신 판독가능 저장 매체.

청구항 68

네트워크 디바이스를 구성하기 위한 구성 디바이스로서,

상기 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와 페어링 동작들을 개시하기 위한 수단;

상기 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하기 위한 수단;

만일 상기 네트워크 디바이스가 등록해제 상태에 있다고 결정되면,

상기 구성 디바이스와 상기 네트워크 디바이스 간의 단거리 통신 채널을 설정하기 위한 수단; 및

상기 통신 네트워크에 통신가능하게 연결하기 위하여 상기 네트워크 디바이스를 구성하기 위한 네트워크 키를 상기 단거리 통신 채널을 통해 상기 네트워크 디바이스에 전송하기 위한 수단을 포함하는, 네트워크 디바이스를 구성하기 위한 구성 디바이스.

명 세 서

기 술 분 야

[0001] 본 출원은 2012년 3월 20일에 출원된 미국 가출원번호 제61/613,438호, 2012년 4월 23일에 출원된 미국 가출원번호 제61/637,234호 및 2013년 3월 15일에 출원된 미국 출원번호 제13/843,395호의 우선권을 주장한다.

[0002] 본 요지의 실시예들은 일반적으로 통신 네트워크 분야, 특히 단거리 무선 통신을 사용하는 네트워크 보안성 구성에 관한 것이다.

배 경 기 술

[0003] 통신 네트워크들에 있어서, 통신 네트워크에서 디바이스들 간의 보안 연관은 푸시 버튼 구성 및/또는 사용자 구성된 패스프레이즈/키 등을 사용하여 실현될 수 있다. 푸시 버튼 구성에서, 사용자는 특정 시간내에 디바이스들 각각의 버튼을 푸시할 수 있으며, 디바이스들은 서로 연관될 수 있다. 사용자 구성된 패스프레이즈/키 기술에서, 사용자는 통신 네트워크 키로 변환될 수 있거나 또는 네트워크 키로서 직접 구성될 수 있는, 특정 규칙들을 가진 ASCII 인코딩된 패스프레이즈를 입력할 수 있다. 그러나, 사용자 구성된 패스프레이즈/키를 다수의 네트워크 디바이스들내에 수동으로 입력시키는 것은 번거롭다. 또한, 사용자 구성된 패스프레이즈들은 디렉토리 공격들에 약할 수 있으며, 네트워크 키들은 종종 수동으로 구성하기에 너무 복잡하다. 푸시 버튼 구성은 매우 비보안적이며, 네트워크의 디바이스에 대한 물리적 액세스를 통해, 푸시 버튼은 네트워크의 디바이스들을 연관시키는 악의적인 사용자들의 제어하에서 디바이스를 연관시켜고 그것에 의하여 네트워크와 연관된 보안성 세팅들을 획득하도록 트리거될 수 있다.

발명의 내용

[0004] 네트워크 디바이스들을 구성하기 위한 다양한 실시예들이 개시된다. 일 실시예들에서, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법은 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와의 페어링 동작들을 구성 디바이스에 의해 개시하는 단계; 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 구성 디바이스에 의해 결정하는 단계; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스와 네트워크 디바이스 사이에 단거리 통신 채널을 설정하는 단계; 및 통신 네트워크에 통신가능하게 연결하기 위하여 네트워크 디바이스를 구성하기 위한 네트워크 키를 단거리 통신 채널을 통해 네트워크 디바이스에 전송하는 단계를 포함한다.

[0005] 일 실시예들에서, 방법은 네트워크 디바이스가 등록 상태에 있다고 결정되면, 네트워크 디바이스를 등록해제해야 하는지를 결정하는 단계를 더 포함한다.

[0006] 일부 실시예들에서, 네트워크 디바이스를 등록해제해야 하는지를 결정하는 단계는 네트워크 디바이스가 구성 디바이스에 등록되어 있는지 또는 상이한 구성 디바이스에 등록되어 있는지의 여부를 결정하는 단계; 및 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정하고 네트워크 디바이스를 등록해제할 것을 결정하는 것에 응

답하여, 단거리 통신 채널을 통해 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 네트워크 디바이스에 전송하는 단계를 포함한다.

[0007] 일부 실시예들에서, 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 전송하는 상기 단계는 네트워크 디바이스에서의 페어링 동작들 동안 저장되는 데이터를 삭제할 적어도 하나의 명령들을 전송하는 단계를 포함한다.

[0008] 일부 실시예들에서, 네트워크 디바이스와의 페어링 동작들을 개시하는 상기 단계는 네트워크 디바이스의 디바이스 식별자 및 복수의 키들을 교환하고 저장함으로써 네트워크 디바이스와 페어링하는 단계; 및 비대칭 암호화 방식을 사용하여 네트워크 디바이스와 페어링하는 단계 중 하나를 포함한다.

[0009] 일부 실시예들에서, 비대칭 암호화 방식을 사용하여 네트워크 디바이스와 페어링하는 상기 단계는 네트워크 디바이스에 구성 디바이스의 공개 키를 저장하는 단계를 포함한다.

[0010] 일부 실시예들에서, 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 상기 단계는 제 1 정보를 포함하는 제 1 메시지를 구성 디바이스로부터 네트워크 디바이스로 전송하는 단계; 및 제 1 메시지에 응답하여 수신되는 제 2 메시지에 기초하여 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 단계를 포함한다.

[0011] 일부 실시예들에서, 단거리 통신 연결은 근거리 무선 통신(NFC) 연결이다.

[0012] 일부 실시예들에서, 단거리 통신 연결은 Bluetooth 통신 연결, ZigBee 통신 연결 및 무선 근거리 통신망(WLAN) 통신 연결 중 하나이다.

[0013] 일부 실시예들에서, 단거리 통신 채널은 무결성, 암호화 및 리플레이 보호에 대한 지원을 가진 보안 단거리 통신 채널을 포함한다.

[0014] 일부 실시예들에서, 리플레이 보호는 시퀀스 번호들을 사용하여 구현된다.

[0015] 일부 실시예들에서, 리플레이 보호는 시간스탬프들을 사용하여 구현된다.

[0016] 일부 실시예들에서, 네트워크 디바이스를 구성하기 위한 방법은 단거리 통신 연결을 통해 구성 디바이스에 등록할, 구성 디바이스로부터의 요청을 통신 네트워크의 네트워크 디바이스에서 수신하는 단계; 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 단계; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 네트워크 디바이스가 등록해제 상태에 있음을 표시하기 위하여 구성 디바이스에 응답을 전송하는 단계; 네트워크 디바이스와 구성 디바이스 사이에 단거리 통신 채널을 설정하는 단계; 및 구성 디바이스에 등록하기 위하여 단거리 통신 채널을 통해 구성 디바이스로부터의 적어도 하나의 키를 수신하는 단계를 포함한다.

[0017] 일부 실시예들에서, 등록할 요청은 구성 디바이스의 식별자를 포함한다.

[0018] 일부 실시예들에서, 등록할 요청은 구성 디바이스의 공개 키를 포함한다.

[0019] 일부 실시예들에서, 등록할 요청은 난수에 대한 요청; 또는 난수를 포함한다.

[0020] 일부 실시예들에서, 방법은 네트워크 디바이스에서 난수를 수신하는 것에 응답하여, 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 컴퓨팅하는 단계 및 구성 디바이스에 해싱된 값을 송신하는 단계를 포함한다.

[0021] 일부 실시예들에서, 방법은 네트워크 디바이스에서 난수에 대한 요청을 수신하는 것에 응답하여, 구성 디바이스에 난수를 송신하는 단계를 포함한다.

[0022] 일부 실시예들에서, 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 상기 단계는 구성 디바이스로부터 수신되는 파라미터와 네트워크 디바이스에 저장되는 적어도 하나의 파라미터를 비교하는 단계를 포함한다.

[0023] 일부 실시예들에서, 구성 디바이스에 응답을 송신하는 상기 단계는 네트워크 디바이스에 저장되는 통신 네트워크의 네트워크 키를 구성 디바이스에 송신하는 단계를 포함한다.

[0024] 일부 실시예들에서, 네트워크 디바이스에 저장되는 통신 네트워크의 네트워크 키를 송신하는 상기 단계는 구성 디바이스에 네트워크 키의 해싱된 값을 송신하는 단계를 더 포함한다.

[0025] 일부 실시예들에서, 단거리 통신 채널을 설정하는 상기 단계는 보안 단거리 통신 채널을 설정하기 위하여 키 합의, 키 유도 및 키 확인 절차들을 수행하는 단계를 포함한다.

[0026] 일부 실시예들에서, 방법은 구성 디바이스로부터 등록해제할 요청을 네트워크 디바이스에 수신하는 단계; 네트워크 디바이스가 등록 상태에 있는지 또는 등록 해제 상태에 있는지의 여부를 결정하는 단계; 만일 네트워크 디바이스가 등록 상태에 있다고 결정되면, 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있는지의 여부를 결정하는 단계; 및 만일 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정되면, 네트워크 디바이스에 저장되는 적어도 하나의 키를 삭제하는 단계를 더 포함한다.

[0027] 일 실시예들에서, 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하는 상기 단계는 등록 동작 동안 네트워크 디바이스에 저장되는 파라미터와 등록해제 요청에서 수신되는 적어도 하나의 파라미터를 비교하는 단계를 포함한다.

[0028] 일부 실시예들에서, 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하는 상기 단계는 구성 디바이스로부터 수신되는 메시지에 포함된 무결성 필드가 유효한지 또는 무효한지의 여부를 결정하는 단계를 포함한다.

[0029] 일부 실시예들에서, 네트워크 디바이스를 구성하기 위하여 중간 구성 디바이스를 사용하기 위한 방법은 네트워크 디바이스를 등록하기 위하여 구성 디바이스에서 네트워크 디바이스와의 메시지 교환을 개시하는 단계; 네트워크 디바이스로부터 수신되는 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 단계; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스에 네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신하는 단계; 통신 네트워크의 네트워크 키가 네트워크 디바이스에 저장되는지의 여부를 결정하는 단계; 만일 네트워크 키가 네트워크 디바이스에 저장되어 있다고 결정되면, 네트워크 디바이스로부터 네트워크 키를 수신하는 단계; 및 만일 네트워크 키가 네트워크 디바이스에 저장되지 않는다고 결정되면, 네트워크 디바이스에 네트워크 키를 송신하는 단계를 포함한다.

[0030] 일부 실시예들에서, 네트워크 디바이스로부터의 응답은 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 포함한다.

[0031] 일부 실시예들에서, 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하는 상기 단계는 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널일 때 네트워크 디바이스가 등록해제 상태에 있음을 결정하는 단계; 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널이 아닐 때 네트워크 디바이스가 등록 상태에 있음을 결정하는 단계; 및 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 구성 디바이스에 저장되는 적어도 하나의 키의 해싱된 값과 매칭될 때 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정하는 단계 중 하나 이상을 포함한다.

[0032] 일부 실시예들에서, 방법은 보안 단거리 통신 채널을 통해 네트워크 디바이스를 등록하기 위하여 네트워크 디바이스와 메시지 교환을 개시하는 단계를 더 포함한다.

[0033] 일부 실시예들에서, 방법은 네트워크 디바이스를 등록해제하기 위하여 구성 디바이스에서 네트워크 디바이스와의 제 2 메시지 교환을 개시하는 단계; 네트워크 디바이스로부터의 제 2 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 네트워크 디바이스가 구성 디바이스에 등록되어 있는지의 여부를 결정하는 단계; 및 만일 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정되면, 네트워크 디바이스를 등록해제할 적어도 하나의 명령을 송신하는 단계를 더 포함한다.

[0034] 일부 실시예들에서, 네트워크 디바이스로부터의 제 2 응답은 네트워크 디바이스에 저장되는 적어도 하나의 파라미터의 해싱된 값을 포함한다.

[0035] 일부 실시예들에서, 네트워크 디바이스로부터의 제 2 응답은 네트워크 디바이스의 상태를 포함하며, 상태는 네트워크 디바이스가 구성 디바이스에 등록되어 있는지의 여부를 표시한다.

[0036] 일부 실시예들에서, 네트워크 디바이스를 구성하기 위한 구성 디바이스는 네트워크 인터페이스, 키 관리 유닛을 포함하며; 키 관리 유닛은 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와의 페어링 동작들을 개시하고, 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며, 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스와 네트워크 디바이스 사이에 단거리 통신 채널을 설정하며, 그리고 통신 네트워크에 통신가능하게 연결하기 위하여 네트워크 디바이

스를 구성하기 위한 네트워크 키를 단거리 통신 채널을 통해 네트워크 디바이스에 전송하도록 구성된다.

[0037] 일부 실시예들에서, 키 관리 유닛은 네트워크 디바이스가 등록 상태에 있다고 결정되는 경우 네트워크 디바이스를 등록해제해야 하는지를 결정하도록 추가로 구성된다.

[0038] 일부 실시예들에서, 네트워크 디바이스를 등록해제해야 하는지를 결정하도록 구성된 키 관리 유닛은 네트워크 디바이스가 구성 디바이스에 등록되어 있는지 또는 상이한 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정하고 네트워크 디바이스를 등록해제할 것을 결정하는 것에 응답하여, 단거리 통신 채널을 통해 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 네트워크 디바이스에 전송하도록 구성된 키 관리 유닛을 포함한다.

[0039] 일부 실시예들에서, 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 전송하도록 구성된 키 관리 유닛은 네트워크 디바이스에서의 페어링 동작들 동안 저장되는 데이터를 삭제하기 위한 적어도 하나의 명령들을 전송하도록 구성된 키 관리 유닛을 포함한다.

[0040] 일부 실시예들에서, 네트워크 디바이스와의 페어링 동작들을 개시하도록 구성되는 키 관리 유닛은 네트워크 디바이스의 디바이스 식별자 및 복수의 키들을 교환하고 저장함으로써 네트워크 디바이스와 페어링하는 것 및 비대칭 암호화 방식을 사용하여 네트워크 디바이스와 페어링하는 것 중 하나를 수행하도록 구성되는 키 관리 유닛을 포함한다.

[0041] 일부 실시예들에서, 비대칭 암호화 방식을 사용하여 네트워크 디바이스와 페어링하도록 구성된 키 관리 유닛은 네트워크 디바이스에 구성 디바이스의 공개 키를 저장하도록 구성되는 키 관리 유닛을 포함한다.

[0042] 일부 실시예들에서, 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하도록 구성된 키 관리 유닛은 제 1 정보를 포함하는 제 1 메시지를 구성 디바이스로부터 네트워크 디바이스로 전송하며; 그리고 제 1 메시지에 응답하여 수신되는 제 2 메시지에 기초하여 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하도록 구성되는 키 관리 유닛을 포함한다.

[0043] 일부 실시예들에서, 단거리 통신 연결 채널은 무결성, 암호화 및 릴레이 보호에 대한 지원을 가지는 단거리 통신 채널을 포함한다.

[0044] 일부 실시예들에서, 통신 네트워크의 네트워크 디바이스는 네트워크 인터페이스; 및 등록 관리 유닛을 포함하며; 등록 관리 유닛은, 단거리 통신 연결을 통해 구성 디바이스에 등록할 요청을 수신하며; 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 네트워크 디바이스가 등록해제 상태에 있음을 표시하기 위하여 구성 디바이스에 응답을 전송하며; 네트워크 디바이스와 구성 디바이스 사이에 단거리 통신 채널을 설정하며; 그리고 구성 디바이스에 등록하기 위하여 단거리 통신 채널을 통해 구성 디바이스로부터의 적어도 하나의 키를 수신하도록 구성된다.

[0045] 일부 실시예들에서, 등록할 요청은 구성 디바이스의 식별자를 포함한다.

[0046] 일부 실시예들에서, 등록할 요청은 구성 디바이스의 공개 키를 포함한다.

[0047] 일부 실시예들에서, 등록할 요청은 난수에 대한 요청; 또는 난수를 포함한다.

[0048] 일부 실시예들에서, 네트워크 디바이스에서 난수를 수신하는 것에 응답하여, 등록 관리 유닛은 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 컴퓨팅하며 구성 디바이스에 해싱된 값을 송신하도록 구성된다.

[0049] 일부 실시예들에서, 네트워크 디바이스에서 난수에 대한 요청을 수신하는 것에 응답하여, 등록 관리 유닛은 구성 디바이스에 난수를 송신하도록 구성된다.

[0050] 일부 실시예들에서, 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하도록 구성된 등록 관리 유닛은 구성 디바이스로부터 수신되는 파라미터와 네트워크 디바이스에 저장되는 적어도 하나의 파라미터를 비교하도록 구성된 등록 관리 유닛을 포함한다.

[0051] 일부 실시예들에서, 구성 디바이스에 응답을 송신하도록 구성된 등록 관리 유닛은 네트워크 디바이스에 저장되는 통신 네트워크의 네트워크 키를 구성 디바이스에 송신하도록 구성된 등록 관리 유닛을 포함한다.

[0052] 일부 실시예들에서, 네트워크 디바이스에 저장되는 통신 네트워크의 네트워크 키를 송신하도록 구성된 등록 관리 유닛은 구성 디바이스에 네트워크 키의 해싱된 값을 송신하도록 구성된 등록 관리 유닛을 더 포함한다.

[0053] 일부 실시예들에서, 단거리 통신 채널을 설정하도록 구성된 등록 관리 유닛은 보안 단거리 통신 채널을 설정하기 위하여 키 합의, 키 유도 및 키 확인 절차들을 수행하도록 구성된 등록 관리 유닛을 포함한다.

[0054] 일부 실시예들에서, 등록 관리 유닛은 구성 디바이스로부터 등록해제할 요청을 네트워크 디바이스에 수신하며; 네트워크 디바이스가 등록 상태에 있는지 또는 등록 해제 상태에 있는지의 여부를 결정하며; 만일 네트워크 디바이스가 등록 상태에 있다고 결정되면, 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고 만일 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있으면, 네트워크 디바이스에 저장되는 적어도 하나의 키를 삭제하도록 추가로 구성된다.

[0055] 일부 실시예들에서, 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하도록 구성되는 등록 관리 유닛은 등록 동작 동안 네트워크 디바이스에 저장되는 파라미터와 등록해제 요청에서 수신되는 적어도 하나의 파라미터를 비교하도록 구성된 등록 관리 유닛을 포함한다.

[0056] 일부 실시예들에서, 네트워크 디바이스가 등록해제할 요청을 송신한 구성 디바이스에 등록되어 있다고 결정하도록 구성된 등록 관리 유닛은 구성 디바이스로부터 수신되는 메시지에 포함된 무결성 필드가 유효한지 또는 무효한지의 여부를 결정하도록 구성되는 등록 관리 유닛을 포함한다.

[0057] 일부 실시예들에서, 네트워크 디바이스를 구성하기 위한 구성 디바이스는 네트워크 인터페이스; 및 키 관리 유닛을 포함하며; 키 관리 유닛은 네트워크 디바이스를 등록하기 위하여 네트워크 디바이스와의 메시지 교환을 개시하며; 네트워크 디바이스로부터 수신되는 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스에 네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신하며; 통신 네트워크의 네트워크 키가 네트워크 디바이스에 저장되는지의 여부를 결정하며; 만일 네트워크 키가 네트워크 디바이스에 저장되어 있다고 결정되면, 네트워크 디바이스로부터 네트워크 키를 수신하며; 그리고 만일 네트워크 키가 네트워크 디바이스에 저장되지 않는다고 결정되면, 네트워크 디바이스에 네트워크 키를 송신하도록 구성된다.

[0058] 일부 실시예들에서, 네트워크 디바이스로부터의 응답은 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 포함한다.

[0059] 일부 실시예들에서, 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하도록 구성되는 키 관리 유닛은 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널일 때 네트워크 디바이스가 등록해제 상태에 있음을 결정하는 것, 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널이 아닐 때 네트워크 디바이스가 등록 상태에 있음을 결정하는 것; 및 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 구성 디바이스에 저장되는 적어도 하나의 키의 해싱된 값과 매칭될 때 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정하는 것 중 하나 이상을 수행하도록 구성된 키 관리 유닛을 포함한다.

[0060] 일부 실시예들에서, 키 관리 유닛은 보안 단거리 통신 채널을 통해 네트워크 디바이스를 등록하기 위하여 네트워크 디바이스와 메시지 교환을 개시하도록 추가로 구성된다.

[0061] 일부 실시예들에서, 키 관리 유닛은 네트워크 디바이스를 등록해제하기 위하여 구성 디바이스에서 네트워크 디바이스와의 제 2 메시지 교환을 개시하며; 네트워크 디바이스로부터의 제 2 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 네트워크 디바이스가 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고 만일 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정되면, 네트워크 디바이스를 등록해제할 적어도 하나의 명령을 송신하도록 추가로 구성된다.

[0062] 일부 실시예들은 머신 실행가능 명령들이 저장되는 비-일시적 머신 판독가능 저장 매체에 관한 것으로서, 머신 실행가능 명령들은 네트워크 디바이스와의 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와의 페어링 동작들을 구성 디바이스에 의해 개시하며; 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 구성 디바이스에 의해 결정하며; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스와 네트워크 디바이스 사이에 단거리 통신 채널을 설정하며; 그리고 통신 네트워크에 통신가능하게 연결하기 위하여 네트워크 디바이스를 구성하기 위한 네트워크 키를 단거리 통신 채널을 통해 네트워크 디바이스에 전송하기 위한 명령들을 포함한다.

[0063] 일부 실시예들에서, 명령들은 네트워크 디바이스가 등록 상태에 있다고 결정되면, 네트워크 디바이스를 등록해

제해야 하는지를 결정하기 위한 명령들을 더 포함한다.

[0064] 일부 실시예들에서, 네트워크 디바이스를 등록해제해야 하는지를 결정하는 상기 명령들은 네트워크 디바이스가 구성 디바이스에 등록되어 있는지 또는 상이한 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정하고 네트워크 디바이스를 등록해제할 것을 결정하는 것에 응답하여, 단거리 통신 채널을 통해 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 네트워크 디바이스에 전송하기 위한 명령들을 포함한다.

[0065] 일부 실시예들에서, 네트워크 디바이스를 등록해제할 적어도 하나의 메시지를 전송하기 위한 명령들은 네트워크 디바이스에서의 페어링 동작들 동안 저장되는 데이터를 삭제하기 위한 적어도 하나의 명령을 전송하기 위한 명령들을 포함한다.

[0066] 일부 실시예들은 머신 실행가능 명령들이 저장되는 비-일시적 머신-판독가능 저장 매체에 관한 것이며, 머신 실행가능 명령들은 네트워크 디바이스를 등록하기 위하여 구성 디바이스에서 네트워크 디바이스와의 메시지 교환을 개시하며; 네트워크 디바이스로부터 수신되는 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하며; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스에 네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신하며; 통신 네트워크의 네트워크 키가 네트워크 디바이스에 저장되는지의 여부를 결정하며; 만일 네트워크 키가 네트워크 디바이스에 저장되어 있다고 결정되면, 네트워크 키로부터 네트워크 키를 수신하며; 그리고 만일 네트워크 키가 네트워크 디바이스에 저장되지 않는다고 결정되면, 네트워크 디바이스에 네트워크 키를 송신하기 위한 명령들을 포함한다.

[0067] 일부 실시예들에서, 네트워크 디바이스로부터의 응답은 네트워크 디바이스에 저장되는 적어도 하나의 키의 해싱된 값을 포함한다.

[0068] 일부 실시예들에서, 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하기 위한 상기 명령들은 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널일 때 네트워크 디바이스가 등록해제 상태에 있음을 결정하기 위한 명령들; 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 널이 아닐 때 네트워크 디바이스가 등록 상태에 있음을 결정하기 위한 명령들; 및 네트워크 디바이스로부터 수신되는 적어도 하나의 키의 해싱된 값이 구성 디바이스에 저장되는 적어도 하나의 키의 해싱된 값과 매칭될 때 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정하기 위한 명령들 중 적어도 하나를 포함한다.

[0069] 일부 실시예들에서, 명령들은 보안 단거리 통신 채널을 통해 네트워크 디바이스를 등록하기 위하여 네트워크 디바이스와 메시지 교환을 개시하기 위한 명령들을 더 포함한다.

[0070] 일부 실시예들에서, 명령들은 네트워크 디바이스를 등록해제하기 위하여 구성 디바이스에서 네트워크 디바이스와의 제 2 메시지 교환을 개시하며; 네트워크 디바이스로부터의 제 2 응답에서 수신되는 적어도 하나의 파라미터에 기초하여 네트워크 디바이스가 구성 디바이스에 등록되어 있는지의 여부를 결정하며; 그리고 만일 네트워크 디바이스가 구성 디바이스에 등록되어 있다고 결정되면, 네트워크 디바이스를 등록해제할 적어도 하나의 명령을 송신하기 위한 명령들을 더 포함한다.

[0071] 일부 실시예들에서, 네트워크 디바이스를 구성하기 위한 구성 디바이스는 네트워크 디바이스와 단거리 통신 연결을 통해 통신 네트워크의 네트워크 디바이스와 페어링 동작들을 개시하기 위한 수단; 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하기 위한 수단; 만일 네트워크 디바이스가 등록해제 상태에 있다고 결정되면, 구성 디바이스와 네트워크 디바이스 사이에 단거리 통신 채널을 설정하기 위한 수단; 및 통신 네트워크에 통신가능하게 연결하기 위하여 네트워크 디바이스를 구성하기 위한 네트워크 키를 단거리 통신 채널을 통해 네트워크 디바이스에 전송하기 위한 수단을 포함한다.

도면의 간단한 설명

[0072] 도 1은 통신 네트워크에서 키 반송 디바이스 및 네트워크 디바이스들의 예시적인 블록도를 도시한다.

도 2는 네트워크 디바이스를 구성하는 예시적인 동작들의 흐름도를 예시한다.

도 3은 제 1 및 제 2 구성 기술들을 사용하여 네트워크 디바이스를 구성하는 예시적인 동작들의 흐름도를 예시한다.

도 4는 제 3, 제 4 및 제 5 구성 기술들을 사용하여 네트워크 디바이스를 구성하는 예시적인 동작들의 흐름도를 예시한다.

도 5는 제 1 구성 기술을 사용하여 네트워크 디바이스를 등록하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 6은 제 1 구성 기술을 사용하여 네트워크 디바이스를 등록해제하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 7은 제 2 구성 기술을 사용하여 네트워크 디바이스를 등록하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 8은 제 2 구성 기술을 사용하여 네트워크 디바이스를 등록해제하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 9, 도 10, 도 11 및 도 12는 제 3 구성 기술을 사용하여 네트워크 디바이스를 등록하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 13은 제 3 구성 기술을 사용하여 네트워크 디바이스를 등록해제하는 제 1 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 14는 제 3 구성 기술을 사용하여 네트워크 디바이스를 등록해제하는 제 2 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 15, 도 16 및 도 17은 제 4 구성 기술을 사용하여 네트워크 디바이스를 등록하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 18 및 도 19는 제 4 구성 기술을 사용하여 네트워크 디바이스를 등록해제하는 제 1 옵션의 예시적인 구성들의 시퀀스 다이어그램을 예시한다.

도 20은 제 4 구성 기술을 사용하여 네트워크 디바이스를 등록해제하는 제 2 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 21 및 도 22는 제 5 구성 기술을 사용하여 네트워크 디바이스를 등록하는 예시적인 동작들의 시퀀스 다이어그램을 예시한다.

도 23은 제 5 구성 기술을 사용하여 네트워크 디바이스를 등록하는 예시적인 구성들의 시퀀스 다이어그램을 예시한다.

도 24는 예시적인 네트워크 디바이스를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0073] 이하의 설명은 본 발명의 요지의 기술들을 사용하는 예시적인 시스템들, 방법들, 기술들, 명령 시퀀스들 및 컴퓨터 프로그램 제품들을 포함한다. 그러나, 설명된 실시예들이 이들 특정 세부사항들 없이 실시될 수 있음이 이해된다. 예를들어, 비록 예들이 통신 네트워크에서 네트워크 디바이스를 보안적으로 구성하는 키 반송 디바이스를 지칭할지라도, 다른 구현들에서는 키 반송 디바이스가 하나 이상의 통신 네트워크들에서 다수의 네트워크 디바이스들을 동시에 구성할 수 있다. 다른 사례들에서, 설명을 애매하게 하지 않도록 하기 위하여, 공지된 명령 인스턴스들, 프로토콜들, 명령들 및 기술들은 상세하게 제시되지 않았다.

[0074] 일부 실시예들에서, 단거리 통신을 지원하는 키 반송 디바이스는 보안 통신 채널을 통해 네트워크 디바이스들에 네트워크 키를 송신함으로써 통신 네트워크의 네트워크 디바이스들을 보안적으로 구성할 수 있다. 키 반송 디바이스는 네트워크 디바이스 및/또는 키 반송 디바이스에서 페어링 데이터를 교환하고 페어링 데이터를 저장함으로써 키 반송 디바이스에 네트워크 디바이스를 등록할 수 있다. 키 반송 디바이스는 일단 네트워크 디바이스가 키 반송 디바이스에 등록되어 있으면 네트워크 디바이스에 통신 네트워크의 네트워크 키를 송신함으로써 통신 네트워크를 이용하여 네트워크 디바이스를 보안적으로 구성할 수 있다. 키 반송 디바이스는 네트워크 디바이스 및/또는 키 반송 디바이스에 저장되는 네트워크 키 및 페어링 데이터를 삭제함으로써 키 반송 디바이스로부터 네트워크 디바이스를 등록해제할 수 있다.

[0075] 일부 실시예들에서, 키 반송 디바이스는 네트워크 디바이스를 보안적으로 구성하기 위하여 하나 이상의 구성 기

술들을 활용할 수 있다. 예를들어, 제 1 구성 기술에서, 키 반송 디바이스는 키 반송 디바이스 및 네트워크 디바이스 둘다에서 페어링 데이터로서 무결성 키, 암호화 키 및 시퀀스 번호를 저장함으로써 키 반송 디바이스에 네트워크 디바이스를 등록할 수 있다. 또한, 키 반송 디바이스는 페어링 데이터의 부분으로서 네트워크 디바이스의 디바이스 식별자를 저장할 수 있으며, 네트워크 디바이스는 페어링 데이터의 부분으로써 키 반송 디바이스의 디바이스 식별자를 저장할 수 있다. 제 2 구성 기술에서, 키 반송 디바이스 및 네트워크 디바이스는 네트워크 디바이스에서 페어링 데이터로서 키 반송 디바이스의 공개 키를 저장함으로써 페어링할 수 있다. 이후, 제 1 및 제 2 구성 기술들 둘다에서, 키 반송 디바이스는 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하여 네트워크 디바이스를 등록하거나 또는 등록해제하기 위하여 (또는 현재의 구성을 유지하기 위하여) 네트워크 디바이스와 하나 이상의 메시지들을 교환할 수 있다. 제 3 구성 기술에서, 키 반송 디바이스 및 네트워크 디바이스는 페어링 데이터로서 보안 키(예를들어, 등록 키)를 저장함으로써 페어링될 수 있다. 키 반송 디바이스는 네트워크 디바이스가 페어링 데이터에 기초하여 등록 상태에 있는지 또는 등록해제 상태에 있는지를 결정하기 위하여 하나 이상의 메시지들을 보안적으로 교환할 수 있다. 일례에서, 키 반송 디바이스 및 네트워크 디바이스는 페어링 데이터(예를들어, 등록 키) 및/또는 네트워크 키를 포함하는 메시지들을 보안적으로 교환하기 위하여 해싱 알고리즘을 활용할 수 있다. 따라서, 네트워크 디바이스가 등록해제 상태에 있는지를 또는 등록 상태에 있는지의 여부를 결정하는 것에 기초하여, 키 반송 디바이스는 네트워크 디바이스를 등록하거나 또는 등록해제할 수 있다(또는 현재의 구성을 유지할 수 있다). 제 4 구성 기술에서, 키 반송 디바이스 및 네트워크 디바이스는 키 반송 디바이스 및 네트워크 디바이스 둘다에 보안 키(예를들어, 등록 키)를 저장하고 페어링 데이터로서 네트워크 디바이스에 상태 필드를 저장함으로써 페어링될 수 있다. 제 4 구성 기술에서, 네트워크 디바이스는 해싱 알고리즘을 사용하여, 키 반송 디바이스와 페어링 데이터(예를들어, 등록 키) 및/또는 네트워크 키를 포함하는 하나 이상의 메시지들을 보안적으로 교환할 수 있다. 네트워크 디바이스는 상태 필드를 사용하여 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 키 반송 디바이스에 표시할 수 있으며 따라서 네트워크 디바이스를 등록해야 하는지 또는 등록해제 해야 하는지를 결정할 수 있다. 제 5 구성 기술은 페어링 데이터 및/또는 네트워크 키를 포함하는 임의의 메시지들을 교환하기 전에 네트워크 디바이스 및 키 반송 디바이스가 보안 통신 채널을 설정할 수 있다는 것을 제외하고 제 4 구성 기술과 유사할 수 있다. 네트워크 디바이스 및 키 반송 디바이스는 보안 통신 채널을 통해 페어링 데이터 및/또는 네트워크 키를 포함하는 메시지들을 보안적으로 교환할 수 있다. 네트워크 디바이스를 보안적으로 구성하기 위하여 키 반송 디바이스를 활용하는 구성 기술들은 도 1-도 24와 관련하여 이하에서 추가로 설명될 것이다.

[0076] 도 1은 통신 네트워크에서 키 반송 디바이스 및 네트워크 디바이스들의 예시적인 블록도들을 도시한다. 도 1은 통신 네트워크(100)를 도시한다. 예를들어, 통신 네트워크(100)는 하나 이상의 네트워크 통신 표준들(예를들어, IEEE 802.3, IEEE 802.11 또는 Wi-Fi®, IEEE P1905.1 , Broadband over Power Line network standards, Ethernet over Coaxial cable, ZigBee® 또는 IEEE 802.15.4 등)을 사용하여 홈 또는 기업 네트워크 시스템일 수 있다. 통신 네트워크(100)는 키 관리 유닛(104) 및 단거리 통신 유닛(106)을 가진 키 반송 디바이스(102)를 포함한다. 통신 네트워크(100)는 또한 등록 관리 유닛(109) 및 단거리 통신 유닛(110)을 가진 네트워크 디바이스(108), 등록 관리 유닛(117) 및 단거리 통신 유닛(118)을 가진 네트워크 디바이스(116), 및 등록 관리 유닛(113) 및 단거리 통신 유닛(114)을 가진 네트워크 디바이스(112)를 포함한다. 일 구현에서, 키 반송 디바이스(102)는 키 관리 유닛(104) 및 단거리 통신 유닛(106)을 포함하는 통신 유닛(예를들어, 집적회로, 시스템-온-칩(system-on-a-chip) 또는 회로 보드)를 포함할 수 있다.

[0077] 키 반송 디바이스(102)는 단거리 통신을 지원하고 통신 네트워크(100)를 관리하는 다양한 타입들의 네트워크 디바이스들, 예를들어, 모바일 폰, 태블릿 컴퓨터, 노트북 컴퓨터, 스마트 원격 제어 디바이스 등 중 하나일 수 있다. 키 반송 디바이스(102)는 통상적으로 네트워크 디바이스의 상태, 등록 확인, 등록 해제 확인 등을 사용자에게 디스플레이할 디스플레이 유닛을 포함한다. 키 반송 디바이스의 단거리 통신 유닛(106)은 네트워크 디바이스들(108, 116 및 112)과 대역외 통신 링크 (즉, 통신 네트워크(100)에 의해 사용되는 대역과 상이한 주파수 대역의 통신 링크)를 설정할 수 있다. 일 구현에서, 단거리 통신 유닛(106)은 대역외 통신 링크로서 근거리 통신(NFC: near field communication) 링크를 설정할 수 있으며, 근거리 통신 인터페이스 및 프로토콜(예를들어, NFCIP)을 활용할 수 있다. 다른 구현들에서, 단거리 통신 유닛(106)은 다른 단거리 통신 기술들/프로토콜들(예를들어, Bluetooth® 등)을 사용하여 통신을 설정할 수 있다.

[0078] 키 반송 디바이스(102)의 키 관리 유닛(104)은 네트워크 디바이스를 보안적으로 구성하기 위하여 네트워크 디바이스(예를들어, 네트워크 디바이스(116, 112 또는 108)와 하나 이상의 메시지들을 교환할 수 있다. 일부 구현들에서, 키 반송 디바이스(102)는 다수의 통신 네트워크 시스템들에서 네트워크 디바이스들을 동시에 구성하는

능력들을 가질 수 있다. 키 관리 유닛(104)은 네트워크 디바이스와 보안 통신 채널을 설정할 수 있다. 예를들어, 보안 통신 채널은 메시지들의 암호화, 메시지들에 대한 무결성 보호를 지원할 수 있으며, 악의적인 키 반송 디바이스들에 의한 리플레이(replay) 공격들으로부터 보호할 수 있다. 일 구현에서, 단거리 통신 유닛(106)이 NFC 링크를 설정할 때, 키 관리 유닛(104)은 (예를들어, ECDH(Elliptic curve Diffie-Hellman) 및 NFC-SEC-01(Advanced Encryption Standard)을 사용하는 NFC-SEC 암호기법 표준을 통해) 보안 통신 채널을 설정하다. 그러나, 다른 구현들에서 다른 보안 채널 기술들(예를들어, Wi-Fi 샘플 구성(WSC)에 특정된 등록 프로토콜)이 활용될 수 있다는 것에 유의해야 한다. 일부 구현들에서, 키 관리 유닛(104)은 보안 채널 키 및 (예를들어, 시퀀스 번호 카운터를 사용하여 생성되는) 시퀀스 번호들을 사용하여 무결성 및 리플레이 보호를 가진 보안 통신 채널을 설정할 수 있다. 시퀀스 번호들은 키 반송 디바이스(102) 및 네트워크 디바이스(예를들어, 네트워크 디바이스(112)가 교환된 메시지들을 추적하여 리플레이 공격들로부터의 보호를 제공하도록 한다. 예를들어, 각각의 교환된 메시지는 시퀀스 번호 카운터에 의해 생성되는 시퀀스 번호를 포함할 수 있으며, 시퀀스 번호는 메시지를 송신/수신할 때 증가될 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 수신된 메시지가 시퀀스 번호 카운터의 현재 값보다 작거나 또는 이 현재 값과 동일한 시퀀스 번호와 연관되는지의 여부를 결정할 수 있다. 만일 수신된 메시지가 시퀀스 번호 카운터의 현재 값보다 작거나 또는 이 현재 값과 동일한 시퀀스 번호와 연관되면, 스테일(stale) 시퀀스 번호는 악의적인 디바이스에 의한 리플레이 공격을 표시할 수 있다. 이후, 키 관리 유닛(104)은 리플레이 공격들을 방지하기 위하여 스테일 시퀀스 번호들을 가진 수신된 메시지들을 무시할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 리플레이 공격들을 검출하기 위하여 시퀀스 번호들을 활용하는 것에 제한되지 않는다. 일부 구현들에서, 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 리플레이 공격들을 검출하기 위하여 시간-스탬프들을 활용할 수 있다.

[0079] 키 반송 디바이스(102)의 키 관리 유닛(104)은 하나 이상의 네트워크 키들을 생성하여 저장하는 능력들을 포함하며, 네트워크 디바이스로 네트워크 키를 송신하고 네트워크 디바이스로부터 네트워크 키를 수신할 수 있다. 예를들어, 네트워크 디바이스가 통신 네트워크(100)로 구성되고 사용자가 네트워크 디바이스를 등록하는 제 1 시간 동안 키 반송 디바이스(102)를 사용할 때, 키 관리 유닛(104)은 네트워크 디바이스로부터 통신 네트워크(100)의 네트워크 키를 수신하고 네트워크 키를 저장할 수 있다. 일 구현에서, 사용자는 통신 네트워크(100)로 구성된 하나 이상의 네트워크 디바이스들을 키 반송 디바이스(102)에 등록할 수 있으며, 키 관리 유닛(104)은 통신 네트워크(100)의 네트워크 키를 네트워크 디바이스에 송신할 수 있다. 다른 구현에서, 사용자는 키 반동 디바이스(102)에 (통신 네트워크(100)로 구성되지 않은) 네트워크 디바이스를 등록할 수 있고, 키 관리 유닛(104)은 통신 네트워크(100)의 네트워크 키를 네트워크 디바이스에 송신할 수 있다. 일부 구현들에서, 통신 네트워크(100)가 없는 경우에, 키 반송 디바이스(102)도 네트워크 디바이스들 중 임의의 디바이스도 네트워크 키를 갖지 않을 수 있으며, 사용자는 키 반송 디바이스(102)에 하나 이상의 네트워크 디바이스들을 등록할 수 있다. 키 관리 유닛(104)은 새로운 랜덤 네트워크 키를 생성할 수 있으며, 키 반송 디바이스(102)에 등록된 네트워크 디바이스들 각각에 네트워크 키를 송신하고 통신 네트워크를 셋업할 수 있다. 일부 구현들에서, 새로운 랜덤 네트워크 키를 생성하는 것 대신에, 키 관리 유닛(104)은 네트워크 관리자로부터 또는 네트워크 디바이스로부터 다른 대역외 통신 링크를 통해 네트워크 키를 수신할 수 있다. 키 관리 유닛(104)은 키 반송 디바이스(102)에 등록된 네트워크 디바이스들에 대한 정보를 저장할 수 있다. 또한, 키 관리 유닛(104)은 키 반송 디바이스(102)에 등록된 네트워크 디바이스들 각각에 대한 보안 통신 채널(예를들어, 보안 채널 키들)에 대한 정보 및 페어링 정보를 저장할 수 있다. 예를들어, 키 관리 유닛(104)은 테이블에서 네트워크 디바이스의 디바이스 식별자에 대응하는 보안 채널 키들을 키 반송 디바이스(102)의 메모리에 저장할 수 있다. 일부 구현들에서, 키 반송 디바이스(102)는 네트워크에서 제 2 키 반송 디바이스 또는 서버에 대해 키 반송 디바이스(102)의 정보 및 세팅들을 익스포트하고 임포트하며 백업하는 기능들을 지원할 수 있다. 이후, 제 2 키 반송 디바이스는 하나 이상의 네트워크 디바이스들을 구성하기 위하여 사용될 수 있다. 다양한 네트워크 구성 기술들에 대한 키 반송 디바이스(102)의 추가 특징들 및 동작들은 도 2-23을 참조로 하여 이하에서 추가로 설명될 것이다.

[0080] 네트워크 디바이스들(108, 112 및 116)은 통신 네트워크(100)의 다양한 타입들의 네트워크 디바이스들, 예를들어 랩탑 컴퓨터, 텔레비전, 카메라, 게임 콘솔, 디지털 서모스탯, 전자 도어 록 등일 수 있다. 일부 구현들에서, 네트워크 디바이스들(108, 112 및 116)은 멀티-홈 디바이스(multi-homed device)들일 수 있으며, 다수의 통신 네트워크 시스템들로 동시에 구성될 수 있다. 일례에서, 네트워크 디바이스들(108, 112 및 116)은 IEEE P1905.1 통신 네트워크의 디바이스들일 수 있다. 일부 구현들에서, 네트워크 디바이스들(116, 112 및 108)의 단거리 통신 유닛들(118, 114 및 110)은 각각 키 반송 디바이스(102)의 단거리 통신 유닛(106)과 단거리 통신 링크(예를들어, NFC 링크)를 설정할 수 있다. 이하에서 추가로 설명되는 바와같이, 네트워크 디바이스들(108, 112 및 116)은 키 관리 유닛(104)으로부터 네트워크 키를 수신하고 키 반송 디바이스(102)에 등록하는 능력들을

포함한다. 예를들어, 네트워크 디바이스들(116, 112 및 108)의 등록 관리 유닛들(117, 113 및 109)은 각각 키 반송 디바이스(102)에 등록하고, 키 반송 디바이스(102)로부터 네트워크 키를 수신할 수 있다. 일부 구현들에서, 키 반송 디바이스(102)의 키 관리 유닛(104)은 네트워크 디바이스들(116, 112 및 108)로부터 네트워크 키를 요청할 수 있다. 키 반송 디바이스가 네트워크 키를 요청할 때, 개별 네트워크 디바이스들(116, 112 및 108)의 등록 관리 유닛들(117, 113 및 109)은 키 관리 유닛(104)에 네트워크 키를 송신할 수 있다. 네트워크 디바이스들(108, 112 및 116)은 키 반송 디바이스(102)에 대응하는 페어링 데이터를 삭제하여 키 반송 디바이스(102)로부터 등록해제함으로써 리셋될 수 있다. 예를들어, 네트워크 디바이스들(108, 112 및 116)은 하드웨어(예를들어, 리셋 버튼 등)를 통해 또는 소프트웨어(예를들어, 프로그램 명령들 등)를 통해 리셋될 수 있다. 일부 구현들에서, 네트워크 디바이스들(108, 112 및 116)은 상이한 색들(예를들어, 등록해제 상태를 위한 적색, 등록 상태를 위한 녹색 및 등록 프로세스가 진행중일때의 황색)을 통해 자신들의 상태를 디스플레이하기 위하여 발광 다이오드(LED)들을 포함할 수 있다. 다양한 네트워크 구성 기술들에 대한 네트워크 디바이스들(108, 112 및 116)의 추가 특징들 및 동작들은 도 2-23을 참조로 하여 이하에서 추가로 설명될 것이다.

[0081] 도 2는 네트워크 디바이스를 구성하기 위한 예시적인 동작들의 흐름도를 예시한다. 예를들어, 도 2는 일단 단거리 통신 링크가 네트워크 디바이스(112)에 설정되면 (도 1을 참조로 하여 앞서 설명되는 바와같이) 키 반송 디바이스(102)에서 수행되는 동작들을 예시한다. 간략화를 위하여, 도 2는 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에 보안 통신 채널을 설정하기 위한 절차들을 예시하지 않고 도 3-23을 참조로 하여 이하에서 더 상세히 설명되는 다양한 구성 기술들의 다른 세부사항들을 예시하지 않는다.

[0082] 블록(202)에서는 네트워크 디바이스를 등록해야 하는지 또는 등록 해제를 해야 하는지가 결정된다. 예를들어, 키 반송 디바이스(102)의 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해야 하는지 또는 등록 해제해야 하는지를 결정한다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록하거나 또는 등록 해제하기 위한, 사용자로부터의 입력을 수신할 수 있다. 다른 구현들에서, 사용자는 단거리 통신 링크(예를들어, NFC)를 통해 (등록해제 상태에 있는) 네트워크 디바이스(112)의 등록을 자동적으로 트리거하기 위하여 네트워크 디바이스(112)의 미리 결정된 근접한 위치에 키 반송 디바이스(102)를 배치시킬 수 있다. 유사하게, 키 관리 유닛(104)은 키 반송 디바이스(102)가 네트워크 디바이스(112)의 미리 결정된 근접 위치내에 배치될 때 (등록 상태에 있는) 네트워크 디바이스(112)를 자동적으로 등록해제할 수 있다. 만일 네트워크(112)를 등록하는 것이 결정되면, 제어는 블록(214)으로 진행한다. 만일 네트워크 디바이스(112)를 등록해제하는 것이 결정되면, 제어는 블록(204)으로 진행한다.

[0083] 블록(204)에서, 네트워크 디바이스를 등록해제하는 것을 결정하는 것에 응답하여, 키 반송 디바이스(102)는 네트워크 디바이스(112)가 등록 상태에 있는지의 여부를 결정한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록 상태에 있는지의 여부를 결정하기 위하여 네트워크 디바이스(112)와 하나 이상의 메시지들을 교환할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록 상태에 있는지의 여부를 결정하기 위하여 메시지들의 교환동안 네트워크 디바이스(112)로부터 수신되는 정보를 프로세싱할 수 있다. 다른 구현들에서, 키 관리 유닛(104)은 메시지들의 교환 동안 네트워크 디바이스(112)의 상태에 대한 정보를 수신할 수 있다. 예를들어, 네트워크 디바이스(112)의 상태는 네트워크 디바이스(112)가 등록 상태에 있는지 아닌지의 여부를 표시할 수 있다. 만일 네트워크 디바이스(112)가 등록 상태에 있으면, 제어는 블록(208)으로 진행한다. 만일 네트워크 디바이스(112)가 등록 상태에 있지 않으면, 제어는 블록(206)으로 진행한다.

[0084] 블록(206)에서, 네트워크 디바이스의 등록해제 상태가 디스플레이된다. 일 구현에서, 키 반송 디바이스(102)의 디스플레이 유닛은 네트워크 디바이스(112)가 등록해제됨을 디스플레이할 수 있다. 예를들어, 블록(204)에서 네트워크 디바이스(112)가 등록상태에 있지 않다고 결정할 때, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록해제됨을 디스플레이할 것을 키 반송 디바이스(102)의 디스플레이 유닛에 명령할 수 있다. 일부 구현들에서, 네트워크 디바이스(112)는 또한 디스플레이 능력들을 가지고 자신이 등록해제됨을 디스플레이할 수 있다.

[0085] 블록(208)에서, 네트워크 디바이스가 키 반송 디바이스에 등록되어 있는지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정한다. 예를들어, 키 관리 유닛(104)은 초기 메시지 교환 동안 네트워크 디바이스(112)로부터 수신되는 정보를 프로세싱함으로써 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 네트워크 디바이스(112)의 상태와 관련하여 수신되는 정보에 기초하여 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있으면, 제어는 블록(210)으로 진행하다. 만일 네트워크

디바이스가 키 반송 디바이스에 등록되지 않으면, 제어는 블록(212)으로 진행한다.

[0086] 블록(210)에서, 네트워크 디바이스를 등록해제하기 위한 명령들이 송신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제할 명령들을 송신한다. 예를들어, 키 관리 유닛(104)은 (키 반송 디바이스(102)에 대응하는) 네트워크 키 및 페어링 데이터를 삭제할 명령들을 네트워크 디바이스(112)에 송신할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 또한 키 반송 디바이스(102)에 저장되는, 네트워크 디바이스(112)와 페어링하기 위한 임의의 페어링 데이터를 삭제할 수 있다. 일부 구현들에서, 네트워크 디바이스(112)의 등록해제는 키 반송 디바이스(102)가 네트워크 디바이스(112)에 그 자체를 보안적으로 인증할 수 있는 경우에에만 유효할 수 있다. 예를들어, 키 반송 디바이스(102)는 자신이 악의적인 디바이스가 아님을 증명하기 위하여 네트워크 디바이스(112)와 하나 이상의 메시지들을 교환할 수 있으며, 등록해제 절차는 인증 이후에 계속될 수 있다.

[0087] 블록(212)에서, 네트워크 디바이스가 키 반송 디바이스에 등록되지 않음을 표시하는 상태가 디스플레이된다. 일 구현에서, 키 반송 디바이스(102)의 디스플레이 유닛은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않음을 디스플레이한다. 예를들어, 키 관리 유닛(104)은 (블록(208)에서 수행된 결정에 따라) 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않는다는 메시지를 디스플레이할 것을 디스플레이 유닛에 명령할 수 있다. 일부 구현들에서, 네트워크 디바이스(112)는 또한 디스플레이 능력들을 가질 수 있고, 등록해제가 허용되지 않음을 표시하기 위하여 자신이 키 반송 디바이스(102)에 등록되지 않음을 디스플레이할 수 있다.

[0088] 블록(214)에서, 네트워크 디바이스를 등록한다는 결정에 응답하여, 키 반송 디바이스(102)는 네트워크 디바이스(112)가 이미 등록 상태에 있는지의 여부를 결정한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록 상태에 있는지의 여부를 결정하기 위하여 네트워크 디바이스(112)와 하나 이상의 메시지들을 교환할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록 상태에 있는지의 여부를 결정하기 위하여 메시지들의 교환 동안 네트워크 디바이스(112)로부터 수신되는 정보를 프로세싱할 수 있다. 다른 구현들에서, 키 관리 유닛(104)은 메시지들의 교환 동안 네트워크 디바이스(112)의 상태에 대한 정보를 수신할 수 있다. 예를들어, 네트워크 디바이스(112)의 상태는 네트워크 디바이스(112)가 등록 상태에 있는지 아닌지의 여부를 표시할 수 있다. 만일 네트워크 디바이스(112)가 등록 상태에 있으면, 제어는 블록(216)으로 진행한다. 만일 네트워크 디바이스(112)가 등록 상태에 있지 않으면, 제어는 블록(218)으로 진행한다.

[0089] 블록(216)에서, 네트워크 디바이스의 등록 상태는 디스플레이된다. 일 구현에서, 키 반송 디바이스(102)의 디스플레이 유닛은 네트워크 디바이스(112)가 등록되어 있다고 디스플레이한다. 예를들어, 키 관리 유닛(104)은 (블록(214)에서 수행된 결정에 기초하여) 네트워크 디바이스(112)가 등록되어 있다고 디스플레이할 것을 디스플레이 유닛에 명령할 수 있다. 일부 구현들에서, 네트워크 디바이스(112)는 또한 디스플레이 능력들을 가지고 등록 상태를 디스플레이할 수 있다.

[0090] 블록(218)에서, 네트워크 디바이스가 네트워크 키를 포함하는지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 네트워크 키를 포함하는지의 여부를 결정한다. 예를들어, 네트워크 디바이스(112)는 네트워크 디바이스(112)와의 메시지들의 교환 동안 수신되는 정보에 기초하여 네트워크 디바이스(112)가 네트워크 키를 포함하는지의 여부를 결정한다. 만일 네트워크 디바이스(112)가 네트워크 키를 포함하면, 제어는 블록(220)으로 진행한다. 만일 네트워크 디바이스가 네트워크 키를 포함하지 않으면, 제어는 블록(222)으로 진행한다.

[0091] 블록(220)에서, 만일 네트워크 디바이스가 네트워크 키를 포함하면, 네트워크 디바이스를 등록하기 위한 명령들이 송신되며, 네트워크 키는 네트워크 디바이스로부터 수신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록할 명령들을 송신하며, 네트워크 디바이스(112)로부터 네트워크 키를 수신한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)에 저장되는 페어링 데이터를 업데이트할 명령들을 송신한다. 키 관리 유닛(104)은 네트워크 디바이스(112)와 보안 통신 채널을 설정할 수 있고, 보안 통신 채널을 통해 네트워크 디바이스(112)에서 페어링 데이터를 업데이트할 명령들을 송신할 수 있다. 키 관리 유닛(104)은 또한 네트워크 디바이스(112)로부터 보안 통신 채널을 통해 통신 네트워크(100)의 네트워크 키를 요청할 수 있다. 예를들어, 네트워크 디바이스(112)는 통신 네트워크(100)로 사전에 구성될 수 있으며, 통신 네트워크(100)의 네트워크 키는 네트워크 디바이스(112)에 저장될 수 있다. 키 관리 유닛(104)은 네트워크 디바이스(112)로부터 보안 통신 채널을 통해 통신 네트워크(100)의 네트워크 키를 수신할 수 있으며, 키 반송 디바이스(102)에 네트워크 키를 저장할 수 있다.

[0092] 블록(222)에서, 만일 네트워크 디바이스가 네트워크 키를 포함하면, 네트워크 디바이스를 등록하기 위한 명령들이 송신되며, 네트워크 키는 네트워크 디바이스에 송신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록할 명령들을 송신하며, 통신 네트워크(100)의 네트워크 키를 네트워크 디바이스(112)에 송신한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)에서 페어링 데이터를 업데이트할 명령들을 송신한다. 키 관리 유닛(104)은 네트워크 디바이스(112)와 보안 통신 채널을 설정할 수 있으며, 보안 통신 채널을 통해 네트워크 디바이스(112)에서 페어링 데이터를 업데이트할 명령들을 송신한다. 키 관리 유닛은 또한 통신 네트워크(100)의 네트워크 키를 보안 통신 채널을 통해 네트워크 디바이스(112)에 송신할 수 있다. 예를들어, 키 반송 디바이스(102)는 통신 네트워크(100)로 구성될 수 있으며, 통신 네트워크(100)의 네트워크 키는 키 반송 디바이스(102)에 저장될 수 있다. 키 반송 디바이스(102)는 통신 네트워크(100)의 네트워크 키를 네트워크 디바이스(112)에 송신할 수 있다. 일부 구현들에서, 키 반송 디바이스(102)는 통신 네트워크(100)로 구성되지 않을 수 있으며, 통신 네트워크(100)의 네트워크 키는 키 반송 디바이스(102)에 저장되지 않을 수 있다. 키 반송 디바이스(102)는 새로운 랜덤 네트워크 키를 생성하여 네트워크 키를 네트워크 디바이스(112)에 송신할 수 있다.

[0093] 도 2의 흐름도에 설명된 절차들이 원래 예시적이며 간략화를 위하여 도 2의 흐름도에서 모든 절차들이 설명되지 않는다는 것에 유의해야 한다. 하나 이상의 절차들이 상이한 순서로 수행될 수 있다는 것에 추가로 유의해야 한다. 예를들어, (블록(220 및 222)에서) 네트워크 디바이스(122)를 등록하기 위한 명령들은 네트워크 디바이스(112)가 네트워크 키를 포함하는지의 여부를 결정하기 전에 송신될 수 있다.

[0094] 도 3은 제 1 및 제 2 구성 기술들을 사용하여 네트워크 디바이스를 구성하기 위한 예시적인 동작들의 흐름도를 예시한다. 도 3은 통신 디바이스를 사용하여 네트워크 디바이스를 구성하기 위하여 (도 5-6에서 이하에서 설명되는) 제 1 구성 기술 및 (도 7-8에서 이하에서 설명되는) 제 2 구성 기술 둘다에 공통적인 예시적인 동작들을 설명한다. 일례에서, 통신 디바이스는 여기에서 설명되는 통신 네트워크의 키 반송 디바이스로서 지칭될 수 있다(예를들어, 통신 네트워크(100)의 키 반송 디바이스(102)가 도 1에 도시된다). 통신 디바이스(또는 키 반송 디바이스)는 또한 통신 네트워크(예를들어, 통신 네트워크(100))의 구성 디바이스로서 지칭될 수 있다.

[0095] 블록(302)에서, 네트워크 디바이스와의 페어링 동작들은 단거리 통신 연결을 통해 통신 디바이스에서 개시된다. 일 구현에서, 키 반송 디바이스(102)는 NFC를 통해 네트워크 디바이스(112)와의 페어링 동작들을 개시한다. 예를들어, 키 반송 디바이스(102)의 키 관리 유닛(104)은 네트워크 디바이스를 등록하거나 또는 등록해제하기 위하여 네트워크 디바이스(112)의 등록 관리 유닛(113)과의 페어링 동작들을 개시할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 사용자 입력에 기초하여 등록 관리 유닛(113)과의 페어링 동작들을 개시할 수 있다. 다른 구현들에서, 키 관리 유닛(104)은 키 반송 디바이스(102)가 네트워크 디바이스(112)의 부근에 있을 때 그리고 단거리 통신 링크가 설정되자 마자 등록 관리 유닛(113)과의 페어링 동작들을 개시할 수 있다. 흐름은 블록(304)으로 진행한다.

[0096] 블록(304)에서, 네트워크 디바이스가 등록상태에 있는지 또는 등록해제 상태에 있는지가 결정된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)가 등록 또는 등록해제 요청을 네트워크 디바이스(112)에 전송한 이후에 네트워크 디바이스(112)로부터 수신되는 하나 이상의 응답 메시지들에 기초하여 네트워크 디바이스(112)가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하기 위하여 네트워크 디바이스(112)의 등록 관리 유닛(113)과 하나 이상의 등록 또는 등록해제 요청 및 응답 메시지들을 교환할 수 있다. 도 5, 도 6, 도 7 및 도 8은 스테이지들 A-D2에서 이러한 메시지 교환들을 예시하며, 이는 이하에서 더 상세히 설명될 것이다. 만일 네트워크 디바이스(112)가 등록해제 상태에 있으면, 제어는 블록(306)으로 진행하며, 키 관리 유닛(104)은 동작 절차들을 수행할 수 있다. 만일 네트워크 디바이스(112)가 등록 상태에 있으면, 제어는 블록(312)으로 진행하며, 키 관리 유닛(104)은 등록해제 절차들을 수행할 수 있다.

[0097] 블록(306)에서, 보안 통신 채널이 네트워크 디바이스(112)에 설정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)의 등록 관리 유닛(113)과 보안 통신 채널을 설정한다. 예를들어, 키 관리 유닛(104)은 키 합의, 키 유도 및 키 확인 절차들을 수행함으로써 보안 통신 채널을 설정할 수 있다. 키 관리 유닛(104) 및 네트워크 디바이스(112)는 보안 통신 채널에 대한 하나 이상의 보안 채널 키들(예를들어, 무결성 키, 암호화 키 및 시퀀스 번호 카운터)을 결정하여 보안 채널 키들을 세이브할 수 있다. 예를들어, 키 관리 유닛(104) 및 네트워크 디바이스(112)는 도 5 및 도 7의 스테이지 E에서 키 합의, 키 유도 및 키 확인 절차들을 수행한다. 흐름은 블록(308)으로 계속된다.

[0098] 블록(308)에서, 보안 통신 채널은 네트워크 디바이스(112)에 설정된다. 일 구현에서, 키 관리 유닛(104)은 블록(306)에서 설정되는 보안 통신 채널을 통해 네트워크 디바이스(112)의 등록 관리 유닛(113)에 통신 네트워크의 네트워크 키를 전송한다. 예를들어, 도 5 및 도 7에서, 키 관리 유닛(104)은 스테이지 F에서 등록 관리 유닛(113)에 네트워크 키를 전송한다. 네트워크 키를 수신할 때, 등록 관리 유닛(113)은 네트워크 키를 세이브할 수 있으며, 통신 네트워크(100)로 네트워크 디바이스(112)를 구성할 수 있다(예를들어, 통신 네트워크(100)를 연결될 수 있다). 또한, 등록 절차들의 완료시에, 키 관리 유닛(104) 및 등록 관리 유닛(113)은 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 각각 저장되는 페어링 데이터(예를들어, 도 5에서 디바이스 식별자 및 보안 채널 키들과 도 7에서 공개 키)를 업데이트할 수 있다.

[0099] 블록(312)에서, 네트워크 디바이스가 통신 디바이스로 등록되어 있는지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정한다. 예를들어, 키 관리 유닛(104)은 도 6 및 도 8의 스테이지들 D1 및 D2에서의 메시지 교환들에 기초하여 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 키 관리 유닛 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 단지 등록해제 절차들로 진행할 수 있다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있으면, 제어는 블록(314)으로 진행한다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않으면, 키 관리 유닛(104)은 등록해제 절차들을 중지할 수 있다.

[0100] 블록(314)에서, 적어도 하나의 메시지는 네트워크 디바이스를 등록해제하기 위하여 네트워크 디바이스에 송신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위하여 네트워크 디바이스(112)의 등록 관리 유닛(113)에 적어도 하나의 메시지를 송신한다. 일 구현에서, 키 관리 유닛(104)은 보안 통신 채널을 통해 네트워크 디바이스(112)를 등록해제할 명령들을 송신할 수 있다. 예를들어, 도 6에서, 네트워크 디바이스(112) 및 키 반송 디바이스(102)는 페어링 데이터의 부분으로서 보안 채널 키들을 저장한다. 도 6의 스테이지들 E1-F에 예시된 바와같이, 키 관리 유닛(104)은 보안 채널 키들을 활용하여 보안 통신 채널을 설정하고 보안 통신 채널을 통해 네트워크 디바이스(112)를 등록해제할 명령들을 송신할 수 있다. 등록해제할 명령들을 수신할 때, 네트워크 디바이스(112)의 등록 관리 유닛(113)은 키 반송 디바이스(102)로부터 등록해제 명령들이 수신되는지의 여부를 결정할 수 있다. 등록 관리 유닛(113)은 등록해제 명령들이 키 반송 디바이스(102)로부터 수신되지 않은 경우에 에러를 플래그할 수 있다. 또 다른 구현에서, 도 8의 스테이지 E에 예시된 바와같이, 키 관리 유닛(104)은 네트워크 디바이스(112)에 자신의 아이덴티티를 증명하기 위하여 키 합의, 키 유도 및 키 확인 절차들을 수행할 수 있다. 등록 관리 유닛(113)은 키 합의, 키 유도 및 키 확인 절차들이 성공적이지 않은 경우에 등록해제 절차들을 중단할 수 있다.

[0101] 도 3의 흐름도에서 설명되는 절차들이 본래 예시적이며 간략화를 위하여 도 3이 제 1 및 제 2 구성 기술들을 구현할 때 수행되는 모든 동작들의 세부사항들 모두를 예시하지 않는다는 것에 유의해야 한다. 제 1 및 제 2 구성 기술들에 대하여 키 반송 디바이스(102) 및 네트워크 디바이스(112)에서 수행되는 예시적인 동작들의 추가 세부사항들은 도 5-8를 참조로 하여 이하에서 추가로 설명될 것이다.

[0102] 도 4는 제 3, 제 4 및 제 5 구성 기술들을 사용하여 네트워크 디바이스를 구형하기 위한 예시적인 동작들의 흐름도를 예시한다. 도 4는 통신 디바이스를 사용하여 네트워크 디바이스를 구성하기 위하여 (도 9-14에서 이하에서 설명되는) 제 3 구성 기술, (도 15-20에서 이하에서 설명되는) 제 4 구성 기술 및 (도 21-23에서 이하에서 설명되는) 제 5 구성 기술들에 공통적인 예시적인 동작들을 설명한다. 일례에서, 통신 디바이스는 여기에서 설명되는 통신 네트워크의 키 반송 디바이스(예를들어, 도 1에 도시된 통신 네트워크(100)의 키 반송 디바이스(102))로 지칭될 수 있다. 통신 디바이스(또는 키 반송 디바이스)는 또한 통신 네트워크(예를들어, 통신 네트워크(100))의 구성 디바이스로 지칭될 수 있다.

[0103] 블록(402)에서, 제 1 메시지 교환은 통신 디바이스의 네트워크 디바이스로 개시된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)와 제 1 메시지 교환을 개시한다. 예를들어, 제 1 메시지 교환은 난수 및 (난수를 사용하여 암호화되는) 암호화된 데이터를 포함할 수 있다. 제 3, 제 4 및 제 5 구성 기술들에서, 페어링 데이터는 키 반송 디바이스(102)(RKk)에 저장되는 등록 키 및 네트워크 디바이스(112)(RKn)에 저장되는 등록 키를 포함한다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 또한 각각 NK 및 NK'로서 네트워크 키를 저장할 수 있다. 제 1 메시지 교환 동안, 제 1 반송 디바이스(102)는 난수 N1를 가진 "헬로" 요청(또한 등록 또는 등록해제 요청으로서 지칭될 수 있음)을 송신할 수 있으며, 네트워크 디바이스(112)는 (예를들어, 도 9 및 도 13의 스테이지들 A-C에서 예시된 바와같이) 암호화된 RKn, 암호화된 NK' 및 다른 난수 N2에 응답할 수 있다. 네트워크 디바이스(112)는 키 반송 디바이스(102) 및 난수 N1에게 알려진 해싱 알고리즘을 사용하여 RKn을 암호

화할 수 있다. 네트워크 디바이스(112)는 또한 키 반송 디바이스(102)에게 알려진 해싱 알고리즘을 사용하여 NK'를 암호화할 수 있다. 난수 N2는 하나 이상의 메시지 교환들에서 암호화된 데이터를 네트워크 디바이스(112)에 송신하기 위하여 키 반송 디바이스(102)에 의해 활용될 수 있다. 일부 구현들에서, (도 14 및 도 20의 스테이지들 A-C에서 그리고 도 15 및 도 18의 스테이지들 A1-A2에서 예시된 바와같이) 제 1 메시지 교환은 키 반송 디바이스(102)로부터의 난수에 대한 요청 및 네트워크 디바이스(112)로부터의 난소를 가진 응답일 수 있다. 일부 구현들에서, (예를들어, 도 21 및 도 23의 스테이지 A에서 예시된 바와같이) 제 1 메시지 교환은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이의 보안 통신 채널의 설정일 수 있다. 흐름은 블록(404)으로 계속된다.

[0104] 스테이지(404)에서, 네트워크 디바이스가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부가 결정된다. 일 구현에서, 키 관리 디바이스(104)는 제 1 메시지 교환에서 네트워크 디바이스(112)로부터 수신되는 데이터를 프로세싱함으로써 네트워크 디바이스(112)가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정한다. 예를들어, 도 9 및 도 10은 스테이지들 D 및 K에서 네트워크 디바이스(112)가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하기 위한 동작들을 예시한다. 도 13은 스테이지들 D 및 E에서 네트워크 디바이스(112)가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하기 위한 동작들을 예시한다. 일부 구현들에서, 키 관리 유닛(104)은 제 1 메시지 교환 이후에 후속 메시지 교환에 기초하여 네트워크 디바이스(112)가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정할 수 있다. 예를들어, (도 15, 도 18 및 도 23의 스테이지 H에 그리고 도 21의 스테이지 I에 예시된 바와같이) 키 관리 유닛(104)은 네트워크 디바이스(112)로부터 네트워크 디바이스(112)의 상태를 수신할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 등록 상태에 있는지 또는 등록해제 상태에 있는지의 여부를 결정하지 못할 수 있고, 대신에 키 관리 유닛(104)은 사용자로부터의 입력에 기초하여 네트워크 디바이스(112)를 등록하거나 또는 등록해제하는 것을 계속할 수 있다. 예를들어, 도 14 및 도 20에서, 네트워크 디바이스(112)가 등록상태에 있는지 또는 등록해제 상태에 있는지의 여부가 결정되지 않으며, 대신에 스테이지 E에서 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 네트워크 디바이스(112)가 등록상태에 있음이 결정되면, 제어는 블록(414)으로 진행하며, 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 절차들이 수행될 수 있다. 네트워크 디바이스(112)가 등록해제 상태에 있음이 결정되면, 제어는 블록(406)으로 진행하며, 네트워크 디바이스(112)를 등록하기 위한 등록 절차들이 수행될 수 있다.

[0105] 블록(406)에서, 적어도 하나의 등록 키는 네트워크 디바이스를 등록하기 위하여 네트워크 디바이스에 송신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록하기 위하여 적어도 하나의 등록 키를 네트워크 디바이스(112)에 송신한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)에 RKk를 송신할 수 있다. 키 관리 유닛(104)은 (예를들어, 키 합의, 키 유도 및 키 확인 절차들을 사용하여) 보안 통신 채널을 설정하고 (예를들어, 도 9의 스테이지 H, 도 16의 스테이지 N2 및 도 21의 스테이지 B에서 예시된 바와같이) 보안 통신 채널을 통해 RKk를 송신할 수 있다. 일부 구현들에서, 키 반송 디바이스(102)에 저장된 RKk가 널(null)일 때, 키 관리 유닛(104)은 새로운 랜덤 RKk를 생성하여 네트워크 디바이스(112)에 RKk를 송신할 수 있다. 흐름은 블록(408)으로 계속된다.

[0106] 블록(408)에서는 네트워크 키가 네트워크 디바이스에 저장됨이 결정된다. 일 구현에서, 키 관리 유닛(104)은 제 1 메시지 교환에서 네트워크 디바이스(112)로부터 수신되는 데이터를 프로세싱함으로써 네트워크 키가 네트워크 디바이스(112)에 저장되는지의 여부를 결정한다. 예를들어, (예를들어, 도 10의 스테이지 M, 도 16의 스테이지 Q에 예시된 바와같이) 키 관리 유닛(104)은 네트워크 디바이스(112)로부터 수신되는 암호화된 NK'가 널인지의 여부를 결정한다. 일부 구현들에서, (예를들어, 도 10의 스테이지 M, 도 16의 스테이지 Q에 예시된 바와같이) 제 1 메시지 교환 이후에 후속 메시지 교환에서 네트워크 디바이스(112)에 의해 송신되는 상태는 네트워크 키가 네트워크 디바이스(112)에 저장되는지의 여부를 표시할 수 있다. 네트워크 키가 네트워크 디바이스(112)에 저장됨을 결정할 때, 키 관리 유닛(104)은 네트워크 디바이스(112)에 저장되는 네트워크 키를 활용할 것을 결정할 수 있으며, 제어는 블록(410)으로 진행한다. 만일 네트워크 키가 네트워크 디바이스(112)에 저장되지 않으면, 제어는 블록(412)으로 진행한다.

[0107] 블록(410)에서, 네트워크 키는 네트워크 디바이스(112)로부터 수신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)의 등록 관리 유닛(113)으로부터 네트워크 키를 수신한다. 예를들어, 키 관리 유닛(104)은 네트워크 키를 수신하기 위하여 등록 관리 유닛(113)에 "겟(get)" 네트워크 키 요청을 송신할 수 있다. 일부 구현들에서, (도 11의 스테이지 O2 및 도 16의 스테이지 T에 예시된 바와같이) 겟 네트워크 키 요청은 암호화된 RKk를 포함할 수 있다. RKk는 네트워크 디바이스(112)에게 알려진 해싱 알고리즘을 사용하여 그리고 네트

워크 디바이스(112)로부터 수신되는 N2를 사용하여 암호화될 수 있다. 일부 구현들에서, (도 22의 스테이지 N에 예시된 바와같이) 겟 네트워크 키 요청은 보안 통신 채널을 통해 송신될 수 있고 암호화된 RKk를 포함하지 않을 수 있다. 겟 네트워크 키 요청에 응답하여, 키 관리 유닛(104)은 네트워크 디바이스(112)에 저장된 네트워크 키를 수신하고 네트워크 키를 세이브할 수 있다.

[0108] 블록(412)에서, 네트워크 키는 네트워크 디바이스에 송신된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장된 네트워크 키를 네트워크 디바이스(112)의 등록 관리 유닛(113)에 송신한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)에 "세트(set)" 네트워크 키 요청을 송신할 수 있다. (예를들어 도 12의 스테이지 Y 및 도 17의 스테이지 AD에 예시된 바와같이) 세트 네트워크 키 요청은 네트워크 키 및 암호화된 RKk를 포함할 수 있다. RKk는 네트워크 디바이스(112)에게 알려진 해싱 알고리즘을 사용하여 그리고 네트워크 디바이스(112)로부터 수신되는 N2를 사용하여 암호화될 수 있다. 일부 구현들에서, (예를들어, 도 22의 스테이지 U에 예시된 바와같이) 세트 네트워크 키 요청은 보안 통신 채널을 통해 송신될 수 있고 암호화된 RKk를 포함하지 않을 수 있다. 세트 네트워크 키 요청에 응답하여, 키 관리 유닛(104)은 네트워크 키가 네트워크 디바이스(112)에 세이브된다는 확인응답을 포함할 수 있는, 네트워크 디바이스(112)로부터의 세트 네트워크 키 응답을 수신할 수 있다.

[0109] 블록(414)에서는 네트워크 디바이스가 통신 디바이스에 등록됨이 결정된다. 일 구현에서, 키 관리 유닛(104)은 제 1 메시지 교환 동안 수신되는 데이터를 프로세싱함으로써 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정한다. 다른 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정하지 못할 수 있고, 대신에 키 관리 유닛(104)은 네트워크 디바이스(112)에 등록해제 요청을 송신할 수 있다. 네트워크 디바이스(112)는 (블록(416)에서 설명되는 바와같은) 등록해제 요청에 기초하여 키 반송 디바이스(102)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 (예를들어, 도 13의 스테이지 E에 예시된 바와같이) 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정하기 위하여 네트워크 디바이스(112)로부터 수신되는 (제 1 메시지 교환 동안 수신되는) 암호화된 RKn이 (RKn을 암호화하기 위하여 네트워크 디바이스(112)에 의해 활용되는 동일한 난수 및 해싱 알고리즘을 사용하여 암호화되는) 암호화된 RKk와 매칭되는지의 여부를 검증할 수 있다. 다른 구현들에서, 키 관리 유닛(104)은 (예를들어, 도 18의 스테이지 I에서) 네트워크 디바이스(112)로부터 수신되는 네트워크 디바이스(112)의 상태에 기초하여 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있으면, 제어는 블록(416)으로 진행한다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않으면, 키 반송 디바이스(102)는 네트워크 디바이스(112)를 등록해제할 수 없을 수 있다.

[0110] 블록(416)에서, 네트워크 디바이스를 등록해제할 적어도 하나의 명령이 송신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)의 등록 관리 유닛(113)에 등록해제 요청을 송신할 수 있다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)의 등록 관리 유닛(112)에 등록해제 요청을 송신할 수 있다. (도 13의 스테이지 G, 도 14의 스테이지 E, 도 19의 스테이지 L 및 도 20의 스테이지 E에 예시된 바와같이) 등록해제 요청은 암호화된 RKk를 포함할 수 있다. RKk는 네트워크 디바이스(112)에게 알려진 해싱 알고리즘을 사용하여 그리고 네트워크 디바이스(112)로부터 수신되는 난수를 사용하여 암호화될 수 있다. 일부 구현들에서, (예를들어, 도 23의 스테이지 B에 예시된 바와같이) 키 관리 유닛(104)은 반드시 암호화된 RKk를 가진 등록해제 요청을 송신하지 않을 수 있으나, 등록해제 요청은 암호화된 RKk 대신에 RKk를 포함할 수 있다. 일부 구현들에서, (예를들어, 도 14의 스테이지 F, 도 19의 스테이지 M, 도 20의 스테이지 F 및 도 23의 스테이지 E에 예시된 바와같이) 등록해제 요청을 수신할 때, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)를 등록해제하기 위한 하나 이상의 동작들을 수행하고 키 관리 유닛(104)에 등록해제 응답을 송신할 수 있다. 만일 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않음을 키 관리 유닛(104)에 표시할 수 있다.

[0111] 도 4의 흐름도에서 설명되는 절차들이 본래 예시적이며 간략화를 위하여 도 4가 제 3, 제 4 및 제 5 구성 기술들을 구현할 때 수행되는 모든 동작들의 세부사항들 모두를 예시하지 않는다는 것에 유의해야 한다. 제 3, 제 4 및 제 5 구성 기술들에 대하여 키 반송 디바이스(102) 및 네트워크 디바이스(112)에서 수행되는 예시적인 동작들의 추가 세부사항들은 도 9-23를 참조로 하여 이하에서 추가로 설명될 것이다.

[0112] 도 5는 제 1 구성 기술을 네트워크 디바이스를 등록하기 위한 예시적인 동작들의 시퀀스 다이어그램을

예시한다. 도 5는 (도 1를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 네트워크 디바이스의 디바이스 식별자(IDY), 무결성 키(KI), 암호화 키(KE) 및 시퀀스 번호 카운터(SN)를 포함한다. 네트워크 디바이스(112)상에 저장되는 페어링 데이터는 키 반송 디바이스의 디바이스 식별자(IDB), 무결성 키(KI'), 암호화 키(KE'), 및 시퀀스 번호 카운터(SN')를 포함할 수 있다. IDY, KI, KE, SN, IDB, KI', KE' 및 SN'이 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 페어링 데이터를 저장하기 위한 예시적인 변수들을 나타낼 수 있다는 것에 유의해야 한다. 키 반송 디바이스(102)의 디바이스 식별자가 IDA이고 네트워크 디바이스(112)의 디바이스 식별자가 IDX이라는 것에 또한 유의해야 한다. 키 반송 디바이스(102)가 키 반송 디바이스(102)에 등록되는 다수의 네트워크 디바이스들에 대응하는 페어링 데이터(즉, IDY, KI, KE 및 SN)의 다수의 세트들을 저장할 수 있다는 것에 추가로 유의해야 한다. 도 5는 스테이지들 A-I2의 시퀀스에서 네트워크 디바이스(112)를 등록하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 5가 키 관리 유닛(104) 및 등록 관리 유닛(1133)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0113] 스테이지 A에서, 등록 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 반송 디바이스(102)의 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록 요청을 송신한다. 예를들어, 등록 요청은 네트워크 디바이스(112)에서 페어링 데이터를 업데이트하기 위한 명령 및 IDA를 포함할 수 있다.

[0114] 스테이지 B에서는 IDB가 널임이 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 IDB의 값이 널인지의 여부를 결정한다. 만일 IDB가 널이면, 등록 관리 유닛(113)은 스테이지 C2에서의 응답을 키 관리 유닛(104)에 송신한다. 만일 IDB가 널이 아니면, 등록 관리 유닛(113)은 IDB가 IDA와 동일한지의 여부를 결정할 수 있다.

[0115] 스테이지 C1에서는 IDB가 IDA와 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 IDB가 IDA와 동일한지의 여부를 결정한다. 만일 IDB가 IDA와 동일하면, 스테이지 D1에서 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다. 만일 IDB가 IDA와 동일하지 않으면, 스테이지 D2에서 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다.

[0116] 스테이지 C2에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 OK 응답을 송신한다. 예를들어, OK 응답은 네트워크 디바이스(112)가 등록될 준비가 되어 있다는 확인응답을 포함할 수 있으며 또한 IDX를 포함할 수 있다.

[0117] 스테이지 D1에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 사전에 등록되었음을 표시하기 위하여 키 관리 유닛(104)에 응답을 송신한다.

[0118] 스테이지 D2에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 다른 키 반송 디바이스에 등록되어 있다고 표시하기 위하여 키 관리 유닛(104)에 응답을 송신한다.

[0119] 스테이지 E에서, 키 합의, 키 유도 및 키 확인 동작들은 보안 통신 채널을 설정하기 위하여 수행된다. 일 구현에서, 키 관리 유닛(104) 및 등록 관리 유닛(113)은 보안 통신 채널을 설정하기 위하여 키 합의, 키 유도 및 키 확인 동작들을 수행한다. 예를들어, 키 관리 유닛(104) 및 등록 관리 유닛(113)은 보안 채널 키들(예를들어, 암호화 키, 무결성 키 및 시퀀스 번호 키)을 결정할 수 있다. 키 관리 유닛(104) 및 등록 관리 유닛(113)은 보안 채널 키들을 사용하여 보안 통신 채널을 설정할 수 있다. 보안 통신 채널은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 교환되는 임의의 메시지들에 대한 무결성 및 리플레이 보호를 보장할 수 있다. 키 관리 유닛(104) 및 등록 관리 유닛(113)은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에 보안 통신 채널이 존재하는 동안 암호화 키, 무결성 키 및 시퀀스 번호 카운터를 저장할 수 있다. 키 관리 유닛(104) 및 등록 관리 유닛(113)은 또한 스테이지들 I1 및 I2에서 이하에서 설명되는 바와같이 페어링 데이터로서 보안 채널 키들을 저장할 수 있다.

[0120] 스테이지 F에서, 네트워크 키는 보안 통신 채널을 통해 송신된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 통신 네트워크(100)의 네트워크 키를 보안 통신 채널을 통해 등록 관리 유닛(113)에 송신한다. 예를들어, 키 관리 유닛(104)은 메시지 생성시에 시퀀스 번호 카운터(SN)의 값과 함께 메시지(예를들어, 암호화 키를 사용하여 암호화되는 메시지)에서 네트워크 키를 송신할 수 있다. 키 반송 디바이스(102)

및 네트워크 디바이스(112)에 저장되는 시퀀스 번호 카운터들은 메시지가 생성될 때마다 증가될 수 있다는 것에 유의해야 한다.

[0121] 스테이지 G에서, 네트워크 키가 키 반송 디바이스(102)로부터 수신되는지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 키가 키 반송 디바이스(102)로부터 수신됨을 결정한다. 예를들어, 등록 관리 유닛(113)은 네트워크 키가 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정하기 위하여 스테이지 F에서 수신되는 메시지의 시퀀스 번호 카운터의 값을 활용할 수 있다. 등록 관리 유닛(113)은 키 반송 디바이스(102)로부터 수신되는 마지막 메시지 이후에 스테이지 F에서 수신되는 메시지의 시퀀스 번호 카운터의 값이 시퀀스에 있음을 검증함으로써 네트워크 키가 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정할 수 있다. 만일 네트워크 키가 키 반송 디바이스(102)로부터 수신되지 않으면, 등록 관리 유닛(113)은 스테이지 H1에서의 에러 메시지를 키 관리 유닛(104)에 송신할 수 있다. 만일 네트워크 키가 키 반송 디바이스(102)로부터 수신되면, 등록 관리 유닛(113)은 스테이지 H2에서의 등록 확인 메시지를 보안 통신 채널을 통해 키 관리 유닛(104)에 송신할 수 있다.

[0122] 스테이지 H1에서, 에러 메시지는 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 F에서 네트워크 디바이스(112)에 송신되는 네트워크 키가 키 반송 디바이스(102)로부터 송신되지 않았음을 표시하기 위하여 키 관리 유닛(104)에 에러 메시지를 송신한다. 일부 구현들에서, 스테이지 H1에서 에러 메시지를 수신할 때, 키 관리 유닛(104)은 등록 관리 유닛(113)에 네트워크 키를 송신하기 위하여 스테이지 F에서의 동작들을 반복할 수 있다.

[0123] 스테이지 H2에서, 등록 확인 메시지는 보안 통신 채널을 통해 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 NK가 네트워크 디바이스(112)에서 성공적으로 수신되었음을 키 관리 유닛(104)에 표시하기 위하여 등록 확인 메시지(예를들어, 암호화 키를 사용하여 암호화되는 메시지)를 보안 통신 채널을 통해 송신한다.

[0124] 스테이지 I1에서는 키 반송 디바이스(102)에서의 페어링 데이터가 업데이트된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 (네트워크 디바이스(112)에 대응하는) 페어링 데이터를 업데이트한다. 예를들어, 키 관리 유닛(104)은 (스테이지 C2에 수신되는) IDX와 동일하게 IDY를 세팅하고, 보안 통신 채널의 무결성 키와 동일하게 KI를 세팅하고, 보안 통신 채널의 암호화 키와 동일하게 KE를 세팅하며 보안 통신 채널의 시퀀스 번호 카운터와 동일하게 SN을 세팅할 수 있다.

[0125] 스테이지 I2에서는 네트워크 디바이스(112)에서의 페어링 데이터가 업데이트된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 페어링 데이터를 업데이트한다. 예를들어, 등록 관리 유닛(113)은 (스테이지 A에서 수신되는) IDA와 동일하게 IDB를 세팅하고, 보안 통신 채널의 무결성 키와 동일하게 KI'를 세팅하며, 보안 통신 채널의 암호화 키와 동일하게 KE'를 세팅하며, 보안 통신 채널의 시퀀스 번호 카운터와 동일하게 SN'을 세팅할 수 있다.

[0126] 도 6은 제 1 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 6은 (도 5를 참조로 하여 앞서 설명되는 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 네트워크 디바이스(112) 및 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 도 5에 설명된 페어링 데이터와 유사할 때 네트워크 디바이스(112)를 등록해제하기 위하여 제 1 구성 기술을 활용할 수 있다. 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 단지 네트워크 디바이스(112)를 등록해제할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 IDY가 IDX와 동일하고, IDB가 IDA와 동일하며, KI'가 등록동안 설정되는 보안 통신 채널의 무결성 키와 동일한 KI와 동일하며, KE'가 보안 통신 채널의 암호화 키와 동일한 KE와 동일하며, SN'가 보안 통신 채널의 시퀀스 번호와 동일한 SN과 동일하다는 것에 유의해야 한다. 도 6은 스테이지들 A-I2의 시퀀스에서 네트워크 디바이스(12)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 6이 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0127] 스테이지 A에서, 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 반송 디바이스(102)의 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 송신한다. 예를들어, 등록해제 요청은 등록해제할(즉, 페어링 데이터를 클리어할) 명령 및 IDA를 포함할 수 있다.

[0128] 스테이지 B에서는 IDB가 널임이 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 IDB의 값이 널인지의 여부를 결정한다. 만일 IDB가 널이면, 등록 관리 유닛(113)은 키 관리 유닛(104)에 스테이지 C1에서의 응답을 송신한다. 만일 IDB가 널이 아니면, 스테이지 C2에서 등록 관리 유닛(113)은 IDB가 IDA와 동일한지의 여부를 결정할 수 있다.

[0129] 스테이지 C1에서, 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(102)에 응답을 송신한다. 예를들어, 응답은 네트워크 디바이스(102)가 등록해제됨(즉, 어느 키 반송 디바이스에도 등록되지 않음)을 키 관리 유닛(104)에 표시할 수 있다.

[0130] 스테이지 C2에서, IDB가 IDA와 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 IDB가 IDA와 동일한지의 여부를 결정한다. 만일 IDB가 IDA와 동일하면, 등록 관리 유닛(113)은 스테이지 D2에서 키 관리 유닛(104)에 응답을 송신한다. 만일 IDB가 IDA와 동일하지 않으면, 스테이지 D1에서 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다.

[0131] 스테이지 D1에서는 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 다른 키 반송 디바이스에 등록되어 있다고 표시하기 위하여 키 관리 유닛(104)에 응답을 송신한다.

[0132] 스테이지 D2에서는 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 OK 응답을 송신한다. 예를들어, OK 응답은 네트워크 디바이스(112)가 등록해제될 준비가 되어 있다는 확인응답을 포함할 수 있다. OK 응답은 또한 IDX를 포함할 수 있다.

[0133] 스테이지 E1에서, 네트워크 디바이스(112)에 대한 보안 채널 키들이 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)에 대한 보안 채널 키들을 결정한다. 예를들어, 키 관리 유닛(104)은 스테이지 D2에서 수신되는 IDX에 기초하여 보안 채널 키들을 결정한다. 키 관리 유닛(104)은 네트워크 디바이스(112)의 등록 동안 키 반송 디바이스(102)에 저장되는 보안 채널 키들(예를들어, 무결성 키, 암호화 키 및 시퀀스 번호 카운터)를 찾을 수 있다.

[0134] 스테이지 E2에서, 보안 통신 채널이 설정된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 E1에서 결정되는 보안 채널 키들을 사용하여 등록 관리 유닛(113)과 보안 통신 채널을 설정한다. 보안 통신 채널은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 교환되는 메시지들에 대한 무결성 및 리플레이 보호를 보장할 수 있다.

[0135] 스테이지 F에서, 하나 이상의 명령들이 네트워크 디바이스(112)를 등록해제 하기 위하여 보안 통신 채널을 통해 송신된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위하여 등록 관리 유닛(113)에 하나 이상의 명령들을 가진 메시지(예를들어, 암호화 키를 사용하여 암호화된 메시지)를 송신할 수 있다. 예를들어, 메시지는 네트워크 디바이스(112)에 저장되는 네트워크 키 및 페어링 데이터를 클리어하기 위한 명령들을 포함할 수 있다. 메시지는 또한 메시지 생성시에 시퀀스 번호 카운터(SN)의 값을 포함할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 저장되는 시퀀스 번호 카운터들은 메시지가 생성될 때마다 증가될 수 있다는 것에 유의해야 한다.

[0136] 스테이지 G에서는 키 반송 디바이스(102)로부터 명령들이 수신되는지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 명령들이 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정한다. 예를들어, 등록 관리 유닛(113)은 명령들이 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정하기 위하여 스테이지 F에서 수신되는 메시지의 시퀀스 번호 카운터(SN)의 값을 활용할 수 있다. 등록 관리 유닛(113)은 키 반송 디바이스(102)로부터 수신되는 마지막 메시지 이후에 스테이지 F에서 수신되는 메시지의 시퀀스 번호 카운터의 값이 시퀀스에 있음을 검증함으로써 명령들이 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정할 수 있다. 만일 명령들이 키 반송 디바이스(102)로부터 수신되지 않으면, 등록 관리 유닛(113)은 스테이지 H1에서의 에러 메시지를 키 관리 유닛(104)에 송신할 수 있다. 만일 명령들이 키 반송 디바이스(102)로부터 수신되면, 등록 관리 유닛(113)은 스테이지 H2에서의 등록해제 확인 메시지를 보안 통신 채널을 통해 키 관리 유닛(104)에 송신할 수 있다.

[0137] 스테이지 H에서는 에러 메시지가 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 F에서 수신되는 명령들이 키 반송 디바이스(102)로부터 송신되지 않았음을 표시하기 위하여 키 관리 유닛(104)에 에러 메시지를 송신한다. 일부 구현들에서, 스테이지 H1에서 에러 메시지를 수신할 때, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제할 명령들을 재송신할 수 있다.

[0138] 스테이지 H2에서, 등록해제 확인 메시지는 보안 통신 채널을 통해 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 등록해제할 명령들이 키 반송 디바이스(102)로부터 네트워크 디바이스(112)에서 성공적으로 수신되었음을 키 관리 유닛(104)에 표시하기 위하여 보안 통신 채널을 통해 등록해제 확인 메시지(예를들어, 암호화 키를 사용하여 암호화되는 메시지)를 송신한다.

[0139] 스테이지 I1에서, 키 반송 디바이스(102)의 페어링 데이터가 클리어된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 (네트워크 디바이스(112)에 대응하는) 페어링 데이터를 클리어한다. 예를들어, 키 관리 유닛(104)은 널과 동일하게 IDY, KI, KE 및 SN을 세팅할 수 있다.

[0140] 스테이지 I2에서, 네트워크 디바이스(112)에 저장되는 네트워크 키 및 페어링 데이터가 클리어된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(12)에 저장되는 페어링 데이터를 클리어한다. 예를들어, 등록 관리 유닛(113)은 널과 동일하게 IDB, KI', KE' 및 SN'을 세팅할 수 있다. 등록 관리 유닛(113)은 또한 네트워크 디바이스(112)에 저장되는 (키 반송 디바이스(102)에 등록하는 동안 수신되었던) 네트워크 키를 삭제할 수 있다.

[0141] 도 7은 제 2 구성 기술을 사용하여 네트워크 디바이스를 등록하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 7은 (도 1를 참조로 하여 앞서 설명되는 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 키 반송 디바이스의 공개 키를 포함할 때 제 2 구성 기술을 활용할 수 있다. 예를들어, 네트워크 디바이스(112)는 변수 QB로 공개 키를 저장할 수 있다. 키 반송 디바이스(102)의 공개 키가 QA임에 유의해야 하며, 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 QB는 QA로서 세팅될 수 있다. 제 2 구성 기술에서 키 반송 디바이스(102)가 키 반송 디바이스(102)와 페어링되는 네트워크 디바이스들에 대한 페어링 데이터를 저장하지 않는다는 것에 또한 유의해야 한다. 도 7은 스테이지들 A-I의 시퀀스에서 네트워크 디바이스(112)를 등록하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 7이 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0142] 스테이지 A에서, 등록 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 반송 디바이스(102)의 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록 요청을 송신한다. 예를들어, 등록 요청은 등록할 명령 및 QA를 포함할 수 있다.

[0143] 스테이지 B에서는 QB가 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 QB의 값이 널인지의 여부를 결정한다. 만일 QB가 널이면, 등록 관리 유닛(113)은 스테이지 C2에서의 응답을 키 관리 유닛(104)에 송신한다. 만일 QB가 널이 아니면, 스테이지 C1에서 등록 관리 유닛(113)은 QB가 QA와 동일한지의 여부를 결정할 수 있다.

[0144] 스테이지 C1에서는 QB가 QA와 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 QB가 QA와 동일한지의 여부를 결정한다. 만일 QB가 QA와 동일하면, 스테이지 D1에서 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다. 만일 QB가 QA와 동일하지 않으면, 스테이지 D2에서 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다.

[0145] 스테이지 C2에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다. 예를들어, 응답은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 준비가 되어 있다는 확인응답을 포함할 수 있다.

[0146] 스테이지 D1에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 사전에 등록되었음을 표시하기 위하여 키 관리 유닛(104)에 응답을 송신한다.

[0147] 스테이지 D2에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 다른 키 반송 디바이스에 등록되어 있다고 표시하기 위하여 키 관리 유닛(104)에 응답을 송신한다.

[0148] 스테이지 E에서, 키 합의, 키 유도 및 키 확인 동작들은 보안 통신 채널을 설정하기 위하여 수행된다. 일 구현에서, 키 관리 유닛(104) 및 등록 관리 유닛(113)은 보안 통신 채널을 설정하기 위하여 키 합의, 키 유도 및 키 확인 동작들을 수행한다. 예를들어, 키 관리 유닛(104) 및 등록 관리 유닛(113)은 보안 채널 키들(예를들어,

암호화 키, 무결성 키 및 시퀀스 번호 키)을 결정할 수 있다. 키 관리 유닛(104) 및 등록 관리 유닛(113)은 보안 채널 키들을 사용하여 보안 통신 채널을 설정할 수 있다. 보안 통신 채널은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 교환되는 메시지들에 대한 무결성 및 리플레이 보호를 보장할 수 있다. 키 관리 유닛(104) 및 등록 관리 유닛(113)은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에 보안 통신 채널이 존재하는 동안 암호화 키, 무결성 키 및 시퀀스 번호 카운터를 저장할 수 있다.

[0149] 스테이지 F에서, 네트워크 키는 보안 통신 채널을 통해 송신된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 통신 네트워크(100)의 네트워크 키를 보안 통신 채널을 통해 등록 관리 유닛(113)에 송신한다. 예를들어, 키 관리 유닛(104)은 메시지 생성시에 시퀀스 번호 카운터(SN)의 값과 함께 메시지(예를들어, 암호화 키를 사용하여 암호화되는 메시지)에서 네트워크 키를 송신할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 저장되는 시퀀스 번호 카운터들은 메시지가 생성될 때마다 증가될 수 있다는 것에 유의해야 한다.

[0150] 스테이지 G에서, 네트워크 키가 키 반송 디바이스(102)로부터 수신되는지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 키가 키 반송 디바이스(102)로부터 수신됨을 결정한다. 예를들어, 등록 관리 유닛(113)은 네트워크 키가 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정하기 위하여 스테이지 F에서 수신되는 메시지의 시퀀스 번호 카운터의 값을 활용할 수 있다. 등록 관리 유닛(113)은 키 반송 디바이스(102)로부터 수신되는 마지막 메시지 이후에 메시지의 시퀀스 번호 카운터의 값이 시퀀스에 있음을 검증함으로써 네트워크 키가 키 반송 디바이스(102)로부터 수신되는지의 여부를 결정할 수 있다. 만일 네트워크 키가 키 반송 디바이스(102)로부터 수신되지 않으면, 등록 관리 유닛(113)은 스테이지 H1에서의 에러 메시지를 키 관리 유닛(104)에 송신할 수 있다. 만일 네트워크 키가 키 반송 디바이스(102)로부터 수신되면, 등록 관리 유닛(113)은 스테이지 H2에서의 등록 확인 메시지를 보안 통신 채널을 통해 키 관리 유닛(104)에 송신할 수 있다.

[0151] 스테이지 H1에서, 에러 메시지는 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 F에서 네트워크 디바이스(112)에 의해 수신되는 네트워크 키가 키 반송 디바이스(102)로부터 송신되지 않았음을 표시하기 위하여 키 관리 유닛(104)에 에러 메시지를 송신한다. 일부 구현들에서, 스테이지 H1에서 에러 메시지를 수신할 때, 키 관리 유닛(104)은 등록 관리 유닛(113)에 네트워크 키를 재송신할 수 있다.

[0152] 스테이지 H2에서, 등록 확인 메시지는 보안 통신 채널을 통해 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 키가 네트워크 디바이스(112)에서 성공적으로 수신되었음을 키 관리 유닛(104)에 표시하기 위하여 등록 확인 메시지(예를들어, 암호화 키를 사용하여 암호화되는 메시지)를 보안 통신 채널을 통해 송신한다.

[0153] 스테이지 I에서는 네트워크 디바이스(112)에서의 페어링 데이터가 업데이트되며 네트워크 키가 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 페어링 데이터를 업데이트한다. 예를들어, 등록 관리 유닛(113)은 페어링 데이터를 업데이트하기 위하여 (스테이지 A에서 수신되는) QA와 동일하게 QB를 세팅할 수 있다. 등록 관리 유닛(113)은 스테이지 F에서 키 관리 유닛(104)으로부터 네트워크 디바이스(112)에서 수신되는 네트워크 키를 또한 세이브할 수 있다.

[0154] 도 8은 제 2 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 8은 (도 7를 참조로 하여 앞서 설명되는 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 도 7에 설명된 페어링 데이터와 유사할 때 네트워크 디바이스(112)를 등록해제하기 위하여 제 2 구성 기술을 활용할 수 있다. 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 단지 네트워크 디바이스(112)를 등록해제할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 QB가 QA와 동일하다는 것에 유의해야 한다. 도 8은 스테이지들 A-G의 시퀀스에서 네트워크 디바이스(12)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 8이 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0155] 스테이지 A에서, 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 반송 디바이스(102)의 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 송신한다. 예를들어, 등록해제 요청은 등록해제할 (즉, 페어링 데이터를 클리어할) 명령 및 QA를 포함할 수 있다.

[0156] 스테이지 B에서는 QB가 널임이 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장

되는 QB의 값이 널인지의 여부를 결정한다. 만일 QB가 널이면, 등록 관리 유닛(113)은 키 관리 유닛(104)에 스테이지 C1에서의 응답을 송신한다. 만일 QB가 널이 아니면, 스테이지 C2에서 등록 관리 유닛(113)은 QB가 QA와 동일한지의 여부를 결정할 수 있다.

[0157] 스테이지 C1에서, 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 응답을 송신한다. 예를들어, 응답은 네트워크 디바이스(102)가 등록해제됨(즉, 어느 키 반송 디바이스에도 등록되지 않음)을 키 관리 유닛(104)에 표시할 수 있다.

[0158] 스테이지 C2에서, QB가 QA와 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 QB가 QA와 동일한지의 여부를 결정한다. 만일 QB가 QA와 동일하면, 등록 관리 유닛(113)은 스테이지 D1에서 키 관리 유닛(104)에 응답을 송신한다. 만일 QB가 QA와 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 D2에서 키 관리 유닛(104)에 응답을 송신한다.

[0159] 스테이지 D1에서는 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 다른 키 반송 디바이스에 등록되어 있다고 표시하기 위하여 키 관리 유닛(104)에 응답을 송신한다.

[0160] 스테이지 D2에서는 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 응답을 송신한다. 예를들어, 응답은 네트워크 디바이스(112)가 등록해제될 준비가 되어 있다는 확인응답을 포함할 수 있다.

[0161] 스테이지 E에서, 키 합의, 키 유도 및 키 확인 동작들이 수행된다. 일 구현에서, 키 관리 유닛(104) 및 등록 관리 유닛(113)은 키 합의, 키 유도 및 키 확인 절차들을 수행한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)에 자신의 아이덴티티를 증명하기 위하여 키 합의, 키 유도 및 키 확인 동작들을 개시할 수 있다(예를들어, 성공적인 키 확인은 키 반송 디바이스(102)가 QB와 연관된 보안 키(예를들어, 암호화 키)의 지식을 가진다는 것을 표시한다). 일부 구현들에서, 키 관리 유닛(104)은 키 반송 디바이스(102)가 QB와 연관된 비밀키의 지식을 가질 때 유효한 것으로 (등록 관리 유닛(113)에 송신되는 메시지들에) 무결성 키(예를들어, MAC)를 세팅할 수 있다. 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이의 키 합의, 키 유도 및 키 확인 동작들은 네트워크 디바이스(112)가 키 반송 디바이스(102)를 식별하는 것을 가능하게 할 수 있다.

[0162] 스테이지 F1에서는 키 합의, 키 유도 및 키 확인 동작들이 성공적인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 키 반송 디바이스(102)를 사용한 키 합의, 키 유도 및 키 확인 동작들이 성공적인지의 여부를 결정한다. 키 합의, 키 유도 및 키 확인 동작들의 성공은, 등록 관리 유닛(113)으로 하여금, 스테이지 A에서의 등록해제 요청이 키 반송 디바이스(102)로부터 수신되었음을 결정하도록 할 수 있다. 일부 구현들에서, 등록 관리 유닛(113)은 스테이지 A에서의 등록해제 요청이 키 반송 디바이스(102)로부터 수신되었음을 결정하기 위하여 키 관리 유닛(104)으로부터 수신되는 메시지의 무결성 키가 유효한지의 여부를 결정한다. 만일 키 합의, 키 유도 및 키 확인 동작들이 성공적이면, 등록 관리 유닛(113)은 스테이지 F2에서 (등록 동안 키 반송 디바이스(102)로부터 수신되는) 네트워크 키 및 페어링 데이터를 클리어한다. 만일 키 합의, 키 유도 및 키 확인 동작들이 성공적이지 않으면, 등록 관리 유닛(113)은 스테이지 G에서 네트워크 디바이스(112)의 등록해제를 중단한다.

[0163] 스테이지 F2에서, 네트워크 디바이스(112)에 저장되는 네트워크 키 및 페어링 데이터는 클리어된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 네트워크 키 및 페어링 데이터를 클리어한다. 예를들어, 등록 관리 유닛(113)은 네트워크 키를 삭제하고 널로서 QB를 세팅할 수 있다. 일부 구현들에서, 페어링 데이터 및 네트워크 키를 클리어할 때, 네트워크 디바이스(112)는 키 반송 디바이스(102)에 확인 메시지를 송신할 수 있다.

[0164] 스테이지 G에서, 등록해제가 중단된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)의 등록해제를 중단한다. 예를들어, 키 합의, 키 유도 및 키 확인 동작들이 스테이지 F1에서 성공적이지 않을 때, 등록 관리 유닛(113)은 네트워크 디바이스(112)의 등록해제를 중단할 수 있다. 일부 구현들에서, 등록 관리 유닛(113)은 등록해제를 중단할 때 키 관리 유닛(104)에 에러 메시지를 송신할 수 있다.

[0165] 도 9, 도 10, 도 11 및 도 12는 제 3 구성 기술을 사용하여 네트워크 디바이스를 등록하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 9, 도 10, 도 11 및 도 12는 (도 1를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 등록 키(RKk)를 포함하고 네트워크 디바이스(112)상에 저장되는 페어링

데이터가 등록 키(RKn)를 포함할 때 제 3 구성 기술을 활용할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 또한 네트워크 키(NK) 및 네트워크 키(NK')를 저장할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 RKk 및 RKn을 암호화하여 보안적으로 교환하기 위하여 해싱 알고리즘으로 합의될 수 있다. 해싱 알고리즘은 RKk 및 RKn을 암호화하기 위하여 난수를 활용할 수 있다. 예를들어, 난수는 등록 키로 연접될 수 있으며(즉, 난수의 비트들은 연접된 값을 결정하기 위하여 등록 키에 첨부될 수 있으며), 이후 연접된 값의 해싱된 값은 등록 키의 암호화된 값으로서 계산될 수 있다. 난수는 네트워크 디바이스(112)와 키 반송 디바이스(102) 간에 어느 암호화도 없이 교환될 수 있으며, 네트워크 디바이스(112) 및 키 반송 디바이스(102)가 자신들의 등록 키들을 암호화하도록 한다. RKk 및 RKn은 각각 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 등록 키들을 저장하기 위한 예시적인 변수들을 나타낸다는 것에 유의해야 한다. 유사하게, NK 및 NK'는 각각 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 네트워크 키들을 저장하기 위한 예시적인 변수들을 나타낸다는 것에 유의해야 한다. RKk 및 RKn는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 동일하다는 것에 추가로 유의해야 한다. 또한, NK 및 NK'의 값들은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 의해 관리되는 통신 네트워크(즉, 통신 네트워크(100))로 구성될 때 동일하다. RKn 및 NK'는 네트워크 디바이스(112)가 어느 키 반송 디바이스에도 등록되지 않을 때 널일 수 있다는 것에 또한 유의해야 한다. 일부 구현들에서, RKk 및 NK는 또한 (예를들어, 키 반송 디바이스(102)가 통신 네트워크(100)의 네트워크 키를 가지지 않을 때) 널일 수 있다. 그러나, 키 반송 디바이스(102)는 RKk 및/또는 NK의 값들이 널일때 RKk 및 NK의 랜덤값을 생성하는 능력들을 포함한다. 도 9, 도 10, 도 11 및 도 12는 스테이지들 A-D의 시퀀스에서 네트워크 디바이스(112)를 등록하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 9, 도 10, 도 11 및 도 12가 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 수행될 수 있다.

[0166] 스테이지 A에서, 헬로 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 반송 디바이스(102)의 키 관리 유닛(104)은 헬로 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 헬로 요청은 난수 N1을 포함할 수 있다. 난수 N1은 스테이지 B에서 RKn을 암호화하기 위하여 등록 관리 유닛(113)에 의해 활용될 수 있다.

[0167] 스테이지 B에서, RKn 및 NK'의 암호화된 값들이 계산된다. 일 구현에서, 등록 관리 유닛(113)은 RKn 및 NK'의 암호화된 값들을 계산한다. 예를들어, 등록 관리 유닛(113)은 키 반송 디바이스(102)에 따른 해싱 알고리즘을 사용하여 NK'의 해싱된 값 및 N1과 연접된 RKn의 해싱된 값을 계산할 수 있다. RKn 및/또는 NK'가 널일때 RKn 및/또는 NK'의 암호화된 값들이 또한 널일 수 있다는 것에 유의해야 한다.

[0168] 스테이지 C에서, 헬로 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 헬로 응답을 송신한다. 예를들어, 헬로 응답은 (스테이지 B에서 계산되는) RKn 및 NK'의 암호화된 값 및 난수 N2를 포함할 수 있다. 난수 N2는 (스테이지 01에서 이하에서 설명되는 바와같이) RKk를 암호화하기 위하여 키 관리 유닛(104)에 의해 활용될 수 있다.

[0169] 스테이지 D에서, RKn의 암호화된 값이 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 C에서 수신되는) RKn의 암호화된 값이 널인지의 여부를 결정한다. 만일 RKn의 암호화된 값이 널이면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 어느 키 반송 디바이스에도 등록되지 않음을 결정할 수 있으며, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록할 수 있다. 예를들어, RKn의 암호화된 값이 널이면, 키 관리 유닛(104)은 스테이지 E에서의 동작들을 수행할 수 있다. 만일 RKn의 암호화된 값이 널이 아니면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 제어는 링크 2.1로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 K에서의 동작들을 수행할 수 있다.

[0170] 스테이지 E에서는 RKk가 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장된 RKk가 널인지의 여부를 결정한다. 만일 RKk가 널이면, 키 관리 유닛(104)은 스테이지 F에서의 동작들을 수행할 수 있다. 만일 RKk가 널이 아니면, 키 관리 유닛(104)은 스테이지 G에서의 동작들을 수행할 수 있다.

[0171] 스테이지 F에서, 랜덤 RKk가 생성된다. 일 구현에서, 키 관리 유닛(104)은 의사 난수 알고리즘을 사용하여 랜덤 RKk를 생성한다. 예를들어, 등록 키가 키 반송 디바이스(102)에 존재하지 않을 때, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스(112)를 등록하기 위하여 등록 관리 유닛(113)에 송신될 수 있는 새로운 랜덤 등록 키를 생성할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 RKk로서 랜덤 RKk를 세이브한다.

[0172] 스테이지 G에서, 네트워크 디바이스(112)와 보안 통신 채널이 설정된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)을 사용하여 키 합의, 키 유도 및 키 확인 동작들을 수행함으로써 보안 통신 채널을 설정할 수 있다. 보안 통신 채널은 키 관리 유닛(104)이 RKk를 암호화하지 않고 (스테이지 H에서) 등록 관리 유닛(113)에 RKk를 송신하도록 할 수 있다.

[0173] 스테이지 H에서, 등록 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 요청을 보안 통신 채널을 통해 등록 관리 유닛(113)에 송신한다. 예를들어, 등록 요청은 RKk를 포함할 수 있다.

[0174] 스테이지 I에서, RKk는 네트워크 디바이스(112)에 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 H에서 등록 요청에서 키 관리 유닛(104)으로부터 수신되는 RKk를 세이브한다. 예를들어, 등록 관리 유닛(113)은 RKk를 세이브하기 위하여 RKk와 동일하게 RKn을 세팅할 수 있으며, 키 반송 디바이스(102)에 등록할 수 있다.

[0175] 스테이지 J에서, 등록 응답이 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록 응답을 송신한다. 예를들어, 등록 응답은 네트워크 디바이스(112)가 네트워크 반송 디바이스(102)에 등록되어 있다고 키 관리 유닛(104)에 표시할 수 있다. 스테이지 J에서 등록 응답을 수신할 때, 제어는 링크 2.2로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 M에서의 동작들을 수행할 수 있다.

[0176] 스테이지 K에서는 RKn의 암호화된 값이 RKk의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 C에서 수신되는) RKn의 암호화된 값이 RKk의 암호화된 값과 동일한지의 여부를 결정한다. 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N1과 연접되는 RKn의 해싱된 값을 계산함으로써 RKk의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKk의 암호화된 값과 동일하면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정할 수 있으며, 키 관리 유닛(104)은 스테이지 M에서의 동작들을 수행할 수 있다. 만일 RKn의 암호화된 값이 RKk의 암호화된 값과 동일하지 않으면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 (키 반송 디바이스(102)과 상이한) 다른 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 키 관리 유닛(104)은 스테이지 L에서의 등록 동작들을 중지할 수 있다.

[0177] 스테이지 L에서 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스(112)를 등록할 동작들을 중지할 수 있다.

[0178] 스테이지 M에서는 NK'의 암호화된 값이 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 C에서 수신되는) NK'의 암호화된 값이 널인지의 여부를 결정한다. 만일 NK'의 암호화된 값이 널이면, 키 관리 유닛(104)은 네트워크 키가 네트워크 디바이스(112)에 저장되지 않음을 결정할 수 있으며, 제어는 링크 4로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 V에서의 동작들을 수행할 수 있다. 만일 NK'의 암호화된 값이 널이 아니면, 키 관리 유닛(104)은 스테이지 N에서의 동작들을 수행할 수 있다.

[0179] 스테이지 N에서는 네트워크 디바이스(112)의 네트워크 키를 사용해야 하는지가 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)의 네트워크 키를 사용해야 하는지를 결정한다. 예를들어, 키 관리 유닛(104)은 통신 네트워크(100)의 네트워크 키가 키 반송 디바이스(102)에 저장되지 않을 때 네트워크 디바이스(112)에 저장되는 네트워크 키를 사용할 것을 (예를들어, 수신하여 세이브할 것을) 결정할 수 있다. 만일 키 관리 유닛(104)이 네트워크 디바이스(112)의 네트워크 키를 사용할 것을 결정하면, 제어는 링크 3으로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 O1에서의 동작들을 수행할 수 있다. 만일 키 관리 유닛(104)이 네트워크 디바이스(1120의 네트워크 키를 사용하지 않을 것을 결정하면, 제어는 링크 4로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 V에서의 동작들을 수행할 수 있다.

[0180] 스테이지 O1에서, RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N2(즉, 스테이지 C에서 수신되는 N2)와 연접되는 RKk의 해싱된 값을 계산한다.

[0181] 스테이지 O2에서, 겟 네트워크 키 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 겟 네트워크 키 요청을 송신한다. 예를들어, 겟 네트워크 키 요청은 (스테이지 O1에서 계산되는) RKk의 암호화된 값을 포함한다. 겟 네트워크 키 요청은 네트워크 디바이스(112)에 저장되는 NK'에 대한 요청을 포함할 수 있다.

[0182] 스테이지 P에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록

관리 유닛(113)은 (스테이지 O2에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N2와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 겟 네트워크 키 요청이 (악의적인 디바이스가 아니라) 키 반송 디바이스(102)로부터 수신되었음을 검증할 수 있으며, 등록 관리 유닛(113)은 스테이지 R에서 겟 네트워크 키 응답을 송신할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 O2에서의 겟 네트워크 키 요청이 악의적인 디바이스에 의해 송신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 Q에서 에러를 검출할 수 있다.

[0183] 스테이지 Q에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스에 의해 송신되는 겟 네트워크 키 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0184] 스테이지 R에서, 겟 네트워크 키 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 겟 네트워크 키 응답을 송신한다. 예를들어, 겟 네트워크 키 응답은 스테이지 P에서 RKk의 암호화된 값이 RKn의 암호화된 값과 동일함을 등록 관리 유닛(113)이 결정할 때 NK'를 포함할 수 있다. 겟 네트워크 키 응답은 스테이지 P에서 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않을 때 스테이지 Q에서 검출되는 에러를 포함할 수 있다. 일부 구현들에서, 등록 관리 유닛(113)은 키 관리 유닛(104)과 (예를들어, 키 합의, 키 유도 및 키 확인 동작들을 수행함으로써) 보안 채널을 설정할 수 있으며, 보안 통신 채널을 통해 겟 네트워크 키 응답을 송신할 수 있다.

[0185] 스테이지 S에서는 겟 네트워크 키 응답이 에러를 포함하는지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 겟 네트워크 키 응답이 에러를 포함하는지의 여부를 결정한다. 예를들어, 스테이지 Q에서, 키 관리 유닛(104)은 겟 네트워크 키 응답이 등록 관리 유닛(113)에 의해 검출되는 에러를 포함함을 결정할 수 있다. 만일 겟 네트워크 키 응답이 에러를 포함하면, 키 관리 유닛(104)은 스테이지 U에서의 등록 동작들을 중지할 수 있다. 만일 겟 네트워크 키 응답이 에러를 포함하지 않으면, 키 관리 유닛(104)은 스테이지 T에서의 동작들을 수행할 수 있다.

[0186] 스테이지 T에서, NK'가 세이브된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 R에서 등록 관리 유닛(113)으로부터 등록 응답에서 수신되는 NK'를 세이브한다. 예를들어, 키 관리 유닛(104)은 NK'를 세이브하기 위하여 NK'와 동일하게 NK를 세팅할 수 있다.

[0187] 스테이지 U에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다.

[0188] 스테이지 V에서는 NK가 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 NK가 널인지의 여부를 결정한다. 만일 NK가 널이면, 키 관리 유닛(104)은 스테이지 W에서의 동작들을 수행할 수 있다. 만일 NK가 널이 아니면, 키 관리 유닛(104)은 스테이지 X에서의 동작들을 수행할 수 있다.

[0189] 스테이지 W에서는 랜덤 NK가 생성된다. 일 구현에서, 키 관리 유닛(104)은 랜덤 NK를 생성한다. 예를들어, 키 관리 유닛(104)은 의사 난수 알고리즘을 사용하여 랜덤 NK를 생성할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 키 반송 알고리즘(102)에 저장되는 NK로서 랜덤 NK를 세이브한다. 스테이지 W 이후에, 키 관리 유닛(104)은 스테이지 X에서의 동작들을 수행할 수 있다.

[0190] 스테이지 X에서는 RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N2(즉, 스테이지 C에서 수신되는 N2)와 연접되는 RKk의 해싱된 값을 계산할 수 있다.

[0191] 스테이지 Y에서는 세트 네트워크 키 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 세트 네트워크 요청을 송신한다. 예를들어, 세트 네트워크 키 요청은 (스테이지 X에서 계산되는) RKk의 암호화된 값 및 NK를 포함할 수 있다. 일부 구현들에서, 세트 네트워크 키 요청은 NK 대신에 NK의 암호화된 값을 포함할 수 있다. 다른 구현들에서, 키 관리 유닛(104)은 등록 관리 유닛(113)과 보안 통신 채널을 설정할 수 있으며, 보안 통신 채널을 통해 세트 네트워크 키 요청을 송신할 수 있다.

[0192] 스테이지 Z에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 Y에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결

정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N2와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 스테이지 Y에서의 세트 네트워크 키 요청이 (악의적인 디바이스가 아니라) 키 반송 디바이스(102)로부터 수신되었음을 검증할 수 있으며, 등록 관리 유닛(113)은 스테이지 AB에서 NK를 세이브할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 Y에서의 세트 네트워크 키 요청이 악의적인 디바이스에 의해 송신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 AA에서 에러를 검출할 수 있다.

[0193] 스테이지 AA에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스에 의해 송신되는 세트 네트워크 키 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0194] 스테이지 AB에서는 NK가 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 Y에서 세트 네트워크 키 요청에서 수신되는 NK를 세이브한다. 예를들어, 등록 관리 유닛(113)은 네트워크 디바이스(112)에서 NK를 세이브하기 위하여 NK와 동일하게 NK'를 세팅할 수 있다.

[0195] 스테이지 AC에서, 세트 네트워크 키 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 세트 네트워크 키 응답을 송신한다. 예를들어, 스테이지 AB에서, 세트 네트워크 키 응답은 등록 관리 유닛(113)이 NK를 세이브할 때 확인응답을 포함할 수 있다. 세트 네트워크 키 응답은 등록 관리 유닛(113)이 스테이지 AA에서 에러를 검출할 때 에러를 포함할 수 있다.

[0196] 스테이지 AD에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다. 예를들어, 키 관리 유닛(104)은 등록 관리 유닛(113)으로부터 세트 네트워크 키 응답을 수신할 때 등록 동작들을 중지할 수 있다. 일부 구현들에서, 세트 네트워크 키 응답이 에러를 포함할 때, 키 관리 유닛(104)은 등록 관리 유닛(113)에 세트 네트워크 키 요청을 재송신하기 위한 하나 이상의 동작들을 수행할 수 있다.

[0197] 도 13은 제 3 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 제 1 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 13은 (도 9, 도 10, 도 11 및 도 12를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 네트워크 디바이스(112) 및 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 도 9, 도 10, 도 11 및 도 12에 설명되는 페어링 데이터와 유사할 때 제 3 구성 기술을 사용하여 네트워크 디바이스(112)를 등록해제하기 위하여 제 1 옵션을 활용할 수 있다. 제 1 구성 기술을 사용하여 네트워크 디바이스(112)를 등록해제할 제 1 옵션에서, 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정하기 위한 동작들을 수행한다. 키 반송 디바이스(102)는 단지 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 네트워크 디바이스(112)를 등록해제할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 RKn은 RKk와 동일하다는 것에 유의해야 한다. 도 13은 스테이지들 A-L의 시퀀스에서 네트워크 디바이스(112)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 13이 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0198] 스테이지 A에서, 헬로 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 헬로 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 헬로 요청은 난수 N1을 포함할 수 있다. 난수 N1은 스테이지 B에서 RKn을 암호화하기 위하여 등록 관리 유닛(113)에 의해 활용될 수 있다.

[0199] 스테이지 B에서, RKn 및 NK'의 암호화된 값들이 계산된다. 일 구현에서, 등록 관리 유닛(113)은 RKn 및 NK'의 암호화된 값들을 계산한다. 예를들어, 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 NK'의 해싱된 값 및 N1과 연접된 RKn의 해싱된 값을 계산할 수 있다. RKn 및/또는 NK'가 널일때 RKn 및/또는 NK'의 암호화된 값들이 또한 널일 수 있다는 것에 유의해야 한다.

[0200] 스테이지 C에서, 헬로 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 헬로 응답을 송신한다. 예를들어, 헬로 응답은 (스테이지 B에서 계산되는) RKn 및 NK'의 암호화된 값 및 난수 N2를 포함할 수 있다. 난수 N2는 (스테이지 F에서 이하에서 설명되는 바와같이) RKk를 암호화하기 위하여 키 관리 유닛(104)에 의해 활용될 수 있다.

[0201] 스테이지 D에서, RKn의 암호화된 값이 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테

이지 C에서 수신되는) RKn의 암호화된 값이 널인지의 여부를 결정한다. 만일 RKn의 암호화된 값이 널이면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 어느 키 반송 디바이스에도 등록되지 않음을 결정할 수 있으며, 스테이지 L에서 키 관리 유닛(104)은 등록해제 동작들을 중지할 수 있다. 만일 RKn의 암호화된 값이 널이 아니면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 키 관리 유닛(104)은 스테이지 E에서의 동작들을 수행할 수 있다.

[0202] 스테이지 E에서는 RKn의 암호화된 값이 RKk의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 C에서 수신되는) RKn의 암호화된 값이 RKk의 암호화된 값과 동일한지의 여부를 결정한다. 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N1과 연접되는 RKk의 해싱된 값을 계산함으로써 RKk의 암호화된 값을 계산할 수 있다. 만일 RKn의 암호화된 값이 RKk의 암호화된 값과 동일하면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정할 수 있으며, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제할 수 있다. 만일 RKn의 암호화된 값이 RKk의 암호화된 값과 동일하지 않으면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 (키 반송 디바이스(102)과 상이한) 다른 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 키 관리 유닛(104)은 스테이지 L에서의 등록해제 동작들을 중지할 수 있다.

[0203] 스테이지 F에서, RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N2(즉, 스테이지 C에서 수신되는 N2)와 연접되는 RKk의 해싱된 값을 계산한다.

[0204] 스테이지 G에서, 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 송신한다. 예를들어, 등록해제 요청은 (스테이지 F에서 계산되는) RKk의 암호화된 값 및 RKn 및 NK'를 삭제할 요청을 포함할 수 있다.

[0205] 스테이지 H에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 G에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N2와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 등록해제 요청이 (악의적인 디바이스가 아니라) 키 반송 디바이스(102)로부터 수신되었음을 검증할 수 있으며, 등록 관리 유닛(113)은 스테이지 L에서 RLn 및 NK'의 값을 삭제할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 G에서의 등록해제 요청이 악의적인 디바이스에 의해 송신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 J에서 에러를 검출할 수 있다.

[0206] 스테이지 I에서, RKn 및 NK'의 값들이 삭제된다. 일 구현에서, 등록 관리 유닛(113)은 RKn 및 NK'의 값들을 삭제한다. 일단 RKn 및 NK'의 값들이 삭제되면, 네트워크 디바이스(112)는 더 이상 키 반송 디바이스(102)에 등록되지 않으며, 등록 관리 유닛(113)은 (스테이지 K에서 이하에서 설명되는 바와같이) 네트워크 디바이스(112)의 등록해제를 확인하기 위하여 키 관리 유닛(104)에 확인응답을 송신할 수 있다.

[0207] 스테이지 J에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스에 의해 송신되는 등록해제 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0208] 스테이지 K에서, 등록해제 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록해제 응답을 송신한다. 예를들어, 등록해제 응답은 등록 관리 유닛(113)이 스테이지 I에서 RKn 및 NK'의 값들을 삭제할 때 확인응답을 포함할 수 있다. 등록해제 응답은 등록 관리 유닛(113)이 스테이지 J에서 에러를 검출할 때 에러를 포함할 수 있다.

[0209] 스테이지 L에서, 등록해제 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 동작들을 중지한다. 일부 구현들에서, 키 관리 유닛(104)은 (스테이지 K에서 수신되는) 등록해제 응답이 에러를 포함할 때 등록 관리 유닛(113)에 등록해제 요청을 재송신할 수 있다.

[0210] 도 14는 제 3 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 제 2 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 14는 (도 9, 도 10, 도 11 및 도 12를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 네트워크 디바이스(112) 및 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 도 9, 도 10, 도 11 및 도 12에 설명되는 페어링 데이

터와 유사할 때 제 3 구성 기술을 사용하여 네트워크 디바이스(112)를 등록해제하기 위하여 제 2 옵션을 활용할 수 있다. 제 3 구성 기술을 사용하여 네트워크 디바이스(112)를 등록해제할 제 2 옵션에서, 네트워크 디바이스(112)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정하기 위한 동작들을 수행한다. 키 반송 디바이스(102)로부터 등록해제 요청을 수신할 때, 네트워크 디바이스(112)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 네트워크 디바이스(112)가 결정할 때 단지 등록해제 동작들을 수행할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 RKn은 RKk와 동일하다는 것에 유의해야 한다. 도 14는 스테이지들 A-J의 시퀀스에서 네트워크 디바이스(112)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 14가 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0211] 스테이지 A에서, 임시 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 임시 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 임시 요청은 등록 관리 유닛(113)으로부터의 난수에 대한 요청을 포함한다.

[0212] 스테이지 B에서, 난수가 생성된다. 일 구현에서, 등록 관리 유닛(113)은 난수(즉, N1)을 생성한다. 예를들어, 등록 관리 유닛(113)은 N1이 키 반송 디바이스(102)와 네트워크 디바이스(112)사이에서 합의된 해싱 알고리즘을 사용하여 등록 키를 암호화하기 위하여 활용될 수 있도록 N1을 생성할 수 있다.

[0213] 스테이지 C에서, 임시 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 임시 응답을 송신한다. 예를들어, 임시 응답은 (스테이지 B에서 생성되는) N1을 포함할 수 있다.

[0214] 스테이지 D에서, RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N1 (즉, 스테이지 C에서 수신되는 N1)와 연접되는 RKk의 해싱된 값을 계산할 수 있다.

[0215] 스테이지 E에서, 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 송신한다. 예를들어, 등록해제 요청은 (스테이지 D에서 계산되는) RKk의 암호화된 값 및 RKn 및 NK'를 삭제할 요청을 포함할 수 있다.

[0216] 스테이지 F에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 G에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N1와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 등록해제 요청이 키 반송 디바이스(102)로부터 수신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 G에서 RKn 및 NK'의 값을 삭제할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 등록해제 요청이 키 반송 디바이스(102)로부터 수신되지 않았음을(그리고, 대신에 악의적인 디바이스로부터 수신되었음을) 결정할 수 있으며, 등록 관리 유닛(13)은 스테이지 H에서 에러를 검출할 수 있다.

[0217] 스테이지 G에서, RKn 및 NK'의 값들이 삭제된다. 일 구현에서, 등록 관리 유닛(113)은 RKn 및 NK'의 값들을 삭제한다. 일단 RKn 및 NK'의 값들이 삭제되면, 네트워크 디바이스(112)는 더 이상 키 반송 디바이스(102)에 등록되지 않으며, 등록 관리 유닛(113)은 (스테이지 I에서 이하에서 설명되는 바와같이) 네트워크 디바이스(112)의 등록해제를 확인하기 위하여 키 관리 유닛(104)에 확인응답을 송신할 수 있다.

[0218] 스테이지 H에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스로부터 수신되는 등록해제 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0219] 스테이지 I에서, 등록해제 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록해제 응답을 송신한다. 예를들어, 등록해제 응답은 등록 관리 유닛(113)이 스테이지 G에서 RKn 및 NK'의 값들을 삭제할 때 확인응답을 포함할 수 있다. 등록해제 응답은 등록 관리 유닛(113)이 스테이지 H에서 에러를 검출할 때 에러를 포함할 수 있다.

[0220] 스테이지 J에서, 등록해제 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 동작들을 중지한다. 일부 구현들에서, 키 관리 유닛(104)은 (스테이지 I에서 수신

되는) 등록해제 응답이 에러를 포함할 때 등록 관리 유닛(113)에 등록해제 요청을 재송신할 수 있다.

[0221] 도 15, 도 16 및 도 17은 제 4 구성 기술을 사용하여 네트워크 디바이스를 등록하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 15, 도 16 및 도 17은 (도 1를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 등록 키(RKk)를 포함하고 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 등록 키(RKn) 및 네트워크 디바이스(112)의 상태(상태)를 포함할 때 제 4 구성 기술을 활용할 수 있다. 제 4 구성 기술에서, 네트워크 디바이스(112)는 네트워크 디바이스(112)의 상태(예를들어, 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지, 다른 키 반송 디바이스에 등록되어 있는지 또는 등록해제되는지의 여부)를 결정하기 위한 동작들을 수행한다. 네트워크 디바이스(112)는 키 반송 디바이스(102)에 (예를들어, Status를 송신함으로써) 자신의 상태를 송신할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 또한 네트워크 키(NK) 및 네트워크 키(NK')를 저장할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 RKk 및 RKn을 암호화하여 보안적으로 교환하기 위하여 해상 알고리즘으로 합의될 수 있다. 해싱 알고리즘은 RKk 및 RKn을 암호화하기 위하여 난수를 활용할 수 있다. 예를들어, 난수는 등록 키와 연접될 수 있으며(예를들어, 난수의 비트들은 연접된 값을 결정하기 위하여 등록 키에 첨부될 수 있으며) 이후 연접된 값의 해싱된 값은 등록 키의 암호화된 값으로서 계산될 수 있다. 난수는 네트워크 디바이스(112)와 키 반송 디바이스(1022)사이에서의 어느 암호화도 없이 교환될 수 있으며, 네트워크 디바이스(112) 및 키 반송 디바이스(102)가 자신들의 등록 키들을 암호화하도록 한다. RKk 및 RKn, 및 Status는 각각 키 반송 디바이스(102)에 등록 키를 저장하고, 네트워크 디바이스(112)에 등록 키를 저장하며 그리고 네트워크 디바이스(112)의 상태를 저장하기 위한 예시적인 변수들을 나타낸다는 것에 유의해야 한다. 유사하게, NK 및 NK'는 각각 키 반송 디바이스(102)에 네트워크 키를 저장하고 네트워크 디바이스(112)에 네트워크 키를 저장하기 위한 예시적인 변수들을 나타낸다. Status는 "등록된" 것으로서 세팅되며 RKk 및 RKn의 값들은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 동일하다는 것에 추가로 유의해야 한다. 또한, NK 및 NK'의 값들은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 의해 관리되는 통신 네트워크(즉, 통신 네트워크(100))로 구성될 때 동일하다. Status는 "등록되지 않은 것"으로서 세팅될 수 있으며, RKn 및 NK'는 네트워크 디바이스(112)가 어느 키 반송 디바이스에도 등록되지 않을 때 널일 수 있다는 것에 또한 유의해야 한다. 일부 구현들에서, RKn 및 NK는 또한 (예를들어, 키 반송 디바이스(102)가 통신 네트워크(100)의 네트워크 키를 가지지 않을 때) 널일 수 있다. 그러나, 키 반송 디바이스(102)는 RKk 및/또는 NK의 값들이 널일 때 RKk 및 NK의 랜덤 값을 생성하는 능력들을 포함한다. 도 15, 도 16 및 도 17은 스테이지들 A1-AI의 시퀀스에서 네트워크 디바이스(112)를 등록하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 15, 도 16 및 도 17가 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0222] 스테이지 A1에서, 임시 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 임시 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 임시 요청은 네트워크 디바이스(113)로부터의 난수에 대한 요청을 포함한다.

[0223] 스테이지 A2에서, 임시 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 임시 응답을 송신한다. 예를들어, 임시 응답은 N1(등록 관리 유닛(113)에 의해 생성되는 난수)를 포함할 수 있다. N1은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 합의되는 해상 알고리즘을 사용하여 등록 키를 암호화하기 위하여 활용될 수 있다.

[0224] 스테이지 B에서, 헬로 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 헬로 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 헬로 요청은 Status에 대한 요청 및 RKk의 암호화된 값을 포함할 수 있다. 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N1(즉, 스테이지 A2에서 수신되는 N1)와 연접되는 RKk의 해싱된 값을 계산함으로써 RKk의 암호화된 값을 계산할 수 있다.

[0225] 스테이지 C에서는 RKn이 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 RKn이 널인지의 여부를 결정한다. 예를들어, 등록 관리 유닛(113)은 스테이지 B에서 수신되는 RKn의 암호화된 값이 널인지의 여부를 검증함으로써 RKn이 널임을 결정할 수 있다. 만일 RKn이 널이면, 등록 관리 유닛(113)은 스테이지 D에서 "등록되지 않은 것"으로서 Status를 세팅할 수 있다. 만일 RKn이 널이 아니면, 등록 관리 유닛(113)은 스테이지 E에서 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정할 수 있다.

[0226] 스테이지 D에서, Status는 "등록되지 않은 것"으로서 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "등록되

지 않은 것"으로서 Status를 세팅하며, 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0227] 스테이지 E에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 B에서 수신되는) RKn의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N1와 연접된 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(120)에 등록되어 있다고 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 G에서 "등록된 것"으로서 Status를 세팅할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 (키 반송 디바이스(102)와 상이한) 다른 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 등록 관리 유닛(113)은 "상이한 KCD에 등록된 것"으로서 Status를 세팅할 수 있다.

[0228] 스테이지 F에서, Status는 "상이한 KCD에 등록된 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "상이한 KCD에 등록된 것"으로 네트워크 디바이스(112)에 저장된 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0229] 스테이지 G에서, Status는 "등록된 것"으로서 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "등록된 것"으로서 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0230] 스테이지 H에서, 헬로 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 헬로 응답을 송신한다. 예를들어, 헬로 응답은 Status, NK'의 암호화된 값 및 난수(N2)를 포함할 수 있다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 NK'의 암호화된 값을 계산할 수 있다. N2는 (스테이지 S에서 이하에서 설명되는 바와같이) 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 합의된 해싱 알고리즘을 사용하여 RKk를 암호화하기 위하여 키 반송 디바이스(102)에 의해 활용될 수 있다.

[0231] 스테이지 I에서는 수신된 Status가 "등록되지 않은 것"인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 H에서 수신되는 Status가 "등록되지 않은 것"인지의 여부를 결정한다. 만일 Status가 "등록되지 않은 것"이면, 제어는 링크 2로 진행하며, 키 관리 유닛(104)은 스테이지 L에서의 동작들을 수행할 수 있다. 만일 Status가 "등록되지 않은 것"이 아니면, 키 관리 유닛(104)은 스테이지 J에서의 동작들을 수행할 수 있다.

[0232] 스테이지 J에서는 Status가 "상이한 KCD에 등록된 것"인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 상태가 "상이한 KCD에 등록된 것"인지의 여부를 결정한다. 만일 Status가 "상이한 KCD에 등록된 것"이면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않음을 결정할 수 있으며, 키 관리 유닛(104)은 스테이지 K에서의 등록 동작들을 중지할 수 있다. 만일 Status가 "상이한 KCD에 등록된 것"이 아니면, 제어는 링크 3으로 진행하며, 키 관리 유닛(104)은 스테이지 AA에서의 동작들을 수행할 수 있다.

[0233] 스테이지 K에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다.

[0234] 스테이지 L에서는 RKk가 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 RKk가 널인지의 여부를 결정한다. 만일 RKk가 널이면, 키 관리 유닛(104)은 스테이지 M에서 랜덤 RKk를 생성한다. 만일 RKk가 널이 아니면, 키 관리 유닛(1044)은 스테이지 N1에서 보안 통신 채널을 설정한다.

[0235] 스테이지 M에서, 랜덤 RKk가 생성된다. 일 구현에서, 키 관리 유닛(104)은 의사 난수 알고리즘을 사용하여 랜덤 RKk를 생성한다. 예를들어, 등록 키가 키 반송 디바이스(102)에 존재하지 않을 때, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스를 등록하기 위하여 네트워크 디바이스에 송신될 수 있는 새로운 랜덤 등록 키를 생성할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 RKk로서 랜덤 RKk를 세이브한다.

[0236] 스테이지 N1에서, 보안 통신 채널은 네트워크 디바이스(112)와 설정된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)과 키 합의, 키 유도 및 키 확인 동작들을 수행함으로써 보안 통신 채널을 설정할 수 있다. 보안 통신 채널은 해싱 알고리즘을 사용하여 RKk를 암호화하지 않고 키 관리 유닛(104)이 (스테이지 N2에서) 등

록 관리 유닛(113)에 RKk를 송신하도록 할 수 있다.

[0237] 스테이지 N2에서, 등록 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 요청을 등록 관리 유닛(113)에 송신한다. 등록 요청은 RKk를 포함할 수 있다.

[0238] 스테이지 O에서, RKk는 네트워크 디바이스(112)에 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 N1에서 키 관리 유닛(104)으로부터 수신되는 RKk를 세이브한다. 예를들어, 등록 관리 유닛(113)은 RKk를 세이브하기 위하여 RKk로서 RKn을 세팅하고 "등록된 것"으로 Status를 세팅할 수 있다. RKk를 세이브할 때, 네트워크 디바이스(112)는 키 반송 디바이스(102)에 등록되며, 등록 관리 유닛(113)은 스테이지 P에서 키 관리 유닛(104)에 확인응답을 송신할 수 있다.

[0239] 스테이지 P에서, 등록 응답이 키 관리 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록 응답을 송신한다. 예를들어, 등록 응답은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록된다는 확인응답을 포함할 수 있다. 일부 구현들에서, 등록 응답은 네트워크 디바이스(112)에 저장되는 Status를 포함할 수 있다.

[0240] 스테이지 Q에서는 NK'의 암호화된 값이 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 H에서 수신되는 NK'의 암호화된 값이 널인지의 여부를 결정한다. 만일 NK'의 암호화된 값이 널이면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 네트워크 키를 가지지 않음을 결정하며, 제어는 링크 3으로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 AA에서의 동작들을 수행할 수 있다. 만일 NK'의 암호화된 값이 널이 아니면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 네트워크 디바이스(112)에 저장되는 네트워크 키를 가짐을 결정하며, 키 관리 유닛(104)은 스테이지 R에서의 동작들을 수행할 수 있다.

[0241] 스테이지 R에서, 네트워크 디바이스(112)의 네트워크 키를 사용해야 하는지가 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)의 네트워크 키를 사용해야 하는지를 결정한다. 예를들어, 키 관리 유닛(104)은 통신 네트워크(100)의 네트워크 키가 키 반송 디바이스(102)에 저장되지 않을 때 네트워크 디바이스(112)에 저장되는 네트워크 키를 사용할 것을 (예를들어, 수신하여 세이브할 것을) 결정할 수 있다. 만일 키 관리 유닛(104)이 네트워크 디바이스(112)의 네트워크 키를 사용하지 않을 것을 결정하면, 제어는 링크 3으로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 AA에서의 동작들을 수행할 수 있다. 만일 키 관리 유닛(104)이 네트워크 디바이스(1120의 네트워크 키를 사용할 것을 결정하면, 키 관리 유닛(104)은 스테이지 S에서의 동작들을 수행할 수 있다.

[0242] 스테이지 S에서, RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N2(즉, 스테이지 H에서 수신되는 N2)와 연접되는 RKk의 해싱된 값을 계산한다.

[0243] 스테이지 T에서, 겟 네트워크 키 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 겟 네트워크 키 요청을 송신한다. 예를들어, 겟 네트워크 키 요청은 (스테이지 S에서 계산되는) RKk의 암호화된 값을 포함한다. 겟 네트워크 키 요청은 네트워크 디바이스(112)에 저장되는 NK'에 대한 요청을 포함할 수 있다.

[0244] 스테이지 U에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 T에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N2와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 겟 네트워크 키 요청이 (악의적인 디바이스가 아니라) 키 반송 디바이스(102)로부터 수신되었음을 검증할 수 있으며, 등록 관리 유닛(113)은 스테이지 W에서 겟 네트워크 키 응답을 송신할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 T에서의 겟 네트워크 키 요청이 악의적인 디바이스에 의해 송신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 V에서 에러를 검출할 수 있다.

[0245] 스테이지 V에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스에 의해 송신되는 겟 네트워크 키 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0246] 스테이지 W에서, 겟 네트워크 키 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 겟 네트워크 키 응답을 송신한다. 예를들어, 겟 네트워크 키 응답은 스테이지 U

에서 RKk의 암호화된 값이 RKn의 암호화된 값과 동일함을 등록 관리 유닛(113)이 결정할 때 NK'를 포함할 수 있다. 겟 네트워크 키 응답은 스테이지 U에서 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않을 때 스테이지 V에서 검출되는 에러를 포함할 수 있다. 일부 구현들에서, 게 네트워크 키 응답은 NK'의 암호화된 값을 포함할 수 있다. 다른 구현들에서, 등록 관리 유닛(113)은 키 관리 유닛(104)과 보안 채널을 설정할 수 있으며, 보안 통신 채널을 통해 겟 네트워크 키 응답을 송신할 수 있다.

[0247] 스테이지 X에서는 겟 네트워크 키 응답이 에러를 포함하는지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 겟 네트워크 키 응답이 에러를 포함하는지의 여부를 결정한다. 예를들어, 스테이지 V에서, 키 관리 유닛(104)은 겟 네트워크 키 응답이 등록 관리 유닛(113)에 의해 검출되는 에러를 포함함을 결정할 수 있다. 만일 겟 네트워크 키 응답이 에러를 포함하면, 키 관리 유닛(104)은 스테이지 Z에서의 등록 동작들을 중지할 수 있다. 만일 겟 네트워크 키 응답이 에러를 포함하지 않으면, 키 관리 유닛(104)은 스테이지 Y에서의 동작들을 수행할 수 있다.

[0248] 스테이지 Y에서, NK'가 세이브된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 W에서 등록 관리 유닛(113)으로부터 등록 응답에서 수신되는 NK'를 세이브한다. 예를들어, 키 관리 유닛(104)은 NK'를 세이브하기 위하여 NK'와 동일하게 NK를 세팅할 수 있다.

[0249] 스테이지 Z에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다.

[0250] 스테이지 AA에서는 NK가 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 NK가 널인지의 여부를 결정한다. 만일 NK가 널이면, 키 관리 유닛(104)은 스테이지 AB에서의 동작들을 수행할 수 있다. 만일 NK가 널이 아니면, 키 관리 유닛(104)은 스테이지 AC에서의 동작들을 수행할 수 있다.

[0251] 스테이지 AB에서는 랜덤 NK가 생성된다. 일 구현에서, 키 관리 유닛(104)은 랜덤 NK를 생성한다. 예를들어, 키 관리 유닛(104)은 의사 난수 알고리즘을 사용하여 랜덤 NK를 생성할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 키 반송 알고리즘(102)에 저장되는 NK로서 랜덤 NK를 세이브한다. 스테이지 AB 이후에, 키 관리 유닛(104)은 스테이지 AC에서의 동작들을 수행할 수 있다.

[0252] 스테이지 AC에서는 RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N2(즉, 스테이지 H에서 수신되는 N2)와 연접되는 RKk의 해싱된 값을 계산할 수 있다.

[0253] 스테이지 AD에서는 세트 네트워크 키 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 세트 네트워크 요청을 송신한다. 예를들어, 세트 네트워크 키 요청은 (스테이지 AC에서 계산되는) RKk의 암호화된 값 및 NK를 포함할 수 있다. 일부 구현들에서, 세트 네트워크 키 요청은 NK 대신에 NK의 암호화된 값을 포함할 수 있다. 다른 구현들에서, 키 관리 유닛(104)은 등록 관리 유닛(113)과 보안 통신 채널을 설정할 수 있으며, 보안 통신 채널을 통해 세트 네트워크 키 요청을 송신할 수 있다.

[0254] 스테이지 AE에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 AD에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N2와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 스테이지 AD에서의 세트 네트워크 키 요청이 (악의적인 디바이스가 아니라) 키 반송 디바이스(102)로부터 수신되었음을 검증할 수 있으며, 등록 관리 유닛(113)은 스테이지 AF에서 NK를 세이브할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 AD에서의 세트 네트워크 키 요청이 악의적인 디바이스에 의해 송신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 AG에서 에러를 검출할 수 있다.

[0255] 스테이지 AF에서는 NK가 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 AD에서 세트 네트워크 키 요청에서 수신되는 NK를 세이브한다. 예를들어, 등록 관리 유닛(113)은 네트워크 디바이스(112)에서 NK를 세이브하기 위하여 NK와 동일하게 NK'를 세팅할 수 있다.

[0256] 스테이지 AG에서, 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스에 의해 송신된 세트 네트워크 키의 결과로서 발생한 에러를 검출할 수 있

다.

[0257] 스테이지 AH에서, 세트 네트워크 키 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 세트 네트워크 키 응답을 송신한다. 예를들어, 세트 네트워크 키 응답은 스테이지 AF에서 등록 관리 유닛(113)이 NK를 세이브할 때 확인응답을 포함할 수 있다. 세트 네트워크 키 응답은 스테이지 AG에서 등록 관리 유닛(113)이 에러를 검출할 때 에러를 포함할 수 있다.

[0258] 스테이지 AI에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다. 예를들어, 키 관리 유닛(104)은 등록 관리 유닛(113)으로부터 세트 네트워크 키 응답을 수신할 때 등록 동작들을 중지할 수 있다. 일부 구현들에서, 세트 네트워크 키 응답이 에러를 포함할 때, 키 관리 유닛(104)은 등록 관리 유닛(113)에 세트 네트워크 키 요청을 재송신하기 위한 하나 이상의 동작들을 수행할 수 있다.

[0259] 도 18 및 도 19는 제 4 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 제 1 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 18 및 도 19는 (도 15, 도 16 및 도 17를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102) 및 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 도 15, 도 16 및 도 17에 설명된 페어링 데이터와 유사할 때 제 4 구성 기술을 활용하여 네트워크 디바이스(112)를 등록해제 하기 위하여 제 1 옵션을 활용할 수 있다. 제 4 구성 기술을 사용하여 네트워크 디바이스(112)를 등록해제할 제 1 옵션에서, 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정한 이후에 등록해제 요청을 송신할 수 있다. 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록된다는 정보를 네트워크 디바이스(112)로부터 수신할 수 있다. 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 단지 네트워크 디바이스(112)를 등록해제할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 Status는 "등록된 것"으로 세팅되고 RKn가 RKk와 동일하다는 것에 유의해야 한다. 도 18 및 도 19는 스테이지들 A1-Q의 시퀀스에서 네트워크 디바이스(112)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 18 및 도 19가 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0260] 스테이지 A1에서, 임시 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 임시 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 임시 요청은 네트워크 디바이스(112)로부터의 난수에 대한 요청을 포함한다.

[0261] 스테이지 A2에서, 임시 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 임시 응답을 송신한다. 예를들어, 임시 응답은 N1(등록 관리 유닛(113)에 의해 생성되는 난수)를 포함할 수 있다. N1은 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 합의되는 해상 알고리즘을 사용하여 등록 키를 암호화하기 위하여 활용될 수 있다.

[0262] 스테이지 B에서, 헬로 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 헬로 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 헬로 요청은 Status에 대한 요청 및 RKk의 암호화된 값을 포함할 수 있다. 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N1(즉, 스테이지 A2에서 수신되는 N1)와 연접되는 RKk의 해싱된 값을 계산함으로써 RKk의 암호화된 값을 계산할 수 있다.

[0263] 스테이지 C에서는 RKn이 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 RKn이 널인지의 여부를 결정한다. 예를들어, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 RKn이 널인지의 여부를 검증함으로써 RKn이 널임을 결정할 수 있다. 만일 RKn이 널이면, 등록 관리 유닛(113)은 스테이지 D에서 "등록되지 않은 것"으로서 Status를 세팅할 수 있다. 만일 RKn이 널이 아니면, 등록 관리 유닛(113)은 스테이지 E에서 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정할 수 있다.

[0264] 스테이지 D에서, Status는 "등록되지 않은 것"으로서 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "등록되지 않은 것"으로서 Status를 세팅하며, 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0265] 스테이지 E에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 B에서 수신되는) RKn의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N1와 연접된 RKn의

해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(120)에 등록되어 있다고 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 G에서 "등록된 것"으로서 Status를 세팅할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 (키 반송 디바이스(102)와 상이한) 다른 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 F에서 "상이한 KCD에 등록된 것"으로서 Status를 세팅할 수 있다.

[0266] 스테이지 F에서, Status는 "상이한 KCD에 등록된 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "상이한 KCD에 등록된 것"으로 네트워크 디바이스(112)에 저장된 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0267] 스테이지 G에서, Status는 "등록된 것"으로서 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "등록된 것"으로서 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0268] 스테이지 H에서, 헬로 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 헬로 응답을 송신한다. 예를들어, 헬로 응답은 Status, NK'의 암호화된 값 및 난수(N2)를 포함할 수 있다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 NK'의 암호화된 값을 계산할 수 있다. N2는 (스테이지 K에서 이하에서 설명되는 바와같이) 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이에서 합의된 해싱 알고리즘을 사용하여 RKk를 암호화하기 위하여 키 반송 디바이스(102)에 의해 활용될 수 있다.

[0269] 스테이지 I에서는 Status가 "등록된 것"인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 H에서 수신되는 Status가 "등록된 것"인지의 여부를 결정한다. 만일 Status가 "등록된 것"이면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정하며, 제어는 링크 5로 진행하며, 여기서 키 관리 유닛(104)은 스테이지 K에서의 동작들을 수행할 수 있다. 만일 Status가 "등록된 것"이 아니면, 키 관리 유닛(104)은 스테이지 J에서의 등록해제 동작들을 중지할 수 있다.

[0270] 스테이지 J에서는 등록해제 동작이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 동작들을 중지한다.

[0271] 스테이지 K에서, RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N2(즉, 스테이지 H에서 수신되는 N2)와 연접되는 RKk의 해싱된 값을 계산한다.

[0272] 스테이지 L에서, 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 송신한다. 예를들어, 등록해제 요청은 (스테이지 K에서 계산되는) RKk의 암호화된 값 및 RKn 및 NK'의 값들을 삭제하기 위한 요청을 포함할 수 있다.

[0273] 스테이지 M에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 L에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N2와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 등록해제 요청이 (악의적인 디바이스가 아니라) 키 반송 디바이스(102)로부터 수신되었음을 검증할 수 있으며, 등록 관리 유닛(113)은 스테이지 N에서 RKn 및 NK'의 값들을 삭제할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 스테이지 L에서의 등록해제 요청이 악의적인 디바이스에 의해 송신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 O에서 에러를 검출할 수 있다.

[0274] 스테이지 N에서는 RKn 및 NK'의 값들이 삭제된다. 일 구현에서, 등록 관리 유닛(113)은 RKn 및 NK'의 값들을 삭제한다. 일단 RKn 및 NK'의 값들이 삭제되면, 네트워크 디바이스(112)는 더이상 키 반송 디바이스(102)에 등록되지 않으며, 등록 관리 유닛(113)은 (스테이지 P에서 이하에서 설명되는 바와같이) 네트워크 디바이스(112)의 등록해제를 확인하기 위하여 키 관리 유닛(104)에 확인응답을 송신할 수 있다.

[0275] 스테이지 O에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스에 의해 송신되는 등록해제 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0276] 스테이지 P에서, 등록해제 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록해제 응답을 송신한다. 예를들어, 등록해제 응답은 등록 관리 유닛(113)이 스테이지 N에서 RKn 및 NK'의 값을 삭제할 때 확인응답을 포함할 수 있다. 등록해제 응답은 등록 관리 유닛(113)이 스테이지 O에서 에러를 삭제할 때 에러를 포함할 수 있다.

[0277] 스테이지 Q에서는 등록해제 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 동작들을 중지한다. 일부 구현들에서, 키 관리 유닛(104)은 (스테이지 P에서 수신되는) 등록해제 응답이 에러를 포함할 때 등록 관리 유닛(113)에 등록해제 요청을 재송신할 수 있다.

[0278] 도 20은 제 4 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 제 2 옵션의 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 20은 (도 15, 도 16 및 도 17를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102) 및 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 도 15, 도 16 및 도 17에 설명된 페어링 데이터와 유사할 때 제 4 구성 기술을 활용하여 네트워크 디바이스(112)를 등록해제 하기 위하여 제 2 옵션을 활용할 수 있다. 제 4 구성 기술을 사용하여 네트워크 디바이스(112)를 등록해제할 제 2 옵션에서, 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정하지 않고 등록해제 요청을 송신할 수 있다. 네트워크 디바이스(112)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정하고 등록해제할 RKn 및 NK'를 삭제하기 위하여 하나 이상의 동작들을 수행할 수 있다. 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 단지 네트워크 디바이스(112)를 등록해제할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 Status는 "등록된 것"으로 세팅되고 RKn가 RKk와 동일하다는 것에 유의해야 한다. 도 20은 스테이지들 A-J의 시퀀스에서 네트워크 디바이스(112)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 20이 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0279] 스테이지 A에서, 임시 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 임시 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 임시 요청은 네트워크 디바이스(112)로부터의 난수에 대한 요청을 포함한다.

[0280] 스테이지 B에서, 난수가 생성된다. 일 구현에서, 등록 관리 유닛(113)은 난수(즉, N1)을 생성한다. 예를들어, 등록 관리 유닛(113)은 N1이 키 반송 디바이스(102)와 네트워크 디바이스(112)사이에서 합의된 해싱 알고리즘을 사용하여 등록 키를 암호화하기 위하여 활용될 수 있도록 N1을 생성할 수 있다.

[0281] 스테이지 C에서, 임시 응답이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 임시 응답을 송신한다. 예를들어, 임시 응답은 (스테이지 B에서 생성되는) N1을 포함할 수 있다.

[0282] 스테이지 D에서, RKk의 암호화된 값이 계산된다. 일 구현에서, 키 관리 유닛(104)은 RKk의 암호화된 값을 계산한다. 예를들어, 키 관리 유닛(104)은 네트워크 디바이스(112)와 합의된 해싱 알고리즘을 사용하여 N1 (즉, 스테이지 C에서 수신되는 N1)와 연접되는 RKk의 해싱된 값을 계산할 수 있다.

[0283] 스테이지 E에서, 등록해제 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 송신한다. 예를들어, 등록해제 요청은 (스테이지 D에서 계산되는) RKk의 암호화된 값 및 RKn 및 NK'를 삭제할 요청을 포함할 수 있다.

[0284] 스테이지 F에서는 RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 (스테이지 E에서 수신되는) RKk의 암호화된 값이 RKn의 암호화된 값과 동일한지의 여부를 결정한다. 등록 관리 유닛(113)은 키 반송 디바이스(102)와 합의된 해싱 알고리즘을 사용하여 N1와 연접되는 RKn의 해싱된 값을 계산함으로써 RKn의 암호화된 값을 계산할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하면, 등록 관리 유닛(113)은 (스테이지 E에서 수신되는) 등록해제 요청이 키 반송 디바이스(102)로부터 수신되었음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 G에서 RKn 및 NK'의 값을 삭제할 수 있다. 만일 RKk의 암호화된 값이 RKn의 암호화된 값과 동일하지 않으면, 등록 관리 유닛(113)은 등록해제 요청이 키 반송 디바이스(102)로부터 수신되지 않았음을(그리고, 대신에 악의적인 디바이스로부터 수신되었음을) 결정할 수 있으며, 등록 관리 유닛(13)은 스테이지 H에서 에러를 검출할 수 있다.

[0285] 스테이지 G에서, RKn 및 NK'의 값들이 삭제된다. 일 구현에서, 등록 관리 유닛(113)은 RKn 및 NK'의 값들을 삭

제한다. 일단 RKn 및 NK'의 값들이 삭제되면, 네트워크 디바이스(112)는 더 이상 키 반송 디바이스(102)에 등록되지 않으며, 등록 관리 유닛(113)은 (스테이지 I에서 이하에서 설명되는 바와같이) 네트워크 디바이스(112)의 등록해제를 확인하기 위하여 키 관리 유닛(104)에 확인응답을 송신할 수 있다.

[0286] 스테이지 H에서는 에러가 검출된다. 일 구현에서, 등록 관리 유닛(113)은 에러를 검출한다. 예를들어, 등록 관리 유닛(113)은 악의적인 디바이스로부터 수신되는 등록해제 요청의 결과로서 발생한 에러를 검출할 수 있다.

[0287] 스테이지 I에서, 등록해제 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록해제 응답을 송신한다. 예를들어, 등록해제 응답은 등록 관리 유닛(113)이 스테이지 G에서 RKn 및 NK'의 값들을 삭제할 때 확인응답을 포함할 수 있다. 등록해제 응답은 등록 관리 유닛(113)이 스테이지 H에서 에러를 검출할 때 에러를 포함할 수 있다.

[0288] 스테이지 J에서, 등록해제 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 동작들을 중지한다. 일부 구현들에서, 키 관리 유닛(104)은 (스테이지 I에서 수신되는) 등록해제 응답이 에러를 포함할 때 등록 관리 유닛(113)에 등록해제 요청을 재송신할 수 있다.

[0289] 도 21 및 도 22는 제 5 구성 기술을 사용하여 네트워크 디바이스를 등록하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 21 및 도 22는 (도 1를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102)상에 저장되는 페어링 데이터가 등록 키(RKk)를 포함하고 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 등록 키(RKn) 및 네트워크 디바이스(112)의 상태(Stutus)를 포함할 때 제 5 구성 기술을 활용할 수 있다. 제 5 구성 기술에서, 키 반송 디바이스(102)는 키 반송 디바이스(102)가 네트워크 디바이스(112)를 구성하는 동작들을 시작하기 전에 네트워크 디바이스(112)와 보안 통신 채널을 설정한다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 페어링 데이터에 대해 암호화 동작들을 수행하지 않고 보안 통신 채널을 통해 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 저장되는 페어링 데이터를 포함하는 모든 메시지들을 교환할 수 있다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 또한 네트워크 키(NK) 및 네트워크 키(NK')를 저장할 수 있다. RKk 및 RKn 및 Status는 각각 키 반송 디바이스(102)의 등록 키, 네트워크 디바이스(112)의 등록 키 및 네트워크 디바이스(112)의 상태를 저장하기 위한 예시적인 변수들을 각각 나타낸다는 것에 유의해야 한다. 유사하게, NK 및 NK'는 각각 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 네트워크 키들을 저장하기 위한 예시적인 변수들을 나타낸다. Status는 등록 요청이 키 반송 디바이스(102)로부터 수신되고 네트워크 디바이스(112)가 키 반송 디바이스(102)에 사전에 등록될 때 네트워크 키(예를들어, 통신 네트워크(100)의 네트워크 키)가 네트워크 디바이스(112)에 저장되는지의 여부를 표시하도록 세팅될 수 있다는 것에 추가로 유의해야 한다. RKk 및 RKn의 값들은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 동일하다. 또한, NK 및 NK'의 값들은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 의해 관리되는 통신 네트워크(즉, 통신 네트워크(100))로 구성될 때 동일하다. Status는 "등록되지 않은 것"으로 세팅될 수 있고 RKn 및 NK'는 네트워크 디바이스(112)가 어느 키 반송 디바이스에도 등록되지 않을 때 널일 수 있다는 것에 또한 유의해야 한다. 일부 구현들에서, RKk 및 NK는 또한 (예를들어, 키 반송 디바이스(102)가 통신 네트워크(100)의 네트워크 키를 가지지 않을 때) 널일 수 있다. 그러나, 키 반송 디바이스(102)는 RKk 및/또는 NK의 값들이 널일때 RKk 및 NK의 랜덤값을 생성하는 능력들을 포함한다. 도 21 및 도 22는 스테이지들 A-X의 시퀀스에서 네트워크 디바이스(112)를 등록하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 21 및 도 22가 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0290] 스테이지 A에서, 네트워크 디바이스(112)와 보안 통신 채널이 설정된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)과 키 합의, 키 유도 및 키 확인 동작들을 수행함으로써 보안 통신 채널을 설정할 수 있다. 보안 통신 채널은 페어링 데이터에 대해 암호화 동작들을 수행하지 않고 키 관리 유닛(104) 및 등록 관리 유닛(113)이 페어링 데이터(예를들어, RKk, NK, NK', 및 Status 등)를 교환하도록 할 수 있다. 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이의 보안 통신 채널은 등록 동작들이 완료될 때까지 계속 존재할 수 있다.

[0291] 스테이지 B에서, 등록 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 등록 요청은 RKk 및 네트워크 디바이스(112)에 RKk를 세이브할 요청을 포함할 수 있다.

[0292] 스테이지 C1에서는 RKn이 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 RKn이 널인지의 여부를 결정한다. 만일 RKn이 널이면, 등록 관리 유닛(113)은 스테이지 C2에

서 RKk를 세이브할 수 있다. 만일 RKn이 널이 아니면, 등록 관리 유닛(113)은 스테이지 D에서 RKn이 RKk와 동일한지의 여부를 결정할 수 있다.

[0293] 스테이지 C2에서, RKk가 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 스테이지 B에서 수신되는 RKk를 세이브한다. 예를들어, 등록 관리 유닛(113)은 RKk를 세이브하기 위하여 RKk와 동일하게 RKn을 세팅할 수 있다. 일단 등록 관리 유닛(113)이 RKk를 세이브하면, 네트워크 디바이스(112)는 키 반송 디바이스(102)에 등록된다. 스테이지 C2 이후에, 등록 관리 유닛(113)은 스테이지 F에서 NK'가 널인지의 여부를 결정할 수 있다.

[0294] 스테이지 D에서는 RKn이 RKk와 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 RKn이 (스테이지 B에서 수신되는) RKk와 동일한지의 여부를 결정한다. 만일 RKn이 RKk와 동일하면, 등록 관리 유닛(113)은 스테이지 F에서 NK'가 널인지의 여부를 결정할 수 있다. 만일 RKn이 RKn와 동일하지 않으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)와 다른 키 반송 디바이스에 등록되고 스테이지 E에서 동작들을 수행함을 결정할 수 있다.

[0295] 스테이지 E에서, Status는 "상이한 KCD에 등록된 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "상이한 KCD에 등록된 것"으로 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 I에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0296] 스테이지 F에서는 NK'이 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 NK'가 널인지의 여부를 결정한다. 만일 NK'가 널이면, 등록 관리 유닛(113)은 네트워크 키가 네트워크 디바이스(112)에 저장되지 않음을 결정하고 스테이지 H에서의 동작들을 수행할 수 있다. 만일 NK'가 널이 아니면, 등록 관리 유닛(113)은 네트워크 키가 네트워크 디바이스(112)에 저장됨을 결정하고 스테이지 G에서의 동작들을 수행할 수 있다.

[0297] 스테이지 G에서는 Status가 "NK를 가지는 것"으로서 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "NK를 가지는 것"으로서 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 I에서 등록 응답으로 Status를 송신할 수 있다.

[0298] 스테이지 H에서는 "NK를 가지지 않은 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "NK를 가지지 않은 것"으로서 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 I에서 등록 응답으로 Status를 송신할 수 있다.

[0299] 스테이지 I에서, 등록 응답이 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록 응답을 송신한다. 예를들어, 등록 응답은 네트워크 디바이스(112)에 저장되는 Status를 포함할 수 있다.

[0300] 스테이지 J에서는 Status가 "상이한 KCD에 등록된 것"인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 I에서 수신되는) 상태가 "상이한 KCD에 등록된 것"인지의 여부를 결정한다. 만일 Status가 "상이한 KCD에 등록된 것"이면, 키 관리 유닛(104)은 네트워크 디바이스(112)가 (키 반송 디바이스(102)와 상이한) 다른 키 반송 디바이스에 등록되어 있다고 결정할 수 있으며, 키 관리 유닛(104)은 스테이지 K에서의 등록 동작들을 중지할 수 있다. 만일 Status가 "상이한 KCD에 등록된 것"이 아니면, 제어는 링크 6으로 진행하며, 키 관리 유닛(113)은 스테이지 L에서의 동작들을 수행할 수 있다.

[0301] 스테이지 K에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다.

[0302] 스테이지 L에서는 Status가 "NK를 가지는 것"인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 I에서 수신되는) Status가 "NK를 가지는 것"인지의 여부를 결정한다. 만일 Status가 "NK를 가지는 것"이면, 키 관리 유닛(104)은 네트워크 키가 네트워크 디바이스(112)에 저장됨을 결정할 수 있고, 키 관리 유닛(104)은 스테이지 M에서의 동작들을 수행할 수 있다. 만일 Status가 "NK를 가지는 것"이 아니면, 키 관리 유닛(104)은 네트워크 키가 네트워크 디바이스(112)에 저장되지 않음을 결정할 수 있고, 키 관리 유닛(104)은 스테이지 R에서의 동작들을 수행할 수 있다.

[0303] 스테이지 M에서는 네트워크 디바이스(112)의 네트워크 키를 사용해야 하는지가 결정된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)의 네트워크 키를 사용해야 하는지를 결정한다. 예를들어, 키 관리 유닛(104)은 통신 네트워크(100)의 네트워크 키가 키 반송 디바이스(102)에 저장되지 않을 때 네트워크 디바이스(112)에 저장되는 네트워크 키를 사용할 것을 (예를들어, 수신하여 세이브할 것을) 결정할 수 있다. 만일 키

관리 유닛(104)이 네트워크 디바이스(112)의 네트워크 키를 사용할 것을 결정하면, 키 관리 유닛(104)은 스테이지 N에서 겟 네트워크 키 요청을 송신할 수 있다. 만일 키 관리 유닛(104)이 네트워크 디바이스(1120의 네트워크 키를 사용하지 않을 것을 결정하면, 키 관리 유닛(104)은 스테이지 R에서의 동작들을 수행할 수 있다.

[0304] 스테이지 N에서, 겟 네트워크 키 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)에 겟 네트워크 키 요청을 송신한다. 예를들어, 겟 네트워크 키 요청은 NK'에 대한 요청을 포함한다.

[0305] 스테이지 O에서, 겟 네트워크 키 응답은 네트워크 디바이스(112)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 겟 네트워크 키 응답을 송신한다. 예를들어, 겟 네트워크 키 응답은 네트워크 디바이스(112)에 저장된다. 등록 관리 유닛(113)은 겟 네트워크 키 응답을 송신하기 전에 겟 네트워크 키 요청이 키 반송 디바이스(102)로부터 수신됨을 결정하기 위한 동작들을 수행하지 않을 수 있는데, 왜냐하면 제 5 구성 기술에서 보안 통신 채널이 악의적인 디바이스들로부터 발신되는 임의의 메시지들로부터의 보호를 보장하기 때문이다.

[0306] 스테이지 P에서, NK'가 세이브된다. 일 구현에서, 키 관리 유닛(104)은 스테이지 O에서 수신되는 NK'를 세이브한다. 예를들어, 키 관리 유닛(104)은 NK'를 세이브하기 위하여 NK'와 동일하게 NK를 세팅할 수 있다. NK'를 세이브한 이후에, 키 관리 유닛(104)은 스테이지 Q에서의 등록 요청들을 중지할 수 있다.

[0307] 스테이지 Q에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다.

[0308] 스테이지 R에서는 NK가 널인지의 여부가 결정된다. 일 구현에서, 키 관리 유닛(104)은 키 반송 디바이스(102)에 저장되는 NK가 널인지의 여부를 결정한다. 만일 NK가 널이면, 키 관리 유닛(104)은 스테이지 S에서 랜덤 NK를 생성할 수 있다. 만일 NK가 널이 아니면, 키 관리 유닛(104)은 스테이지 T에서의 동작들을 수행할 수 있다.

[0309] 스테이지 S에서는 랜덤 NK가 생성된다. 일 구현에서, 키 관리 유닛(104)은 랜덤 NK를 생성한다. 예를들어, 키 관리 유닛(104)은 의사 난수 알고리즘을 사용하여 랜덤 NK를 생성할 수 있다. 일부 구현들에서, 키 관리 유닛(104)은 키 반송 알고리즘(102)에 저장되는 NK로서 랜덤 NK를 세이브한다. 스테이지 S 이후에, 키 관리 유닛(104)은 스테이지 T에서의 동작들을 수행할 수 있다.

[0310] 스테이지 T에서는 세트 네트워크 키 요청이 송신된다. 일 구현에서, 키 관리 유닛(104)은 세트 네트워크 요청을 생성한다. 예를들어, 세트 네트워크 키 요청은 키 반송 디바이스(102)에 저장되는 NK를 포함할 수 있다.

[0311] 스테이지 U에서, 세트 네트워크 키 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 (스테이지 T에서 생성되는) 세트 네트워크 키 요청을 등록 관리 유닛(113)에 송신한다.

[0312] 스테이지 V에서는 NK가 세이브된다. 일 구현에서, 등록 관리 유닛(113)은 세트 네트워크 키 요청에서 수신되는 NK를 세이브한다. 예를들어, 등록 관리 유닛(113)은 NK를 세이브하기 위하여 NK와 동일하게 NK'를 세팅할 수 있다. NK를 세이브한 이후에, 등록 관리 유닛(113)은 NK가 네트워크 디바이스(1120에 세이브된다는 확인응답을 키 관리 유닛(113)에 송신할 수 있다. 등록 관리 유닛(113)은 NK를 세이브하기 전에 키 반송 디바이스(102)로부터 수신되었음을 결정하기 위한 동작들을 수행하지 않을 수 있다는 것에 유의해야 한다는데, 왜냐하면 제 5 구성 기술에서 보안 통신 채널이 악의적인 디바이스들로부터 발신되는 임의의 메시지들로부터의 보호를 보장하기 때문이다.

[0313] 스테이지 W에서, 세트 네트워크 키 응답은 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 세트 네트워크 키 응답을 송신한다. 예를들어, 세트 네트워크 키 응답은 NK가 네트워크 디바이스(112)에 세이브되었다는 확인응답을 포함한다. 일부 구현들에서, 세트 네트워크 키 응답은 NK가 네트워크 디바이스(112)에 성공적으로 세이브되지 않을 때 에러를 포함하지 않을 수 있다.

[0314] 스테이지 X에서, 등록 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록하기 위한 등록 동작들을 중지한다. 일부 구현들에서, (스테이지 W에서 수신되는) 세트 네트워크 키 응답에서 에러를 수신할 때, 키 관리 유닛(104)은 등록 관리 유닛(113)에 NK를 재송신할 수 있다.

[0315] 도 23은 제 5 구성 기술을 사용하여 네트워크 디바이스를 등록해제하기 위한 예시적인 동작들의 시퀀스 다이어그램을 예시한다. 도 23는 (도 21 및 도 22를 참조로 하여 앞서 설명된 바와같이) 키 반송 디바이스(102) 및 네트워크 디바이스(112)를 포함한다. 키 반송 디바이스(102)는 키 반송 디바이스(102) 및 네트워크 디바이스(112)상에 저장되는 페어링 데이터가 도 21 및 도 22에 설명된 페어링 데이터와 유사할 때 제 5 구성 기술을 사

용하여 네트워크 디바이스(112)를 등록해제할 수 있다. 제 5 구성 기술에서, 키 반송 디바이스(102)는 키 반송 디바이스(102)가 네트워크 디바이스(112)를 구성하는 동작들을 시작하기 전에 네트워크 디바이스(112)와 보안 통신 채널을 설정한다. 키 반송 디바이스(102) 및 네트워크 디바이스(112)는 페어링 데이터에 대해 암호화 동작들을 수행하지 않고 보안 통신 채널을 통해 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 저장되는 페어링 데이터를 포함하는 모든 메시지들을 교환할 수 있다. 네트워크 디바이스(112)는 네트워크 디바이스(112)가 키 반송 디바이스(102)로부터 등록해제 요청을 수신할 때 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있으며, 등록해제할 RKn 및 NK'를 삭제하기 위한 하나 이상의 동작들을 수행할 수 있다. 키 반송 디바이스(102)는 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 단지 네트워크 디바이스(112)를 등록해제할 수 있다. 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록될 때 RKn이 RKk와 동일하다는 것에 유의해야 한다. 도 23은 스테이지들 A-I의 시퀀스에서 네트워크 디바이스(112)를 등록해제하기 위하여 키 반송 디바이스(102)와 네트워크 디바이스(112) 간의 상호작용들을 예시한다. 비록 도 23이 키 관리 유닛(104) 및 등록 관리 유닛(113)에 의해 수행되는 동작들을 예시할지라도, 일부 구현들에서, 동작들은 키 반송 디바이스(102) 및 네트워크 디바이스(112)의 다른 유닛들에 의해 각각 수행될 수 있다.

[0316] 스테이지 A에서, 네트워크 디바이스(112)와 보안 통신 채널이 설정된다. 일 구현에서, 키 관리 유닛(104)은 등록 관리 유닛(113)과 키 합의, 키 유도 및 키 확인 동작들을 수행함으로써 보안 통신 채널을 설정할 수 있다. 보안 통신 채널은 페어링 데이터에 대해 암호화 동작들을 수행하지 않고 키 관리 유닛(104) 및 등록 관리 유닛(113)이 페어링 데이터(예를들어, RKk, Status 등)를 교환하도록 할 수 있다. 키 반송 디바이스(102)와 네트워크 디바이스(112) 사이의 보안 통신 채널은 등록 동작들이 완료될 때까지 계속 존재할 수 있다.

[0317] 스테이지 B에서, 등록 요청이 네트워크 디바이스(112)에 송신된다. 일 구현에서, 키 관리 유닛(104)은 등록 요청을 등록 관리 유닛(113)에 송신한다. 예를들어, 등록 요청은 RKk 및 네트워크 디바이스(112)에 저장되는 RKn 및 RK'를 삭제할 요청을 포함할 수 있다.

[0318] 스테이지 C에서는 RKn이 널인지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 RKn이 널인지의 여부를 결정한다. 만일 RKn이 널이면, 등록 관리 유닛(113)은 스테이지 D에서의 동작들을 수행할 수 있다. 만일 RKn이 널이 아니면, 등록 관리 유닛(113)은 스테이지 E에서 RKn이 RKk와 동일한지의 여부를 결정할 수 있다.

[0319] 스테이지 D에서, Status가 "등록되지 않은 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "등록되지 않은 것"으로 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0320] 스테이지 E에서는 RKn이 RKk와 동일한지의 여부가 결정된다. 일 구현에서, 등록 관리 유닛(113)은 RKn이 (스테이지 B에서 수신되는) RKk와 동일한지의 여부를 결정한다. 만일 RKn이 RKk와 동일하면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정할 수 있고, 등록 관리 유닛(113)은 스테이지 G에서의 동작들을 수행할 수 있다. 만일 RKn이 RKn와 동일하지 않으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않음을 결정할 수 있으며, 등록 관리 유닛(113)은 스테이지 F에서의 동작들을 수행할 수 있다. 일부 구현들에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 (스테이지 A에서 설정되는 보안 채널에 대응하는) 보안 채널 키들과 등록 요청을 포함하는 메시지에 포함되는 하나 이상의 보안 채널 키들을 비교함으로써 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있는지의 여부를 결정할 수 있다. 만일 메시지에 포함되는 보안 채널 키들이 네트워크 디바이스(112)에 저장되는 보안 채널 키들과 매칭되면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되어 있다고 결정할 수 있다. 만일 메시지에 포함되는 보안 채널 키들이 네트워크 디바이스(112)에 저장되는 보안 채널 키들과 매칭되지 않으면, 등록 관리 유닛(113)은 네트워크 디바이스(112)가 키 반송 디바이스(102)에 등록되지 않음을 결정할 수 있다.

[0321] 스테이지 F에서, Status는 "상이한 KCD에 등록된 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 "상이한 KCD에 등록된 것"으로 Status를 세팅한다. 등록 관리 유닛(113)은 스테이지 H에서 키 관리 유닛(104)에 Status를 송신할 수 있다.

[0322] 스테이지 G에서, RKn 및 NK'는 삭제되고 Status는 "등록되지 않은 것"으로 세팅된다. 일 구현에서, 등록 관리 유닛(113)은 네트워크 디바이스(112)에 저장되는 RKn 및 NK'의 값들을 삭제하고 "등록되지 않은 것"으로 Status를 세팅한다. 등록 관리 유닛(113)은 RKn 및 NK'의 값들을 삭제하기 전에 등록 요청이 키 반송 디바이스(102)로부터 수신되지 않았음을 결정하기 위한 동작들을 수행하지 않을 수 있다는 것에 유의해야 하는데, 왜냐하면

제 5 구성 기술에서 보안 통신 채널은 악의적인 디바이스들로부터 발신되는 임의의 메시지들로부터의 보호를 보장하기 때문이다.

[0323] 스테이지 H에서, 등록해제 응답이 키 반송 디바이스(102)에 송신된다. 일 구현에서, 등록 관리 유닛(113)은 키 관리 유닛(104)에 등록해제 응답을 송신한다. 예를들어, 등록해제 응답은 네트워크 디바이스(112)가 등록되지 않거나 또는 네트워크 디바이스(112)가 (키 반송 디바이스(102)와 상이한) 다른 키 반송 디바이스에 등록되어 있다고 키 관리 유닛(104)에 표시하기 위하여 Status를 포함할 수 있다. 일부 구현들에서, 등록해제 응답은 또한 하나 이상의 등록해제 동작들이 네트워크 디바이스(112)에서 성공적이지 않을 때 에러를 포함할 수 있다.

[0324] 스테이지 I에서, 등록해제 동작들이 중지된다. 일 구현에서, 키 관리 유닛(104)은 네트워크 디바이스(112)를 등록해제하기 위한 등록해제 동작들을 중지한다. 일부 구현들에서, 키 관리 유닛(104)이 스테이지 H에서 등록해제 응답에서 에러를 수신할 때 키 관리 유닛(104)은 등록 관리 유닛(113)에 등록해제 요청을 재송신할 수 있다.

[0325] 도 5-23에서 설명되는 구성 기술들이 본래 예시적이며 간략화를 위하여 도 5-23이 반드시 키 반송 디바이스(102) 및 네트워크 디바이스(112)에 의해 수행되는 모든 동작들을 예시하지는 않는다는 것에 유의해야 한다. 예를들어, 제 1 구성 기술(도 5 및 도 6에서 앞서 설명됨) 및 제 2 구성 기술(도 7 및 도 8에서 앞서 설명됨)은 네트워크 키를 수신하고 네트워크 키가 키 반송 디바이스(102)에서 저장되지 않을 때 랜덤 네트워크 키를 생성하는 동작들을 포함하지 않는다. 그러나, 키 반송 디바이스(102)는 네트워크 키가 키 반송 디바이스(102)에 저장되지 않을 때 이러한 동작들을 수행하는 능력을 포함한다. 도 5-23에 설명된 동작들이 상이한 순서로 수행될 수 있고, 키 반송 디바이스(102) 및 네트워크 디바이스(112)에서 병렬로 수행될 수 있는 식이라는 것에 또한 유의해야 한다. 또한, 키 반송 디바이스(102)는 네트워크 디바이스를 구성하기 위하여 한번에 하나의 구성 기술을 활용하는 것에 제한되지 않는다. 일부 실시예들에서, 키 반송 디바이스(102)는 동일하거나 또는 상이한 통신 네트워크들에서 네트워크 디바이스들을 구성하기 위하여 2개 이상의 구성 기술들을 활용할 수 있다.

[0326] 도 1-23이 실시예들을 이해하는데 도움을 주는 것으로 의도된 예들이며 실시예들을 제한하거나 또는 청구범위를 제한하는 것으로 사용되지 않아야 한다는 것이 이해되어야 한다. 실시예들은 추가의 동작들을 수행할 수 있고, 더 적은 동작을을 수행할 수 있고, 상이한 순서로 동작들을 수행할 수 있고, 병렬로 동작들을 수행할 수 있고 그리고 일부 동작들을 상이하게 수행할 수 있다. 예를들어, 도 2-4 및/또는 도 5-23이 도 2-4에 설명된 절차들을 구현하기 위하여 상이한 결정 단계들로 수정되거나 또는 교체될 수 있다. 도 13 및 도 14는 네트워크 디바이스(112)를 등록해제하기 위한 제 3 구성 기술의 대안 구현들을 예시한다. 유사하게, 도 18, 도 19 및 도 20은 네트워크 디바이스(112)를 등록해제하기 위한 제 4 구성 기술의 대안 구현들을 예시한다. 제 2, 도 3, 도 4 및 도 5 구성 기술들이 NFC-SEC-01에 따를 수 있다는 것에 유의해야 한다. 또한, 제 2, 제 3, 제 4 및 도 5 구성 기술들에서, 페어링 데이터는 키 반송 디바이스(102)와 재동기할 필요성 없이 통신 네트워크(100)에서 네트워크 디바이스들을 구성하기 위하여 다수의 키 반송 디바이스들을 활용하는 것을 가능하게 하는 키 반송 디바이스(102)에 저장되지 않는다.

[0327] 당업자에 의해 인식되는 바와같이, 본 발명의 요지의 양상들은 시스템, 방법 또는 컴퓨터 프로그램 물건으로서 구현될 수 있다. 따라서, 본 발명의 요지의 양상들은 전체적으로 하드웨어 실시예, 소프트웨어 실시예(펌웨어, 상주 소프트웨어, 마이크로 코드 등을 포함함) 또는 일반적으로 모두 "회로", "모듈" 또는 "시스템"으로서 지칭될 수 있는 소프트웨어 및 하드웨어 양상들을 포함하는 실시예의 형태를 취할 수 있다. 게다가, 본 발명의 요지의 양상들은 컴퓨터 판독가능 프로그램 코드가 통합되는 하나 이상의 컴퓨터 판독가능 매체(들)로 구현되는 컴퓨터 프로그램 물건의 형태를 취할 수 있다.

[0328] 하나 이상의 컴퓨터 판독가능 매체(들)의 임의의 실시예들이 활용될 수 있다. 컴퓨터 판독가능 매체는 컴퓨터 판독가능 신호 매체 또는 컴퓨터 판독가능 저장 매체일 수 있다. 컴퓨터 판독가능 저장 매체는 예를들어 전자, 자기, 광학, 전자기, 적외선 또는 반도체 시스템, 장치 또는 디바이스 또는 이들의 임의의 적절한 조합일 수 있으나, 이들로 제한되지 않는다. 컴퓨터 판독가능 저장 매체의 더 특정한 예들(비-배타적인 리스트)은 이하의 것들, 즉 하나 이상의 와이어들을 가진 전기 연결부, 휴대용 컴퓨터 디스켓, 하드 디스크, 랜덤 액세스 메모리(RAM), 판독-전용 메모리(ROM), 소거가능 프로그램 가능 판독 전용 메모리(EPROM 또는 플래시 메모리), 광섬유, 휴대용 컴팩트 디스크 판독-전용 메모리(CD-ROM), 광학 저장 디바이스, 자기 저장 디바이스 또는 이들의 임의의 적절한 조합을 포함할 것이다. 이러한 문헌의 맥락에서, 컴퓨터 판독가능 저장 매체는 명령 실행 시스템, 장치 또는 디바이스에 의해 사용하거나 또는 이와 관련하여 사용하기 위한 프로그램을 포함하거나 또는 저장할 수 있는 임의의 탠저블 매체일 수 있다.

[0329] 컴퓨터 판독가능 신호 매체는 컴퓨터 판독가능 프로그램 코드가 내부에, 예를들어 기저대역에 또는 캐리어 파의 부분으로서 통합되는 전파 데이터 신호를 포함할 수 있다. 이러한 전파 신호는 전자기, 광학 또는 이들의 임의의 적절한 조합을 포함하는 (그러나, 이들에 제한되지 않음) 다양한 형태들 중 임의의 형태를 취할 수 있다. 컴퓨터 판독가능 신호 매체는 컴퓨터 판독가능 저장 매체가 아니고 명령 실행 시스템, 장치 또는 디바이스에 의해 사용하거나 또는 이와 관련하여 사용하기 위한 프로그램을 통신하거나 또는 전파하거나 또는 이송할 수 있는 임의의 컴퓨터 판독가능 매체일 수 있다.

[0330] 컴퓨터 판독가능 매체상에 통합되는 프로그램 코드는 무선, 유선, 광섬유 케이블, RF 등 또는 이들의 임의의 적절한 조합을 포함하는 (그러나, 이들에 제한되지 않음) 임의의 적절한 매체를 사용하여 전송될 수 있다.

[0331] 본 발명의 요지의 양상들에 대한 동작들을 수행하기 위한 컴퓨터 프로그램 코드는 Java, Smalltalk, C++ 등과 같은 객체 지향 프로그래밍 언어 및 "C" 프로그래밍 언어 또는 유사한 프로그래밍 언어들과 같은 종래의 절차적 프로그래밍 언어들로 기록될 수 있다. 프로그램 코드는 사용자 컴퓨터상에서 전체적으로 실행되며, 스탠드-얼론 소프트웨어 패키지로서 사용자의 컴퓨터상에서 부분적으로 실행되며, 사용자의 컴퓨터상에서 부분적으로 실행되며, 그리고 원격 컴퓨터상에서 부분적으로 또는 원격 컴퓨터 또는 서버상에서 전체적으로 실행될 수 있다. 후자의 시나리오에서, 원격 컴퓨터는 근거리 통신망(LAN) 또는 광역 통신망(WAN)을 포함하는 임의의 타입의 네트워크를 통해 사용자 컴퓨터에 연결될 수 있거나 또는 (예를들어, 인터넷 서비스 제공자를 사용하여 인터넷을 통해) 외부 컴퓨터에 대해 연결이 이루어질 수 있다.

[0332] 본 발명의 요지의 양상들은 본 발명의 요지의 실시예들에 따라 방법들, 장치(시스템들) 및 컴퓨터 프로그램 물건들의 흐름도 예시들 및/또는 블록도들과 관련하여 설명된다. 흐름도 예시들 및/또는 블록도들의 각 블록 및/또는 흐름도 예시들 및/또는 블록도들의 블록들의 조합이 컴퓨터 프로그램 명령들에 의해 구현될 수 있다는 것이 이해될 것이다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 또는 다른 프로그램가능 데이터 프로세싱 장치의 프로세서를 통해 실행하는 명령들과 같은 머신을 산출하고 흐름도 및/또는 블록도 블록 또는 블록들에 특정된 기능들/동작들을 구현하기 위한 수단을 생산하기 위하여 범용 컴퓨터, 특수목적 컴퓨터 또는 다른 프로그램가능 데이터 프로세싱 장치의 프로세서에 제공될 수 있다.

[0333] 이들 컴퓨터 프로그램 명령들은 또한 컴퓨터, 다른 프로그램가능 데이터 프로세싱 장치 또는 다른 디바이스들이 특정 방식으로 기능을 하도록 할 수 있는 컴퓨터 판독가능 매체에 저장될 수 있으며, 따라서 컴퓨터 판독가능 매체에 저장된 명령들은 흐름도 및/또는 블록도 블록 또는 블록들에 특정된 기능/동작을 구현하는 명령들을 포함하는 제조물품을 생산한다.

[0334] 컴퓨터 프로그램 명령들은 또한 컴퓨터 구현 프로세스를 생산하기 위하여 일련의 동작 단계들이 컴퓨터, 다른 프로그램가능 장치 또는 다른 디바이스들상에서 실행되는 것을 야기하는 컴퓨터, 다른 프로그램가능 데이터 프로세싱 장치 또는 다른 디바이스들상에 로드될 수 있으며, 따라서 컴퓨터 또는 다른 프로그램가능 장치상에서 실행되는 명령들은 흐름도 및/또는 블록도 블록 또는 블록들에 특정된 기능들/동작들을 구현하기 위한 프로세스들을 제공한다.

[0335] 도 24는 예시적인 네트워크 디바이스(2400)를 도시한다. 일부 구현들에서, 네트워크 디바이스(2400)는 단거리 통신(예를들어, NFC, Bluetooth, ZigBee 등)을 지원하는 통신 디바이스일 수 있다. 네트워크 디바이스(2400)는 (가능한 경우에, 다수의 프로세서들, 다수의 코어들, 다수의 노드들을 포함하고 그리고/또는 멀티-스레딩 등을 구현하는) 프로세서 유닛(2401)을 포함한다. 네트워크 디바이스(2400)는 메모리(2403)를 포함한다. 메모리(2403)는 시스템 메모리(예를들어, 캐시, SRAM, DRAM, 제로 커패시터 RAM, 트윈 트랜지스터 RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM 등) 또는 머신-판독가능 매체의 앞서 이미 설명된 가능한 실현물들 중 임의의 하나 이상일 수 있다. 네트워크 디바이스(2400)는 또한 버스(2411)(PCI, PCI-Express, AHB™, AXI™, AXI™, NoC 등), 저장 디바이스(들)(2405)(예를들어, SD 카드, SIM 카드, 광학 스토리지, 자기 스토리지 등), 통신 유닛(2405)(예를들어, GSM 유닛, CDMA 유닛, FM 유닛, Wi-Fi 유닛 등), I/O 디바이스들(2407)(예를들어, 터치스크린, 카메라, 마이크로폰, 스피커 등) 및 네트워크 인터페이스(2420)(예를들어, Bluetooth 인터페이스, NFC 인터페이스, Wi-Fi 인터페이스, 전력선 인터페이스, 이더넷 인터페이스, 프레임 중계 인터페이스, SONET 인터페이스 등)를 포함한다. 통신 유닛(2405)은 단거리 통신 유닛(2413) 및 관리 유닛(2415)을 포함한다. 단거리 통신 유닛(2413)은 하나 이상의 단거리 통신 기술(예를들어, NFC, ZigBee, Bluetooth 등)을 구현할 컴포넌트들을 포함한다. 관리 유닛(2415)은 도 1-23에 앞서 설명된 실시예들의 일부를 구현하는 기능을 구현한다. 관리 유닛(1415)은 도 1-23에서 앞서 설명된 실시예들 중 일부를 구현하는 기능을 구현한다. 관리 유닛(2415)은 도 5-23에서 앞서 설명된 적어도 5개의 구성 기술들을 사용하여 네트워크 디바이

스들을 보안적으로 구성하는 것을 가능하게 하는 하나 이상의 기능들을 포함할 수 있다.

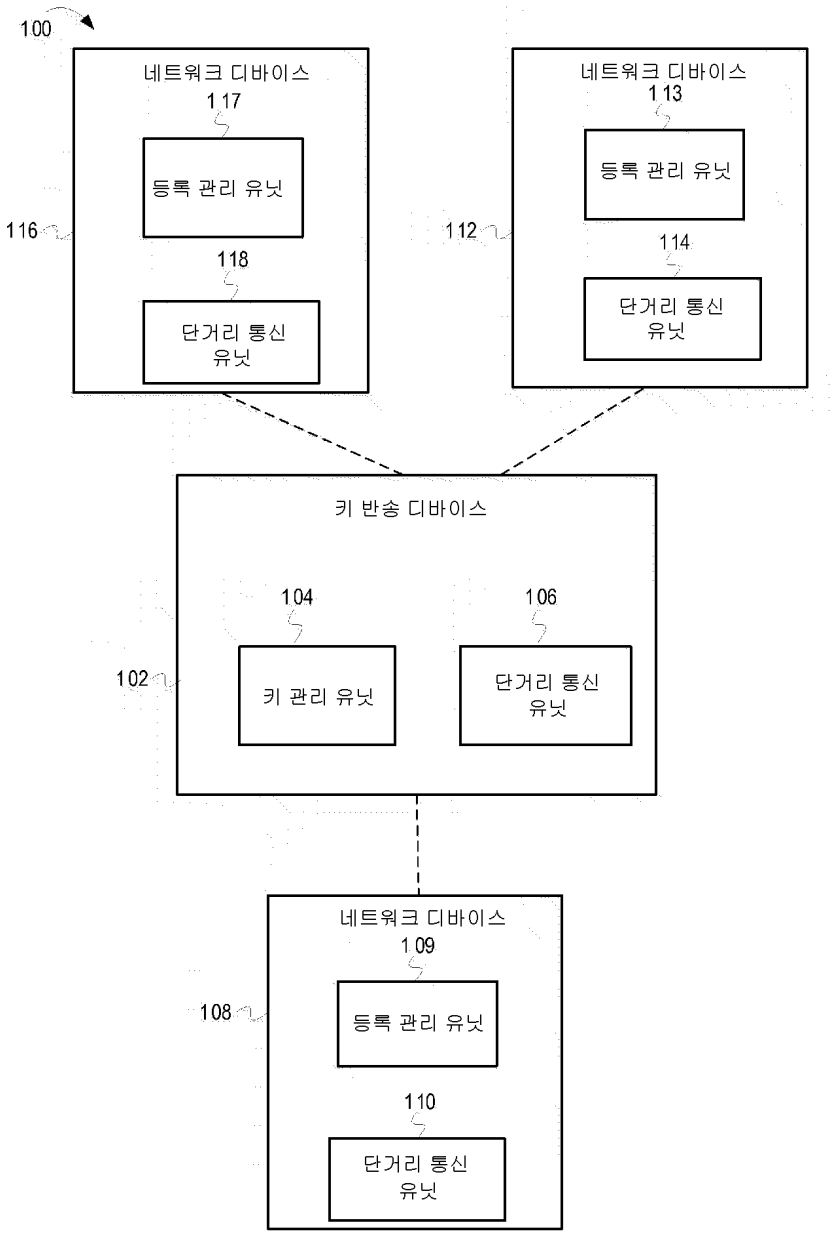
[0336] 이들 기능들 중 임의의 것은 부분적으로(또는 전체적으로) 하드웨어로 구현되고 그리고/또는 프로세서 유닛(2401)상에서 구현되거나 또는 메모리(2403)로 구현될 수 있다. 예를들어, 기능은 주문형 집적회로로, 프로세서 유닛(2401)에서 구현되는 로직으로, 주변 디바이스 또는 카드상의 코-프로세서 등으로 구현될 수 있다. 게다가, 실현물들은 도 24에 예시되지 않은 더 적거나 또는 추가적인 컴포넌트들(예를들어, 비디오 카드들, 오디오 카드들, 추가 네트워크 인터페이스들, 주변 디바이스들 등)를 포함할 수 있다. 프로세서 유닛(2401), 저장 디바이스(들)(2409), I/O 디바이스들(2407), 네트워크 인터페이스(2402) 및 통신 유닛(2405)은 버스(2411)에 커플링된다. 버스(2411)에 커플링되는 것으로 예시될지라도, 메모리(2403)는 프로세서 유닛(2401)에 커플링될 수 있다.

[0337] 실시예들이 다양한 구현들 및 설명들를 참조로 하여 설명되는 반면에, 이들 실시예들이 예시적이며 본 발명의 요지의 범위가 이들에 제한되지 않는다는 것이 이해될 것이다. 일반적으로, 여기에서 설명되는 바와같이 단거리 무선 통신을 사용하여 네트워크 디바이스들을 보안적으로 구성하기 위한 기술들은 임의의 하드웨어 시스템 또는 하드웨어 시스템들과 일치하는 설비들로 구현될 수 있다. 많은 변형들, 수정들, 추가들 및 개선들이 가능하다.

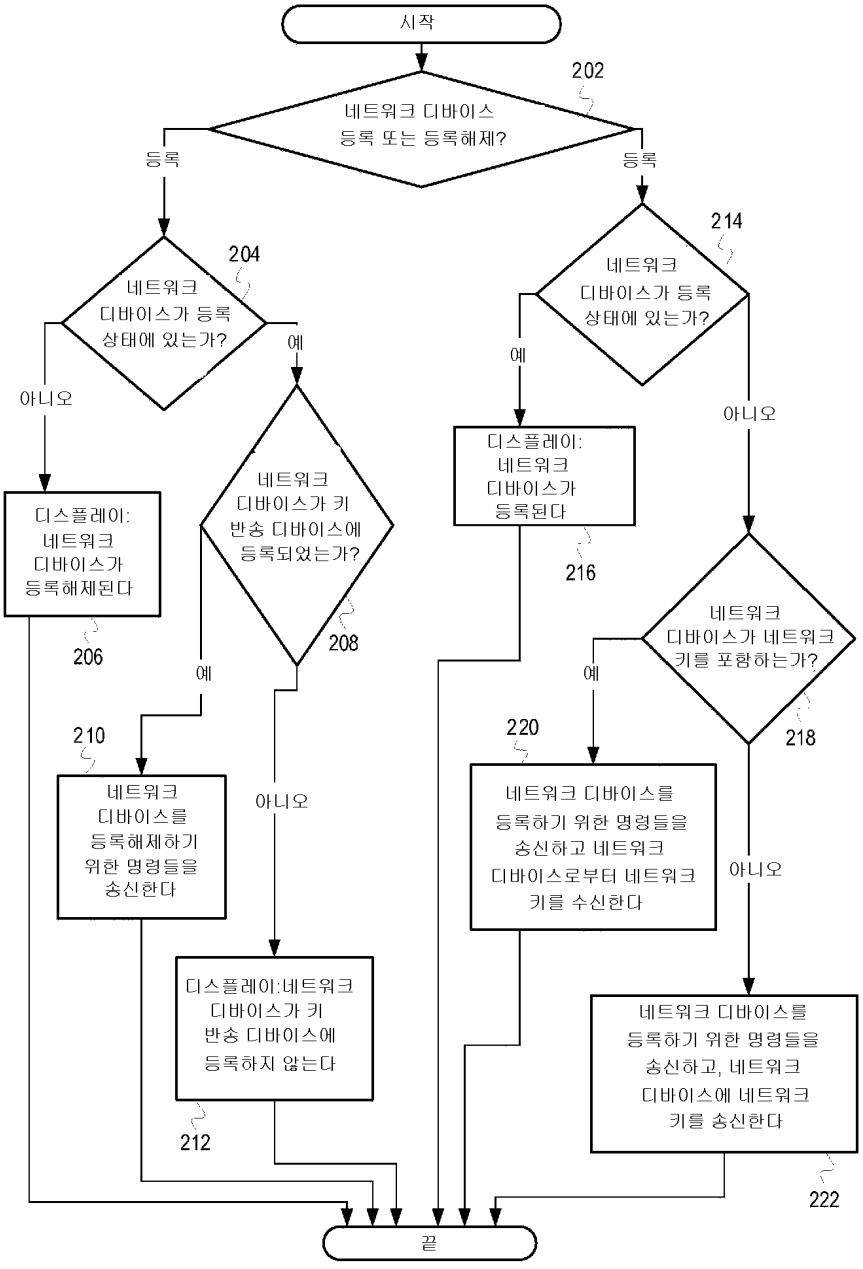
[0338] 단일 사례로서 여기에서 설명되는 컴포넌트들, 동작들 또는 구조들에 대하여 복수의 사례들이 제공될 수 있다. 최종적으로, 다양한 컴포넌트들, 동작들 및 데이터 스토어들 간의 경계들은 어느 정도 임의적이며 특정 동작들은 특정한 예시적인 구성들의 맥락에서 예시된다. 기능의 다른 할당들이 구상되며, 본 발명의 요지의 범위내에 있을 수 있다. 일반적으로, 예시적인 구성들에서 개별 컴포넌트들로서 제시되는 구조들 및 기능은 결합된 구조 또는 컴포넌트로서 구현될 수 있다. 유사하게, 단일 컴포넌트로서 제시되는 구조들 및 기능은 개별 컴포넌트들로서 구현될 수 있다. 이들 및 다른 변형들, 수정들, 추가들 및 개선들이 본 발명의 요지의 범위내에 있을 수 있다.

도면

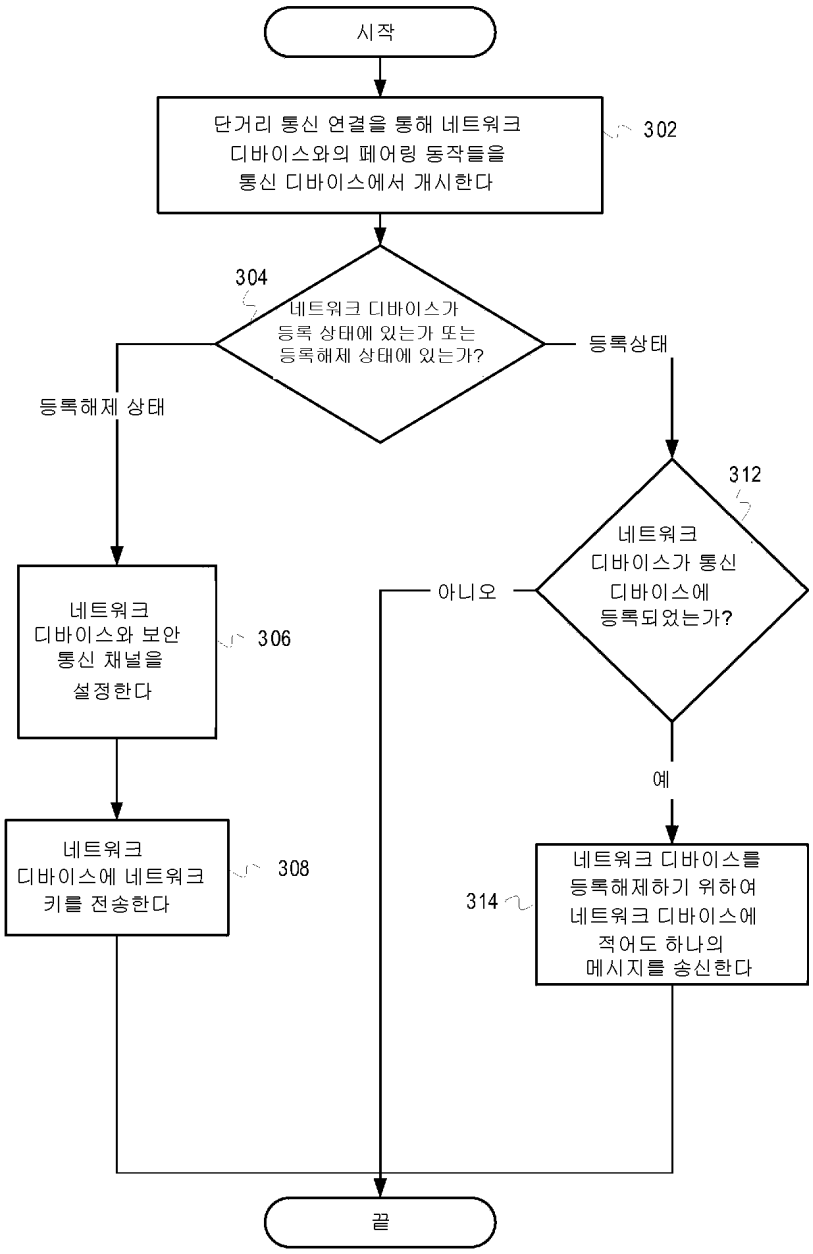
도면1


100
네트워크 디바이스
117
등록 관리 유닛
116
118
단거리 통신 유닛
네트워크 디바이스
113
등록 관리 유닛
112
114
단거리 통신 유닛
키 반송 디바이스
104
106
102
키 관리 유닛
단거리 통신 유닛
네트워크 디바이스
109
등록 관리 유닛
108
110
단거리 통신 유닛

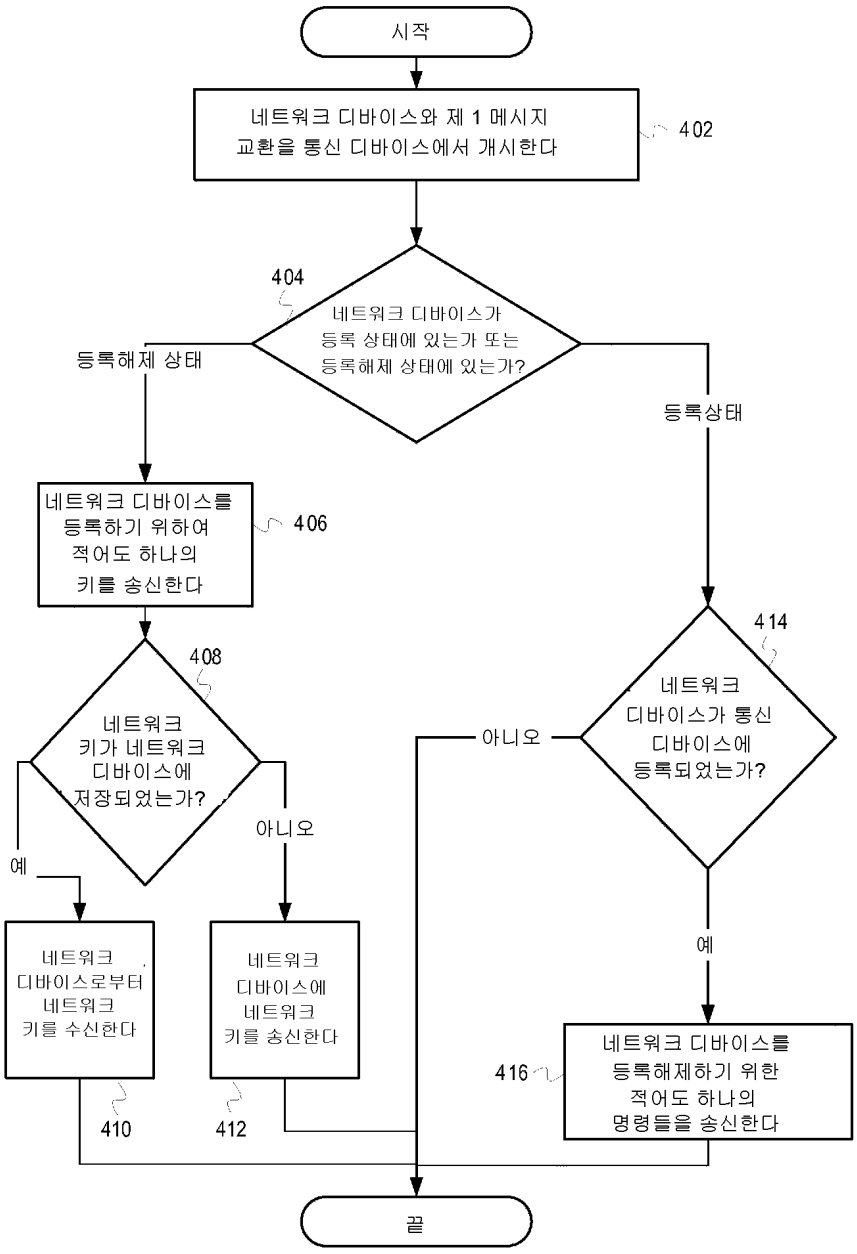
도면2


시작
202
네트워크 디바이스 등록 또는 등록해제?
등록
등록
204
네트워크 디바이스가 등록 상태에 있는가?
예
아니오
214
네트워크 디바이스가 등록 상태에 있는가?
예
아니오
디스플레이: 네트워크 디바이스가 등록해제된다
206
네트워크 디바이스가 키 반송 디바이스에 등록되었는가?
208
디스플레이: 네트워크 디바이스가 등록된다
216
네트워크 디바이스가 네트워크 키를 포함하는가?
218
예
예
210
네트워크 디바이스를 등록해제하기 위한 명령들을 송신한다
아니오
220
네트워크 디바이스를 등록하기 위한 명령들을 송신하고 네트워크 디바이스로부터 네트워크 키를 수신한다
아니오
디스플레이:네트워크 디바이스가 키 반송 디바이스에 등록하지 않는다
212
네트워크 디바이스를 등록하기 위한 명령들을 송신하고, 네트워크 디바이스에 네트워크 키를 송신한다
222
끝

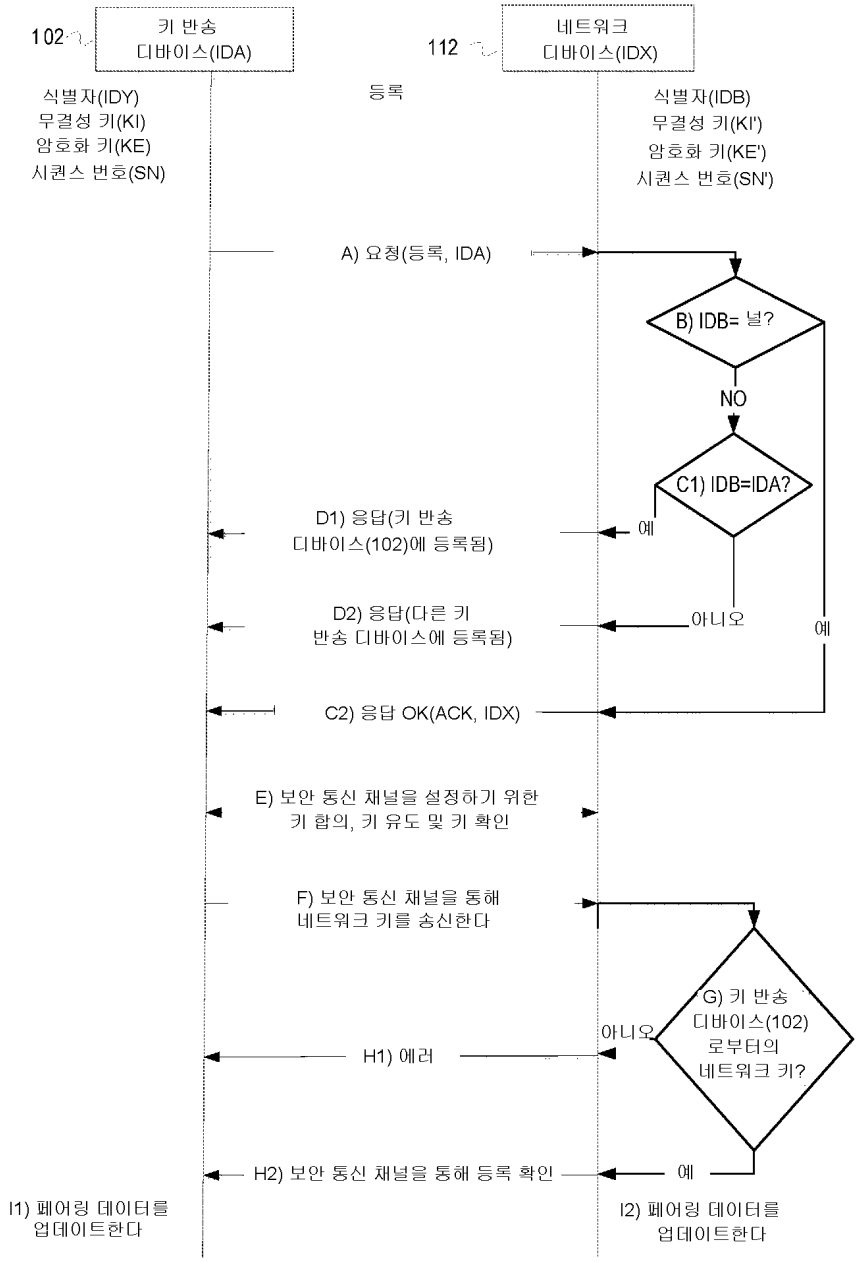
도면3


시작
단거리 통신 연결을 통해 네트워크 디바이스와의 페어링 동작들을 통신 디바이스에서 개시한다
302
304
네트워크 디바이스가 등록 상태에 있는가 또는 등록해제 상태에 있는가?
등록상태
등록해제 상태
312
네트워크 디바이스가 통신 디바이스에 등록되었는가?
아니오
예
네트워크 디바이스와 보안 통신 채널을 설정한다
306
네트워크 디바이스에 네트워크 키를 전송한다
308
314
네트워크 디바이스를 등록해제하기 위하여 네트워크 디바이스에 적어도 하나의 메시지를 송신한다
끝

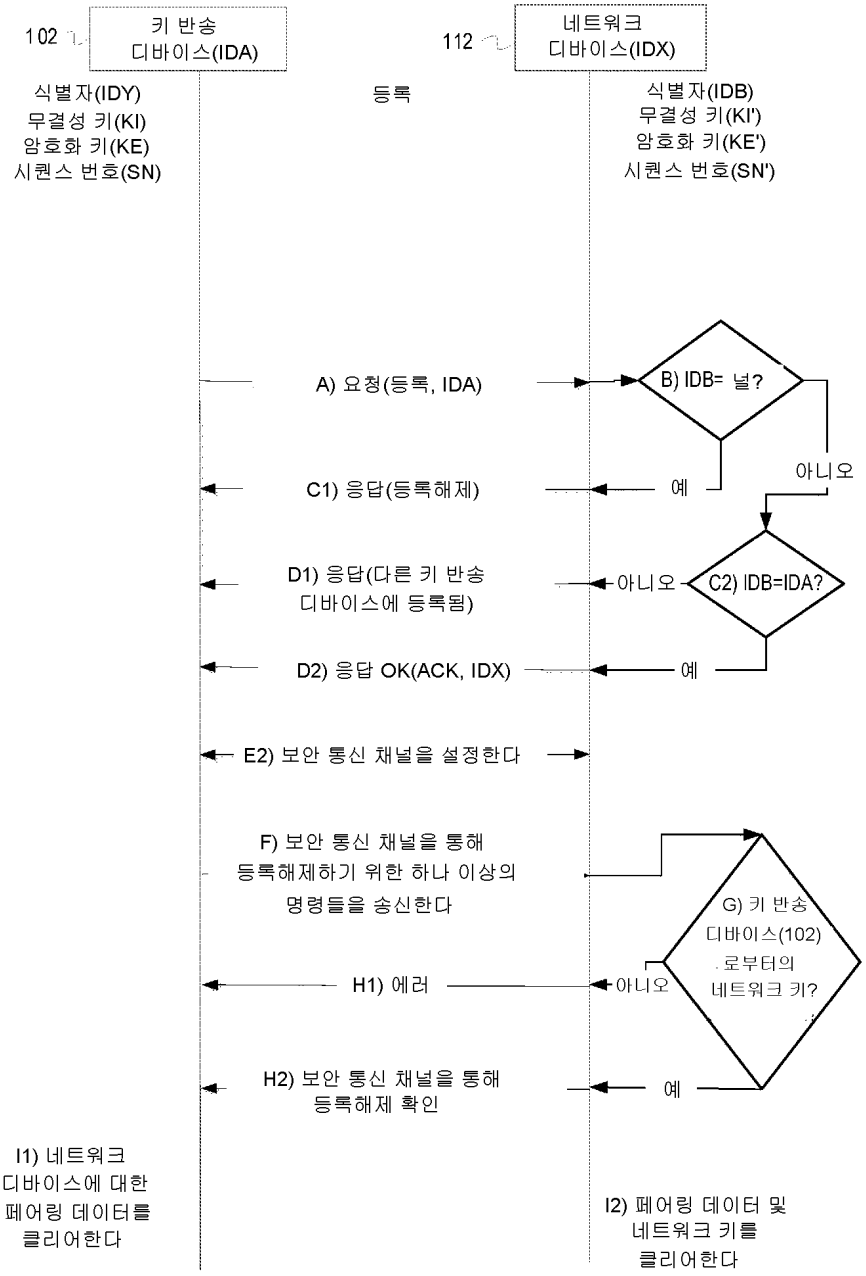
도면4


시작
네트워크 디바이스와 제 1 메시지 교환을 통신 디바이스에서 개시한다
402
404
네트워크 디바이스가 등록 상태에 있는가 또는 등록해제 상태에 있는가?
등록해제 상태
등록상태
네트워크 디바이스를 등록하기 위하여 적어도 하나의 키를 송신한다
406
408
네트워크 키가 네트워크 디바이스에 저장되었는가?
예
아니오
414
네트워크 디바이스가 통신 디바이스에 등록되었는가?
아니오
예
네트워크 디바이스로부터 네트워크 키를 수신한다
410
네트워크 디바이스에 네트워크 키를 송신한다
412
네트워크 디바이스를 등록해제하기 위한 적어도 하나의 명령들을 송신한다
416
끝

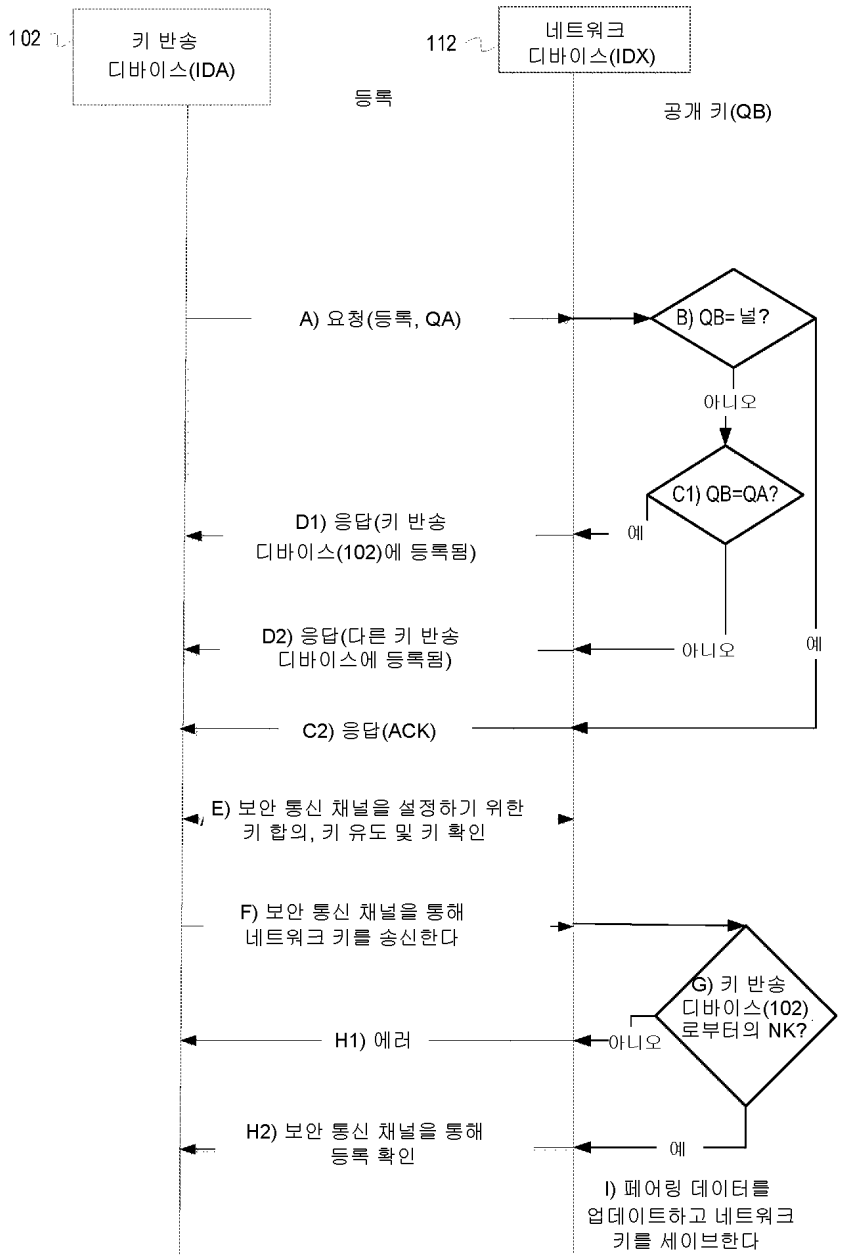
도면5


102
키 반송 디바이스(IDA)
112
네트워크 디바이스(IDX)
식별자(IDY)
무결성 키(KI)
암호화 키(KE)
시퀀스 번호(SN)
등록
식별자(IDB)
무결성 키(KI')
암호화 키(KE')
시퀀스 번호(SN')
A) 요청(등록, IDA)
B) IDB= 널?
NO
C1) IDB=IDA?
예
D1) 응답(키 반송 디바이스(102)에 등록됨)
아니오
D2) 응답(다른 키 반송 디바이스에 등록됨)
예
C2) 응답 OK(ACK, IDX)
E) 보안 통신 채널을 설정하기 위한 키 합의, 키 유도 및 키 확인
F) 보안 통신 채널을 통해 네트워크 키를 송신한다
G) 키 반송 디바이스(102) 로부터의 네트워크 키?
아니오
H1) 에러
예
H2) 보안 통신 채널을 통해 등록 확인
I1) 페어링 데이터를 업데이트한다
I2) 페어링 데이터를 업데이트한다

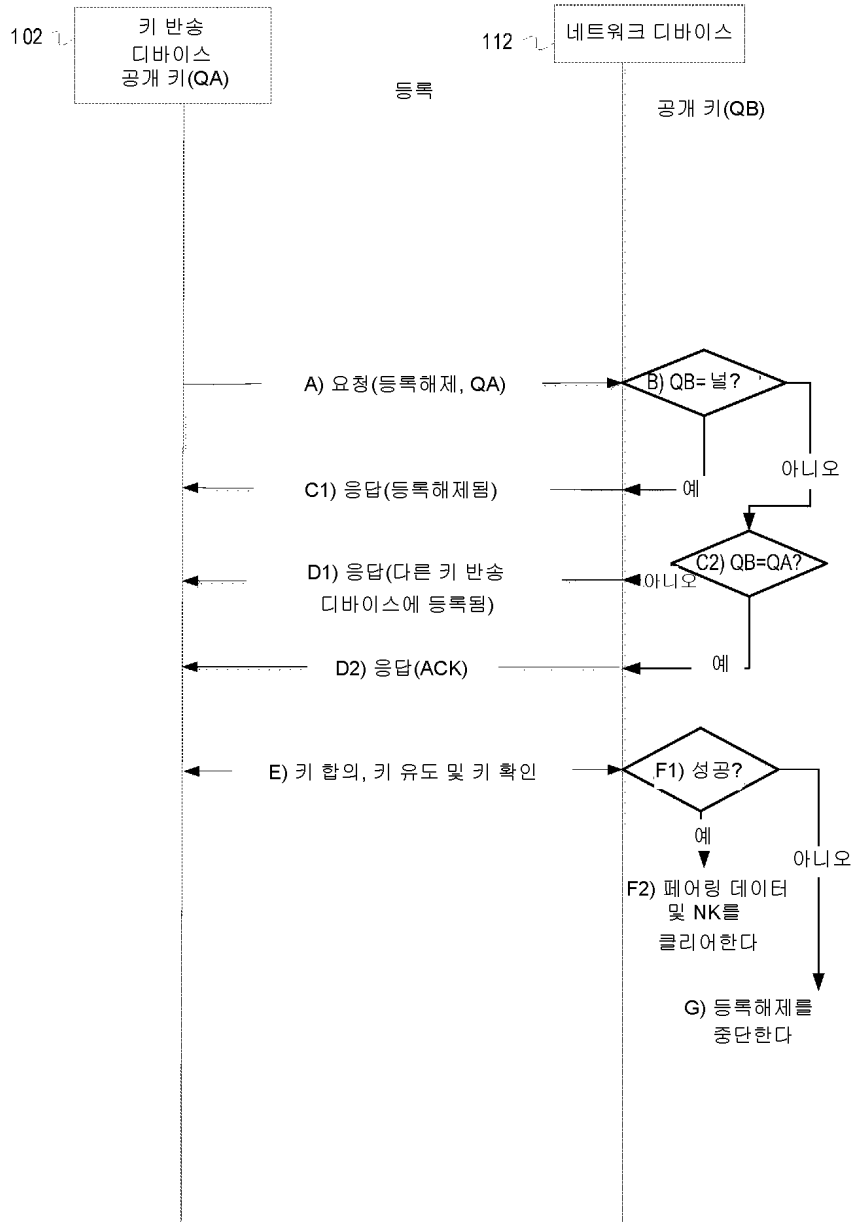
도면6


102
키 반송 디바이스(IDA)
112
네트워크 디바이스(IDX)
식별자(IDY)
무결성 키(KI)
암호화 키(KE)
시퀀스 번호(SN)
등록
식별자(IDB)
무결성 키(KI')
암호화 키(KE')
시퀀스 번호(SN')
A) 요청(등록, IDA)
B) IDB= 널?
예
아니오
C1) 응답(등록해제)
아니오
C2) IDB=IDA?
D1) 응답(다른 키 반송 디바이스에 등록됨)
예
D2) 응답 OK(ACK, IDX)
E2) 보안 통신 채널을 설정한다
F) 보안 통신 채널을 통해 등록해제하기 위한 하나 이상의 명령들을 송신한다
G) 키 반송 디바이스(102) 로부터의 네트워크 키?
아니오
H1) 에러
예
H2) 보안 통신 채널을 통해 등록해제 확인
I1) 네트워크 디바이스에 대한 페어링 데이터를 클리어한다
I2) 페어링 데이터 및 네트워크 키를 클리어한다

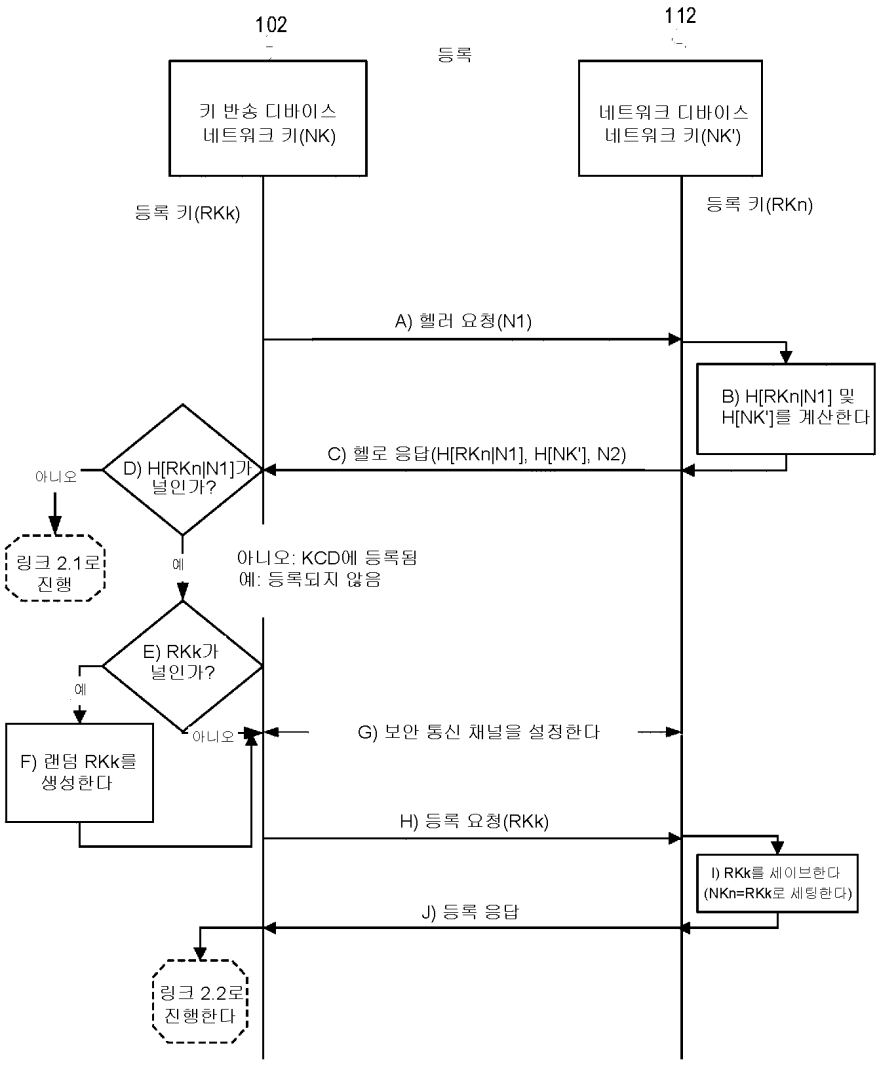
도면7


102
키 반송 디바이스(IDA)
112
네트워크 디바이스(IDX)
등록
공개 키(QB)
A) 요청(등록, QA)
B) QB= 널?
아니오
C1) QB=QA?
예
D1) 응답(키 반송 디바이스(102)에 등록됨)
D2) 응답(다른 키 반송 디바이스에 등록됨)
아니오
예
C2) 응답(ACK)
E) 보안 통신 채널을 설정하기 위한 키 합의, 키 유도 및 키 확인
F) 보안 통신 채널을 통해 네트워크 키를 송신한다
G) 키 반송 디바이스(102) 로부터의 NK?
H1) 에러
아니오
H2) 보안 통신 채널을 통해 등록 확인
예
I) 페어링 데이터를 업데이트하고 네트워크 키를 세이브한다

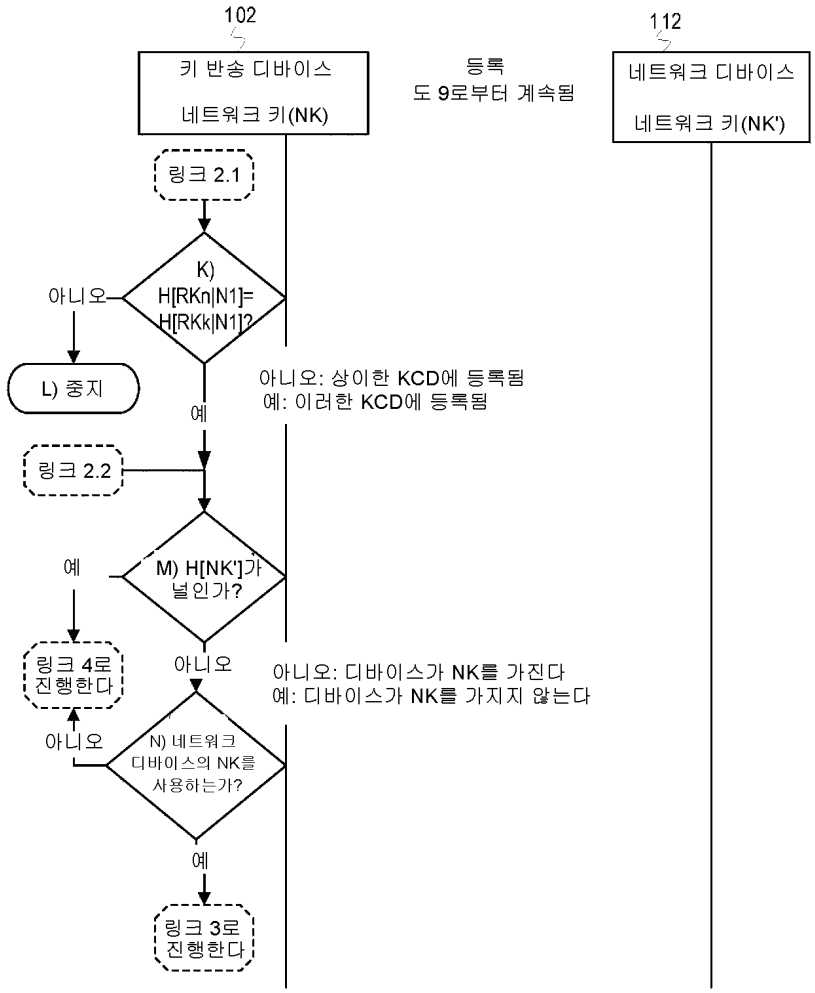
도면8


102
키 반송 디바이스 공개 키(QA)
112
네트워크 디바이스
등록
공개 키(QB)
A) 요청(등록해제, QA)
B) QB= 널?
아니오
C1) 응답(등록해제됨)
예
C2) QB=QA?
D1) 응답(다른 키 반송 디바이스에 등록됨)
아니오
D2) 응답(ACK)
예
E) 키 합의, 키 유도 및 키 확인
F1) 성공?
예
아니오
F2) 페어링 데이터 및 NK를 클리어한다
G) 등록해제를 중단한다

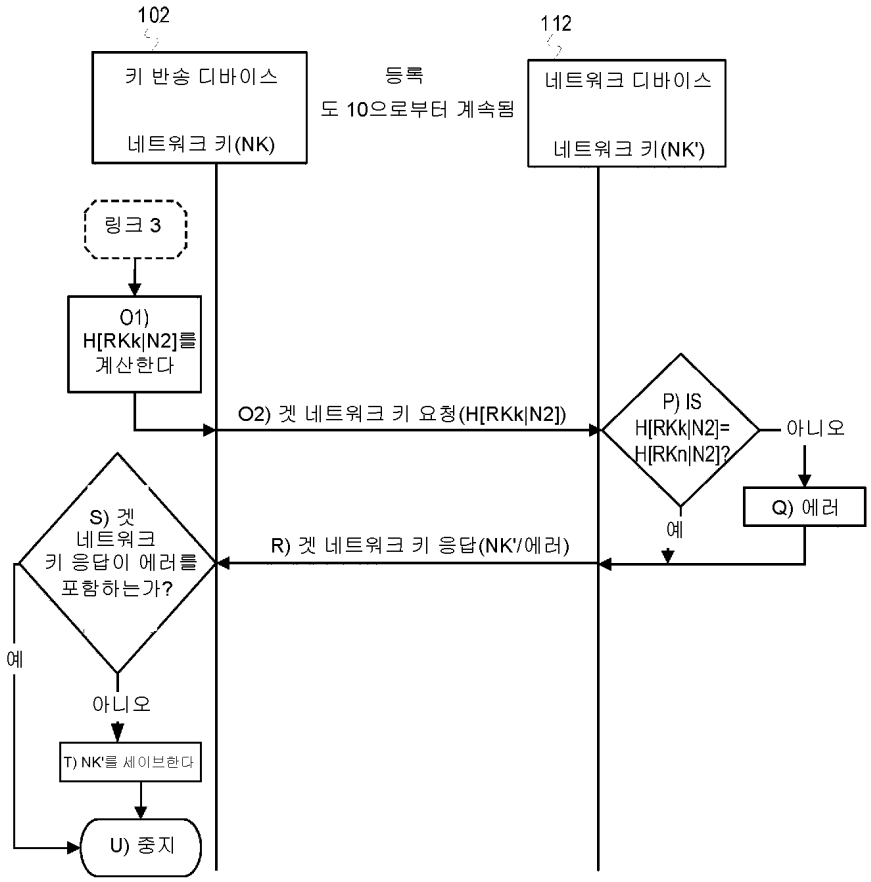
도면9


102
112
등록
키 반송 디바이스
네트워크 키(NK)
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn)
A) 헬러 요청(N1)
B) H[RKn|N1] 및
H[NK']를 계산한다
C) 헬로 응답(H[RKn|N1], H[NK'], N2)
D) H[RKn|N1]가
널인가?
아니오
링크 2.1로
진행
예
아니오: KCD에 등록됨
예: 등록되지 않음
E) RKk가
널인가?
예
아니오
F) 랜덤 RKk를
생성한다
G) 보안 통신 채널을 설정한다
H) 등록 요청(RKk)
I) RKk를 세이브한다
(NKn=RKk로 세팅한다)
J) 등록 응답
링크 2.2로
진행한다

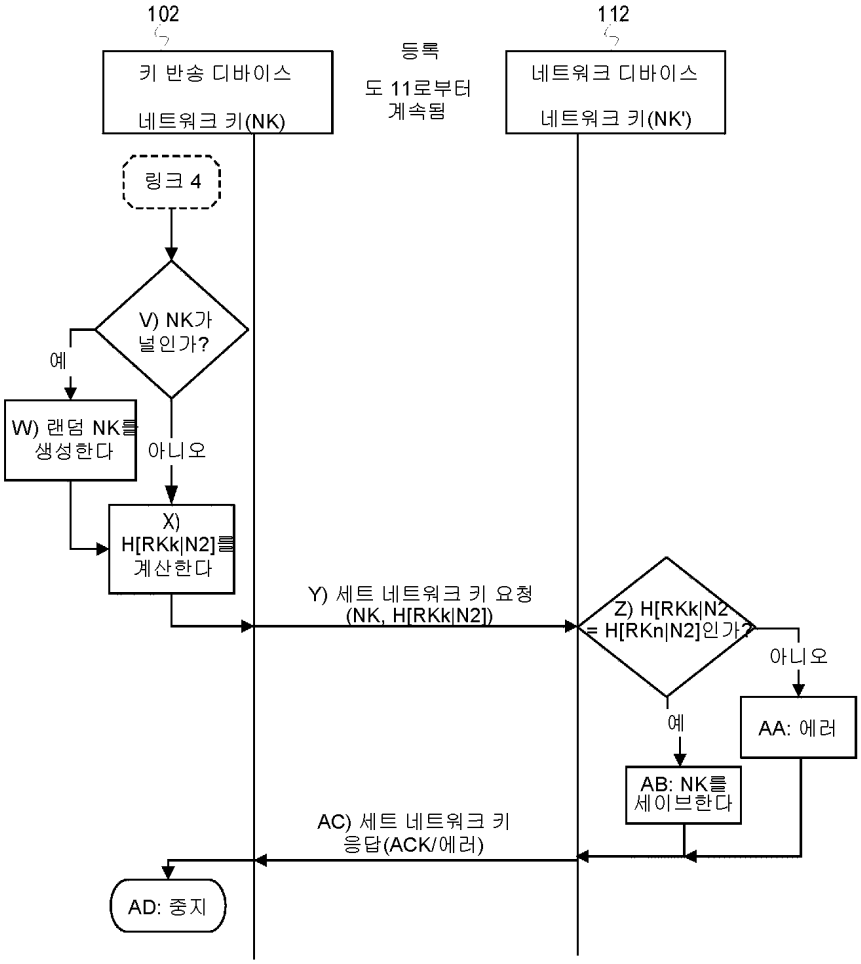
도면10


102
키 반송 디바이스
네트워크 키(NK)
등록
도 9로부터 계속됨
112
네트워크 디바이스
네트워크 키(NK')
링크 2.1
K)
H[RKn|N1]=
H[RKk|N1]?
아니오
L) 중지
예
아니오: 상이한 KCD에 등록됨
예: 이러한 KCD에 등록됨
링크 2.2
M) H[NK']가
널인가?
예
아니오
링크 4로
진행한다
아니오: 디바이스가 NK를 가진다
예: 디바이스가 NK를 가지지 않는다
아니오
N) 네트워크
디바이스의 NK를
사용하는가?
예
링크 3로
진행한다

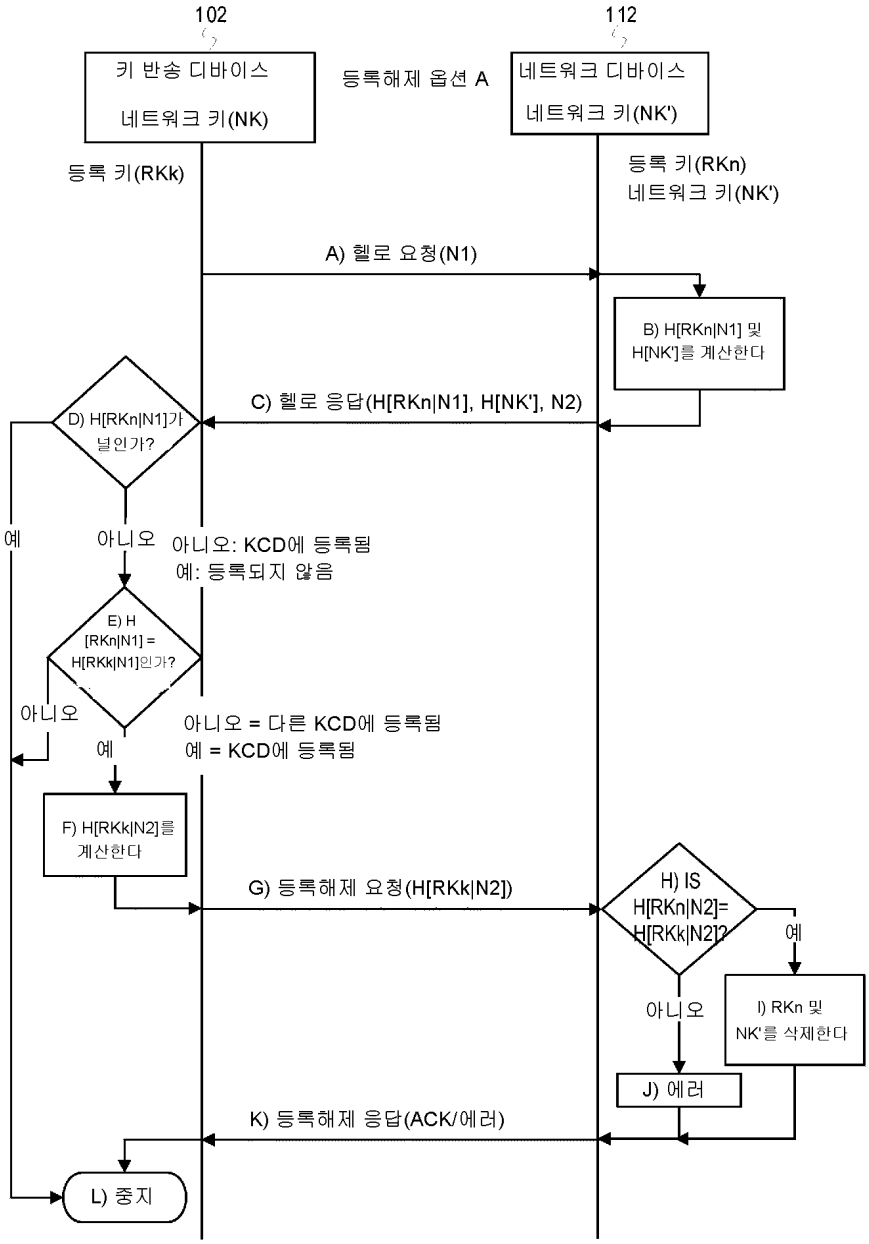
도면11


102
키 반송 디바이스
네트워크 키(NK)
등록
도 10으로부터 계속됨
112
네트워크 디바이스
네트워크 키(NK')
링크 3
O1) H[RKk|N2]를 계산한다
O2) 겟 네트워크 키 요청(H[RKk|N2])
P) IS H[RKk|N2]= H[RKn|N2]?
아니오
Q) 에러
예
R) 겟 네트워크 키 응답(NK'/에러)
S) 겟 네트워크 키 응답이 에러를 포함하는가?
예
아니오
T) NK'를 세이브한다
U) 중지

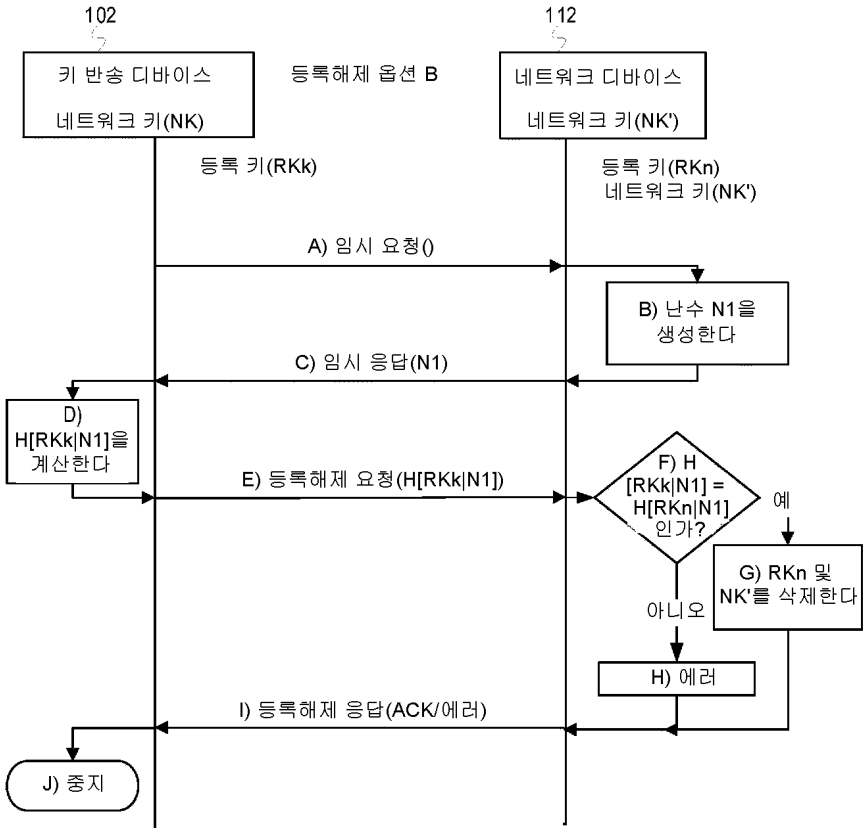
도면12


102
112
등록
도 11로부터
계속됨
키 반송 디바이스
네트워크 키(NK)
네트워크 디바이스
네트워크 키(NK')
링크 4
V) NK가
널인가?
예
아니오
W) 랜덤 NK를
생성한다
X)
H[RKk|N2]를
계산한다
Y) 세트 네트워크 키 요청
(NK, H[RKk|N2])
Z) H[RKk|N2
= H[RKn|N2]인가?
아니오
예
AA: 에러
AB: NK를
세이브한다
AC) 세트 네트워크 키
응답(ACK/에러)
AD: 중지

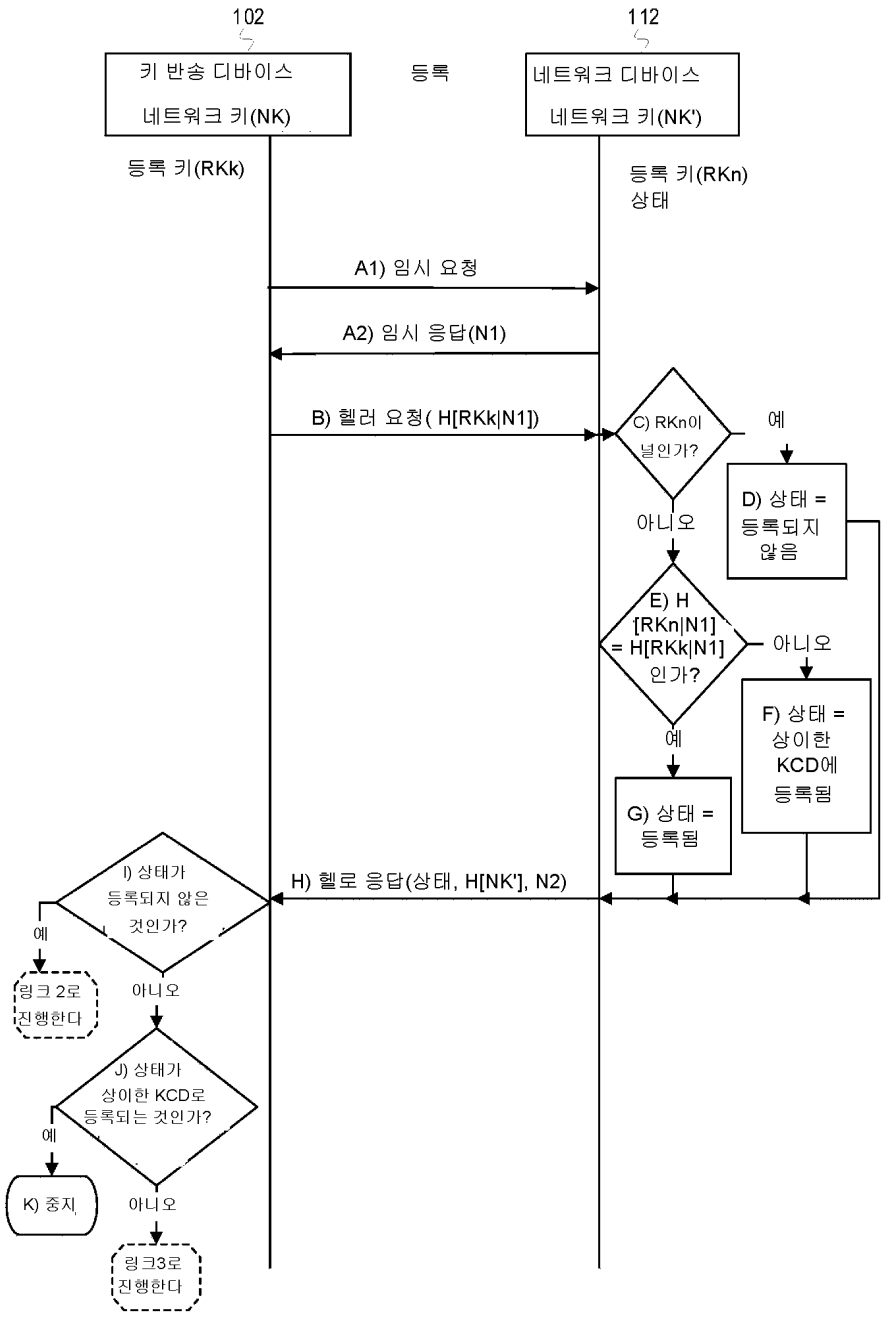
도면13


102
112
키 반송 디바이스
네트워크 키(NK)
등록해제 옵션 A
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn)
네트워크 키(NK')
A) 헬로 요청(N1)
B) H[RKn|N1] 및 H[NK']를 계산한다
C) 헬로 응답(H[RKn|N1], H[NK'], N2)
D) H[RKn|N1]가 널인가?
예
아니오
아니오: KCD에 등록됨
예: 등록되지 않음
E) H [RKn|N1] = H[RKk|N1]인가?
아니오
예
아니오 = 다른 KCD에 등록됨
예 = KCD에 등록됨
F) H[RKk|N2]를 계산한다
G) 등록해제 요청(H[RKk|N2])
H) IS H[RKn|N2]= H[RKk|N2]?
예
아니오
I) RKn 및 NK'를 삭제한다
J) 에러
K) 등록해제 응답(ACK/에러)
L) 중지

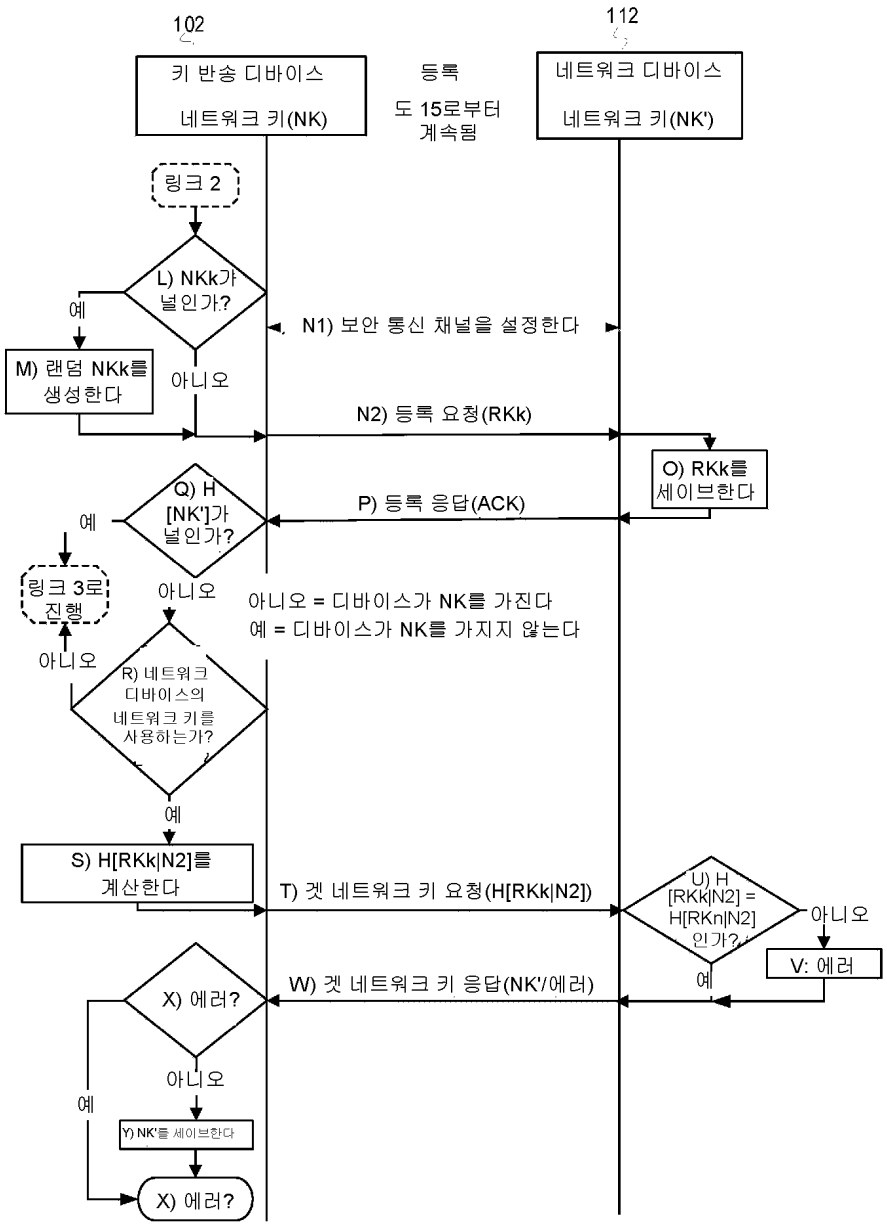
도면14


102
112
키 반송 디바이스
네트워크 키(NK)
등록해제 옵션 B
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn)
네트워크 키(NK')
A) 임시 요청()
B) 난수 N1을 생성한다
C) 임시 응답(N1)
D) H[RKk|N1]을 계산한다
E) 등록해제 요청(H[RKk|N1])
F) H [RKk|N1] = H[RKn|N1] 인가?
예
G) RKn 및 NK'를 삭제한다
아니오
H) 에러
I) 등록해제 응답(ACK/에러)
J) 중지

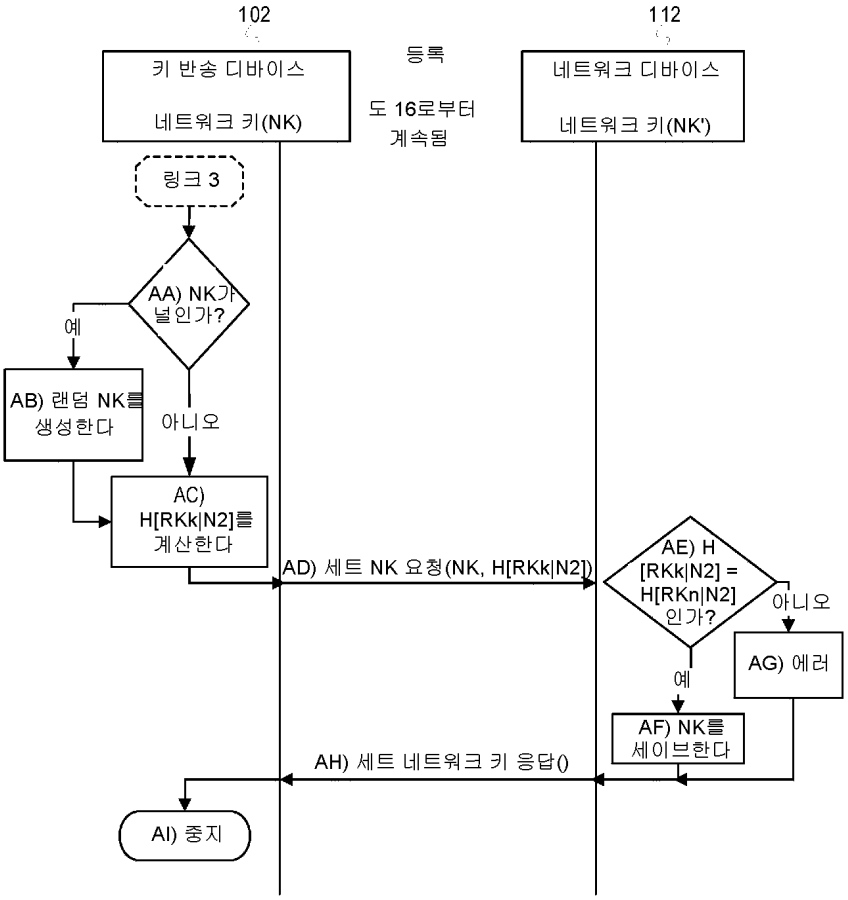
도면15


102
112
키 반송 디바이스
네트워크 키(NK)
등록
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn)
상태
A1) 임시 요청
A2) 임시 응답(N1)
B) 헬러 요청(H[RKk|N1])
C) RKn이 널인가?
예
D) 상태 = 등록되지 않음
아니오
E) H [RKn|N1] = H[RKk|N1] 인가?
아니오
F) 상태 = 상이한 KCD에 등록됨
예
G) 상태 = 등록됨
H) 헬로 응답(상태, H[NK'], N2)
I) 상태가 등록되지 않은 것인가?
예
링크 2로 진행한다
아니오
J) 상태가 상이한 KCD로 등록되는 것인가?
예
K) 중지
아니오
링크3로 진행한다

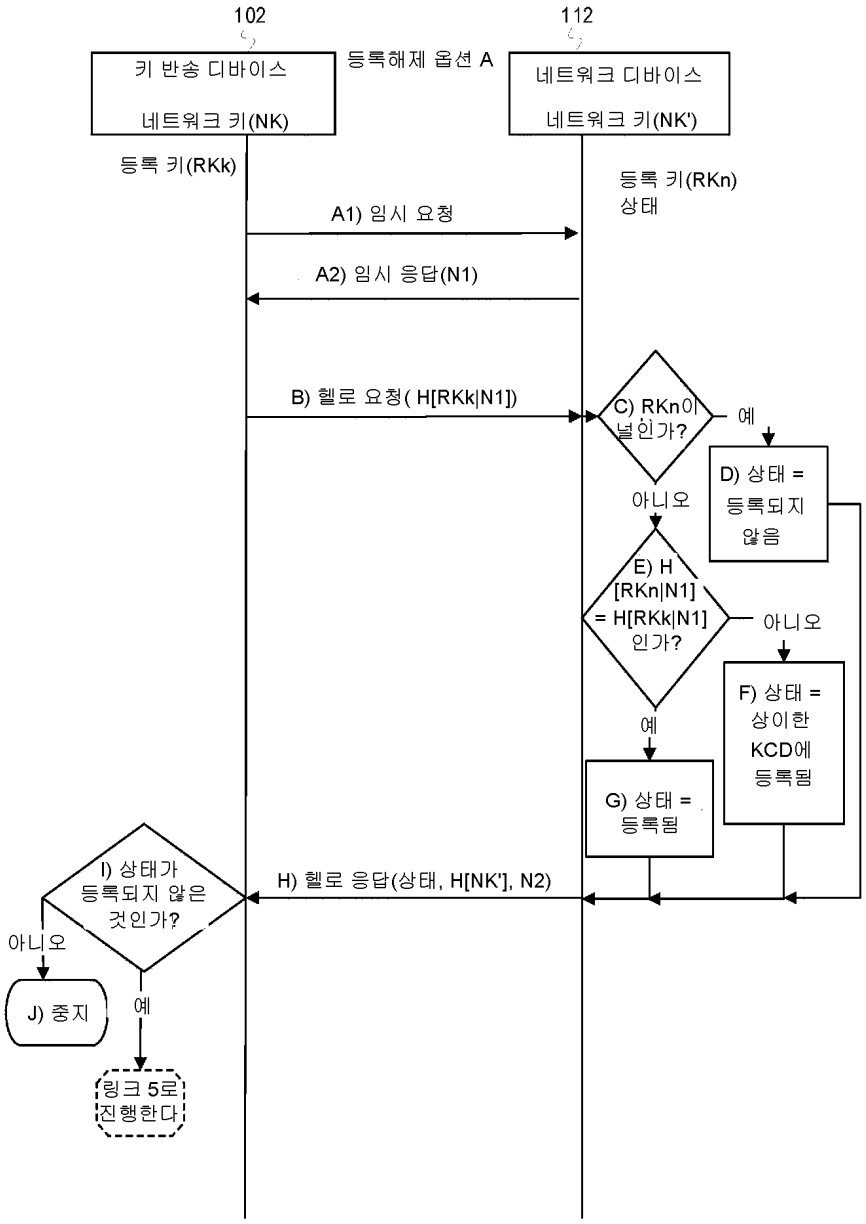
도면16


102
112
키 반송 디바이스
네트워크 키(NK)
등록
도 15로부터 계속됨
네트워크 디바이스
네트워크 키(NK')
링크 2
L) NKk가 널인가?
예
아니오
M) 랜덤 NKk를 생성한다
N1) 보안 통신 채널을 설정한다
N2) 등록 요청(RKk)
O) RKk를 세이브한다
Q) H[NK']가 널인가?
P) 등록 응답(ACK)
예
링크 3로 진행
아니오
아니오 = 디바이스가 NK를 가진다
예 = 디바이스가 NK를 가지지 않는다
아니오
R) 네트워크 디바이스의 네트워크 키를 사용하는가?
예
S) H[RKk|N2]를 계산한다
T) 겟 네트워크 키 요청(H[RKk|N2])
U) H[RKk|N2] = H[RKn|N2] 인가?
아니오
V: 에러
예
W) 겟 네트워크 키 응답(NK'/에러)
X) 에러?
아니오
예
Y) NK'를 세이브한다
X) 에러?

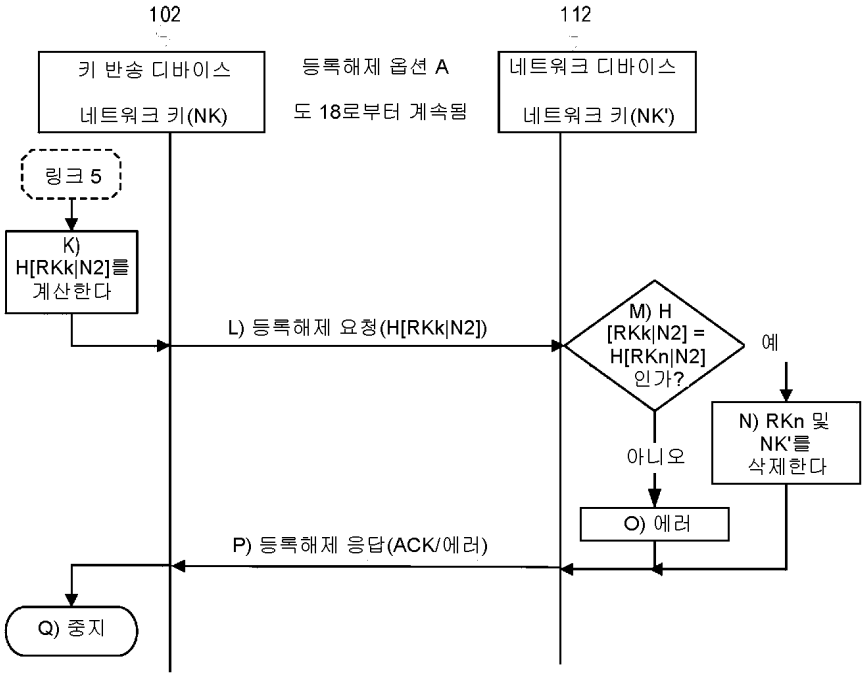
도면17


102
112
키 반송 디바이스
네트워크 키(NK)
등록
도 16로부터
계속됨
네트워크 디바이스
네트워크 키(NK')
링크 3
AA) NK가 널인가?
예
아니오
AB) 랜덤 NK를 생성한다
AC) H[RKk|N2]를 계산한다
AD) 세트 NK 요청(NK, H[RKk|N2])
AE) H[RKk|N2] = H[RKn|N2] 인가?
아니오
AG) 에러
예
AF) NK를 세이브한다
AH) 세트 네트워크 키 응답()
AI) 중지

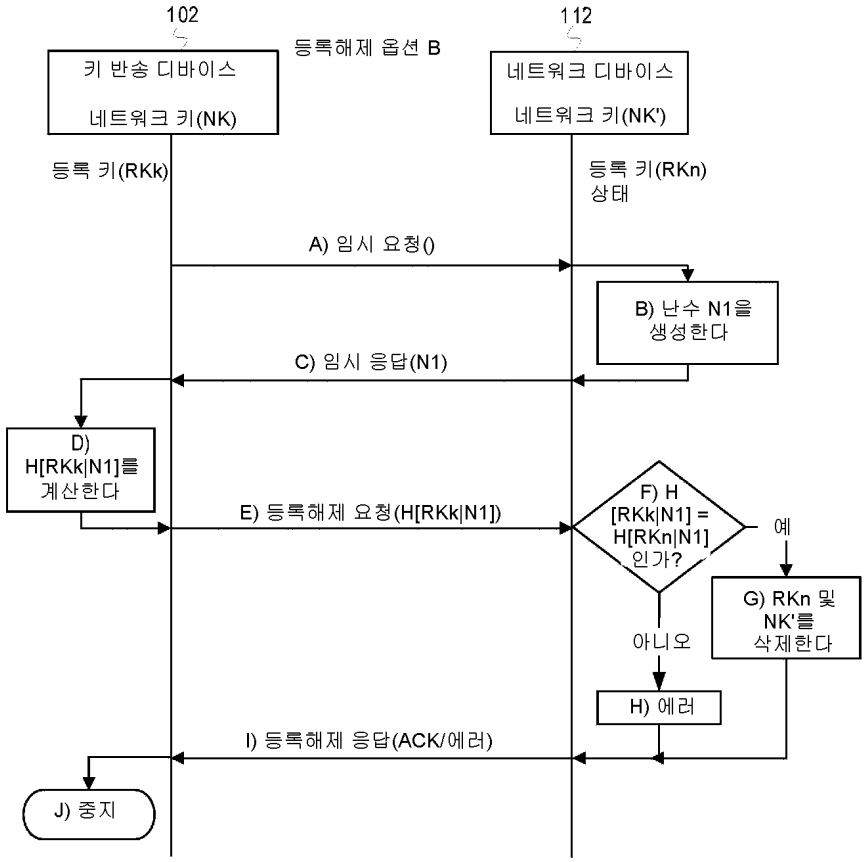
도면18


102
112
키 반송 디바이스
네트워크 키(NK)
등록해제 옵션 A
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn)
상태
A1) 임시 요청
A2) 임시 응답(N1)
B) 헬로 요청(H[RKk|N1])
C) RKn이 널인가?
예
D) 상태 = 등록되지 않음
아니오
E) H[RKn|N1] = H[RKk|N1] 인가?
아니오
F) 상태 = 상이한 KCD에 등록됨
예
G) 상태 = 등록됨
H) 헬로 응답(상태, H[NK'], N2)
I) 상태가 등록되지 않은 것인가?
아니오
J) 중지
예
링크 5로 진행한다

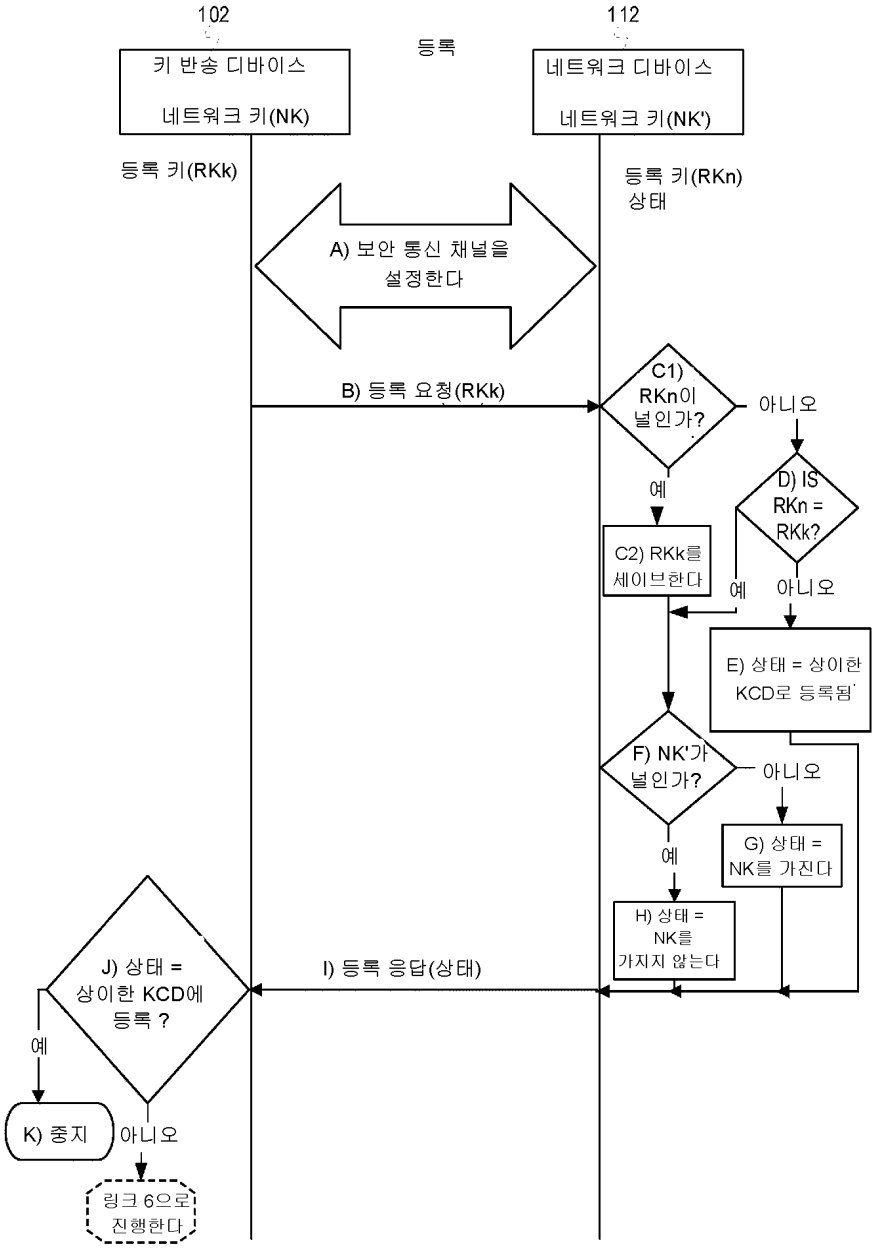
도면19


102
112
키 반송 디바이스
네트워크 키(NK)
등록해제 옵션 A
도 18로부터 계속됨
네트워크 디바이스
네트워크 키(NK')
링크 5
K) H[RKk|N2]를 계산한다
L) 등록해제 요청(H[RKk|N2])
M) H[RKk|N2] = H[RKn|N2] 인가?
예
N) RKn 및 NK'를 삭제한다
아니오
O) 에러
P) 등록해제 응답(ACK/에러)
Q) 중지

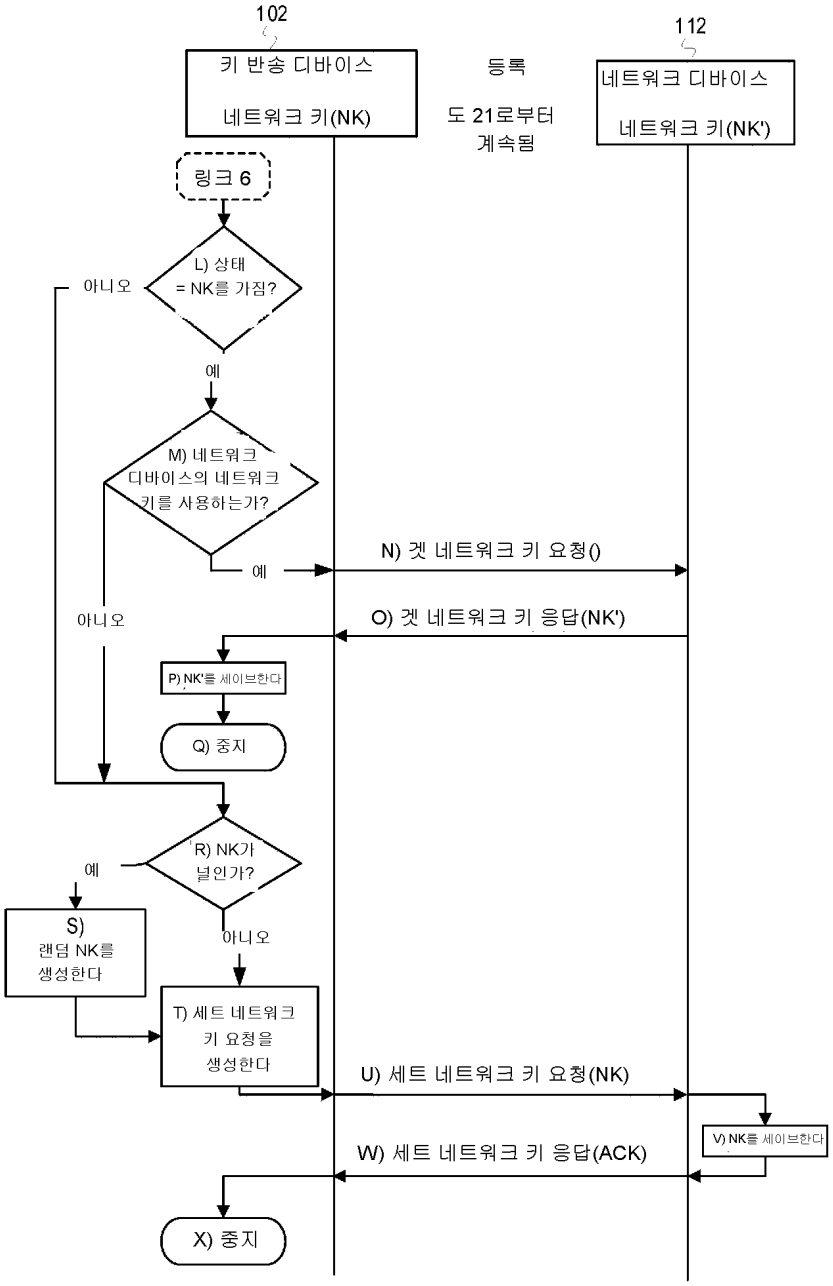
도면20


102
112
키 반송 디바이스
네트워크 키(NK)
등록해제 옵션 B
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn) 상태
A) 임시 요청()
B) 난수 N1을 생성한다
C) 임시 응답(N1)
D) H[RKk|N1]를 계산한다
E) 등록해제 요청(H[RKk|N1])
F) H[RKk|N1] = H[RKn|N1] 인가?
예
G) RKn 및 NK'를 삭제한다
아니오
H) 에러
I) 등록해제 응답(ACK/에러)
J) 중지

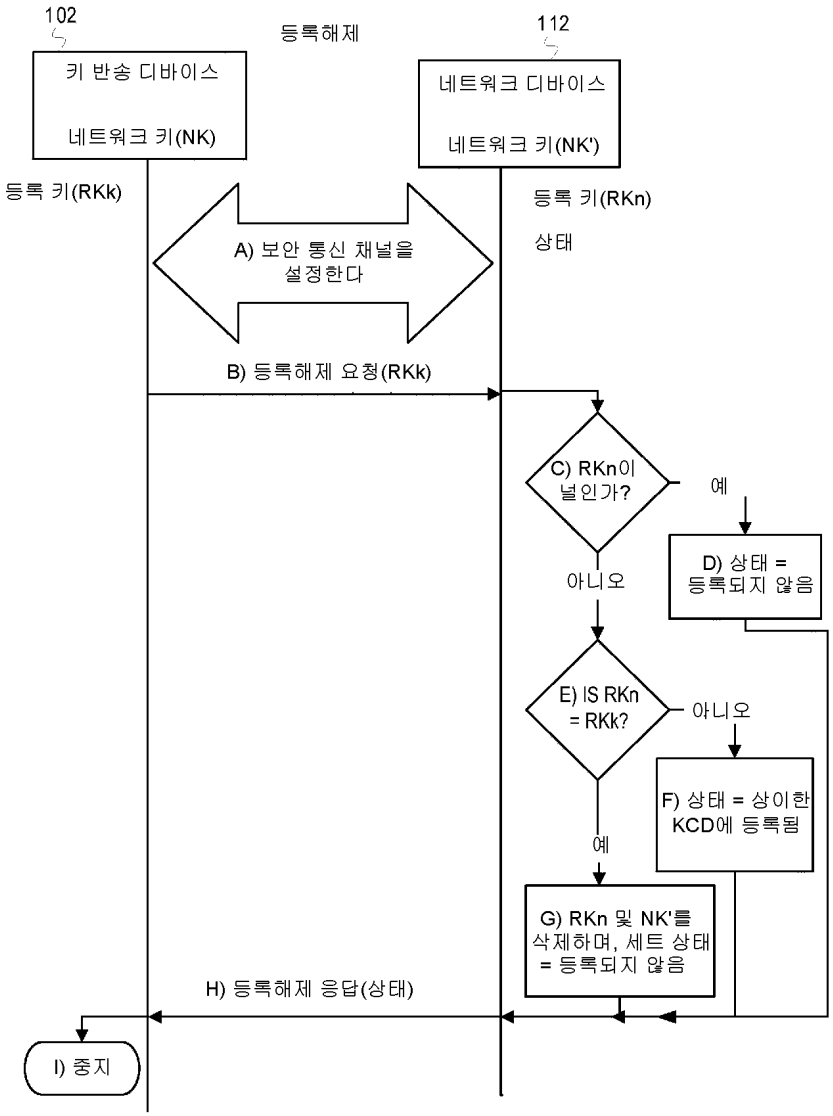
도면21


102
112
등록
키 반송 디바이스
네트워크 키(NK)
등록 키(RKk)
네트워크 디바이스
네트워크 키(NK')
등록 키(RKn)
상태
A) 보안 통신 채널을 설정한다
B) 등록 요청(RKk)
C1) RKn이 널인가?
아니오
예
D) IS RKn = RKk?
C2) RKk를 세이브한다
예
아니오
E) 상태 = 상이한 KCD로 등록됨
F) NK'가 널인가?
아니오
예
G) 상태 = NK를 가진다
H) 상태 = NK를 가지지 않는다
I) 등록 응답(상태)
J) 상태 = 상이한 KCD에 등록 ?
예
K) 중지
아니오
링크 6으로 진행한다

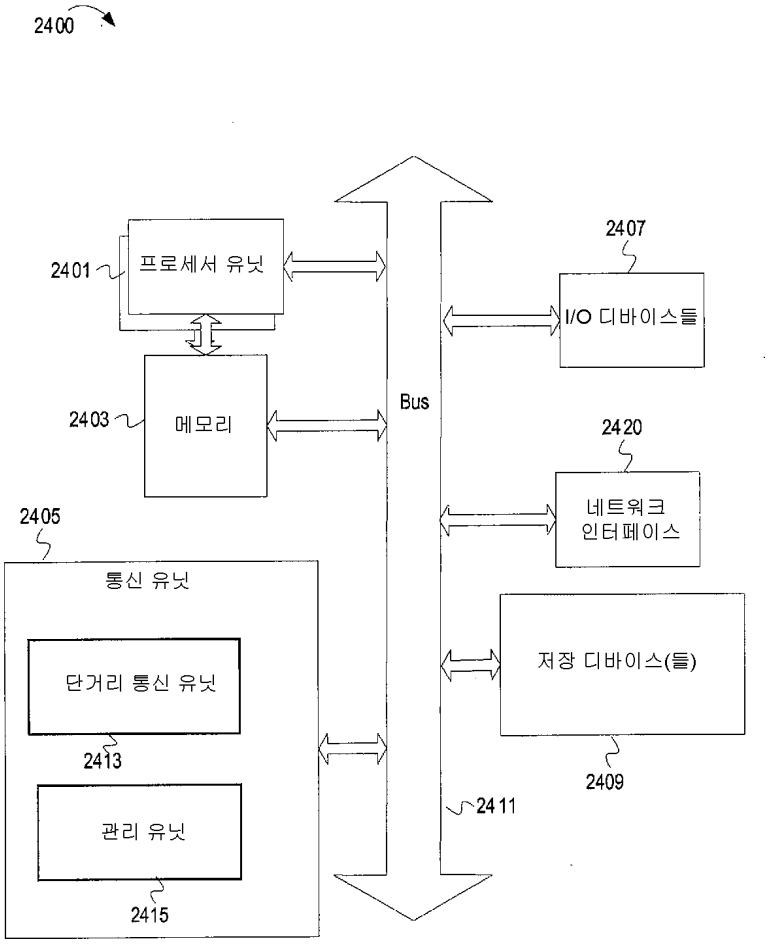
도면22


102
키 반송 디바이스
네트워크 키(NK)
등록
도 21로부터
계속됨
112
네트워크 디바이스
네트워크 키(NK')
링크 6
L) 상태
= NK를 가짐?
아니오
예
M) 네트워크
디바이스의 네트워크
키를 사용하는가?
예
N) 겟 네트워크 키 요청()
아니오
O) 겟 네트워크 키 응답(NK')
P) NK'를 세이브한다
Q) 중지
R) NK가
널인가?
예
아니오
S)
랜덤 NK를
생성한다
T) 세트 네트워크
키 요청을
생성한다
U) 세트 네트워크 키 요청(NK)
V) NK를 세이브한다
W) 세트 네트워크 키 응답(ACK)
X) 중지

도면23


102
등록해제
112
키 반송 디바이스
네트워크 키(NK)
네트워크 디바이스
네트워크 키(NK')
등록 키(RKk)
등록 키(RKn)
상태
A) 보안 통신 채널을 설정한다
B) 등록해제 요청(RKk)
C) RKn이 널인가?
예
D) 상태 = 등록되지 않음
아니오
E) IS RKn = RKk?
아니오
F) 상태 = 상이한 KCD에 등록됨
예
G) RKn 및 NK'를 삭제하며, 세트 상태 = 등록되지 않음
H) 등록해제 응답(상태)
I) 중지

도면24


2400
2401
프로세서 유닛
2403
메모리
Bus
2407
I/O 디바이스들
2420
네트워크
인터페이스
2405
통신 유닛
단거리 통신 유닛
2413
관리 유닛
2415
저장 디바이스(들)
2409
2411